Our daily essential services and applications, be they commercial or military, are increasingly dependent on integrated satellite and terrestrial networks. Until recently, satellite networks have been, by and large, stand-alone in design. Increasingly, however, satellite networks are integrated with terrestrial networks, creating a hybrid system. While this integration has extended access to many communications applications, it has also broadened the opportunity for cybersecurity issues and risks.

Cyber-attacks, focused primarily on identity and financial theft in the commercial world, are becoming a critical issue in space. Cyber-attacks on satellites can include jamming, denial of service (DoS), hacking attacks on communication networks and piracy. Piracy, or unauthorized access, occurs when carriers (with content) are transmitted toward a satellite without any prior contract with the satellite operator. Intentional jamming can be the result of one party’s objection to the content (political, cultural, social, etc.) of the targeted carrier, extenuating circumstances (political situation, social unrest, etc.) and in the worst case, intent to disable a satellite to gain a military or economic advantage.

An Increasing Threat

Communications, finance and trade, air and sea transport, energy and weather forecasting are among the infrastructure applications that rely heavily on satellites to fulfill their promise. These functions are so pervasive in our society that we are essentially oblivious to the role satellites play. Should one or more of these satellites be compromised, either by radio frequency jamming or direct physical attack, the results could be catastrophic. Each infrastructure area has a particular set of unique characteristics and vulnerabilities, yet also has much in common with other functional areas due to their interdependencies, which could lead to a cascading effect if even only one sector was compromised.

Among the top data breaches announced in 2017 were:

**Equifax**, September 7, 2017: Equifax, one of the three largest credit agencies in the U.S., suffered a breach that may affect 143 million consumers.
Yahoo, October 3 reported that the huge data breach in August 2013 affected every user on its service: all three billion user accounts, up from the one billion figure Yahoo initially reported.

Taringa, September 17: The Argentina-based social network Taringa was alerted to a leak of about 28 million user records

A Verizon Data Breach Investigations report states the following for 2017:

- 75% of breaches were perpetrated by outsiders
- 62% featured hacking
- 81% leveraged stolen or weak passwords
- 51% included malware
- 24% of the victims were financial institutions
- 66% of malware was distributed via infected email attachments
- 61% of the data breach victims in this year’s report are businesses with under 1,000 employees
- 95% of phishing attacks that led to a breach were followed by some sort of software installation

Roots of Vulnerability

Unlike optical fiber or copper cables, satellites send their radio frequency (RF) signals through air and space, creating the opportunity for anyone with the appropriate knowledge, means and motivation to interfere with the RF signal. This can be accomplished by jamming, variations of which include blocking undesirable radio and television broadcasts from being transmitted into a country and blocking satellite navigation signals. Increasingly, with the use of Commercial-Off-The-Shelf (COTS) products such as open-source software, vulnerabilities are multiplied. It is one thing to protect proprietary products from latent malware being inserted during development, but the risk is compounded when acquiring the products from a long supply chain.

Another challenge is the speed with which technology advances, coupled with the fact that it can take two to three years to build and launch a satellite designed for a 10-15 year lifespan. In these cases one not only has to embed cybersecurity defenses in the satellite during the design stage; but must be prepared to retro-fit on-orbit satellites with newer cyber defenses during the satellite’s lifespan.

Of all the vulnerabilities those with the most potential for severe disruption are satellite-based navigational systems...Galileo in Europe, BeiDou in China, GLONASS in Russia, the Indian Regional Navigation Satellite System (IRNSS), and the U.S. global positioning system (GPS), which is the most pervasive and supports much of the world’s civil infrastructure.

Military Impact

These vulnerabilities are driving change in military space, as well as in the commercial world, and countering them requires more resilience, agility, and speed in order to predict, pre-empt, and prevent the growing range of threats.

Aside from disruption of civil infrastructure, cyber-attacks on satellites could weaken responses to military threats, by compromising satellite command and control (C2), operational monitoring and payload performance. Doug Loverro, former U.S. Deputy Assistant Secretary of Defense for space policy outlined six major
areas the military needs to invest in, which he dubbed “D4P2”:

- Disaggregation - Separating missions that have different purposes, so that a single satellite is not carrying both conventional and nuclear systems or surveillance and communication systems.
- Diversity - Using multiple systems to achieve the same goal, such as having U.S. equipment that can use both GPS and Europe’s Galileo navigation system.
- Distribution - Spreading out capabilities across multiple satellites, so that no one satellite is fundamental to the system working.
- Deception - Not letting adversaries know which satellites are carrying which systems.
- Protection - Hardening satellites to defend against threats.
- Proliferation - Deploying multiple satellites to conduct the same mission, where a single satellite can carry out the complete capability while the others provide redundancy.

Direct attacks on space-based assets are more likely to result in jamming and denial of service scenarios as previously discussed. However, attacks mounted via a compromised ground station network may potentially yield access to sensitive data or the ability to manipulate command and control systems resulting in considerably greater impact.

