CISO MAG

beyond cybersecurity

Volume 1 | Issue 3 | November - December 2017

CLOUD FORECAST: THUNDERSTORMS AND LIGHTNING

RAPID7

From the CISO Perspective to Cloud Security Assessments

Learn How to Make the Leap With Confidence

The secret is out:
Enterprises large and small have moved to the cloud, and more are making the move daily. Whether you're an early adopter or you've been battling that persistent strain of nephophobia going around, it's important to thoroughly understand and evaluate potential cloud vendors, instilling confidence for your organization and your customers.

Download our Cloud Security Toolkit to help you evaluate potential cloud vendors.

http://bit.ly/2ivU4I9

Get insight into how other companies are approaching cloud opportunities, and instill confidence across your organization today.

INDEX

EDITOR'S NOTE

The world is witnessing a paradigm shift in terms of data storage. As each day passes, organizations are exploring new ways to exploit cloud storage solutions, leveraging IaaS, PaaS, and even SaaS mediums. The adoption rate at present is at an all-time high. The number of organizations gaining competence and advantage through cloud utilization has doubled in the past couple of years and is expected to skyrocket in future. Cloud storage solutions are touted to be advantageous in terms of usability, bandwidth, accessibility, cost savings, and even disaster recovery.

But a wide open network perimeter has given chief information security officers sleepless nights. In the last couple of months, we have all read about poor configuration in S3 buckets resulting in massive leaks. In our cover story, we explore the hurdles faced by CISOs in handling security in a cloud environment, as well as exploring cloud bursting opportunities.

In our Buzz section, we discuss the impending threat of space hacking, where satellites orbiting around the planet turn into threat vectors. We also discuss several scenarios that have already occurred and how several state-sponsored actors are honing their skills in this new realm.

We have Kevin O'Leary, CISO of GE China, Under the Spotlight for this issue. O'Leary shares his insights about the new and controversial China Cyber Law and how seriously the nation is taking cybersecurity. We also interviewed Richard Rushing, CISO of Motorola Mobility. Rushing, who is also known as a 'Wi-Fi Guru', speaks about Wi-Fi security and other cybersecurity issues.

Tell us what you think of this issue. If you have any suggestions, comments or queries, please reach us at editorial@cisomag.com.

Jay Bavisi
Editor-in-Chief

CISO MAG
beyond cybersecurity

Volume 1 | Issue 3
November - December 2017

Editorial
International Editor
Amber Pedroncelli
amber.pedroncelli@eccouncil.org

Senior Editor
Rahul Arora
rahul.arora@eccouncil.org

Senior Feature Writer
Preeti Panwar
preeti.p@eccouncil.org

Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Media and Design
Media Director
Saba Mohammad
saba.mohammad@eccouncil.org

Design Head and Visualizer
MSH Rabbani
rabbani@eccouncil.org

Designer
Jeevana Rao Jinaga
jeevana.j@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

Senior Director,
Compliance & Governance
Cherylann Vanderhide
cherylann@eccouncil.org

Marketing & Sales
General Manager
Meghana Vyas
meghana.vyas@eccouncil.org