Approaches to Cyber Defense in Space

While the U.S. Department of Defense plans to spend $2 billion over the next five years on a new constellation of Global Positioning System satellites that will be hardened to withstand electronic interference from hostile nations, satellite ground systems need to be protected as well. In making the announcement U.S. Air Force Secretary Heather Wilson said the Air Force is motivated to move ahead with this new constellation amid growing concerns that a growing number of nations are developing electronic weapons to jam or interfere with GPS signals. “All those things are an obvious awareness of American dominance in space. I cannot think of a military mission that doesn’t depend on space. Our potential adversaries know it, and we need to protect those vital assets.”
Contending with the reality of future attacks, the strategy of investing in more agile, resilient satellite capabilities is being bolstered by new space. Newly planned LEO and MEO constellations (by OneWeb, SpaceX, O3b and others), are radically changing the economics, lowering the cost of satellites an order of magnitude that makes the concept of resilience through numbers and basic protection capabilities viable. As space becomes an ever more contested environment, small satellites can act as pawns on a chessboard…protecting large military and commercial satellites…the Kings, Queens, and Bishops of space!

Protecting a few critical and expensive satellites, which are obvious targets, with larger numbers of cheaper, yet agile satellites – Pawns if you will – creates a more defensible space.

...And on the Ground

In a recent interview with Via Satellite Magazine (March 2018), KPN Chief Information Security Officer (CISO) Jaya Baloo said that with respect to cyber vulnerability, she would focus on the ground station to determine how one could spoof or clone the communications over a poorly authenticated or an un-authenticated channel. The hacker would assume that on the un-authenticated channel, there would be one or two bands you could communicate with from your ground station to the satellite. If it was un-authenticated, the hacker could then pirate your signal communications to that satellite, she explained.

Approaches to Cyber Security

For terrestrial and space environments Kratos offers a range of cybersecurity testing, monitoring and hardening solutions to reduce vulnerability and minimize risk:

Interference Cancellation

Deliberate jamming, or RFI, is one of the more prevalent attacks. Traditional approaches to resolving interference require identifying the source and when possible working with the interfering party to mitigate the effects. SigX® is a proactive signal cancellation solution from Kratos that offers an alternate approach to resolving interference without relying on cooperation from the interfering party. SigX directly mitigates RF interference (RFI) as shown in Figure 1 by simultaneously canceling up to four CW (Continuous Waveform) or sweeping CW signals in real-time to protect valuable bandwidth and help assure application and/or mission effectiveness.

*Figure 1. SigX cancels CW interference signals in real-time to protect valuable bandwidth.*
Information Assurance

Information Assurance (IA) hardening is another approach to protecting operating systems to ensure system software, firmware and applications are updated to stay ahead of exploits that attack flaws in the underlying code. Kratos RT Logic has a proven history of executing IA hardening for both commercial and government organizations. It now offers IA hardening as a service that provides consistent IA hardened operating system (OS) updates on a quarterly basis and is fully compliant with the U.S Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) hardening requirements.

Security Assessments

Satellite operators use traditional security monitoring tools as well as those uniquely designed for satellites. Kratos offers a SATCOM Cybersecurity Assessment service that addresses the increasing threats and unique requirements of the satellite industry. Cybersecurity Assessments help satellite organizations identify and prioritize threats and their mitigation. The result is a detailed view of satellite network preparedness along with recommended steps required to mitigate risks and ensure compliance with applicable regulations, standards and guidelines.

CyberC4 is an integrated family of products designed for the unique cyber defense needs of satellite ground network environments including situational awareness, and active defense for total protection from cyber-attacks. Kratos protected communications products and services continuously monitor SATCOM networks for cyber threats, harden SATCOM equipment against exploits and defend against insider threats.

The Market

The global military cyber security market is expected to be worth nearly US$10 billion in 2017 and is expected increase to reach almost US$14 billion by 2027, representing a CAGR of about 3.5% during the forecast period. According to the “Global Military Cyber Security Market 2017-2027” report, the global market for military cyber security is expected to be valued at over US$130 billion during the forecast period, and is expected to be dominated by North America, followed by Asia-Pacific and the European markets.

Conclusion

The cyber threat to satellites is not a US, European, or Asian threat…it is of global concern. While anti-cyber technologies and strategies that can anticipate threats as well as react to them will be key to neutralizing cyber-attacks…they will be far more effective if nations work together, share information, develop industry-led standards for knowledge exchange, risk assessment and management, and share technology advances in a timely manner. Just as industrial stove-piped structures can cripple innovation, so to can a stove-piped national approach to cyber security defeat its purpose.

Yen-Wu Chen is Vice President of Asian Operations at Kratos Communication based in Lanham, Maryland U.S.A. He has 40 years’ experience in the IT and satellite sectors and is responsible for Kratos Communications’ Asian business. Mr. Chen has worked at Kratos for over 30 years and has held several engineering and management positions with Singer Link Simulation Systems and Integral Systems, prior to its acquisition by Kratos.

1 Final global numbers for 2017 not yet published. Date for this report is November 2017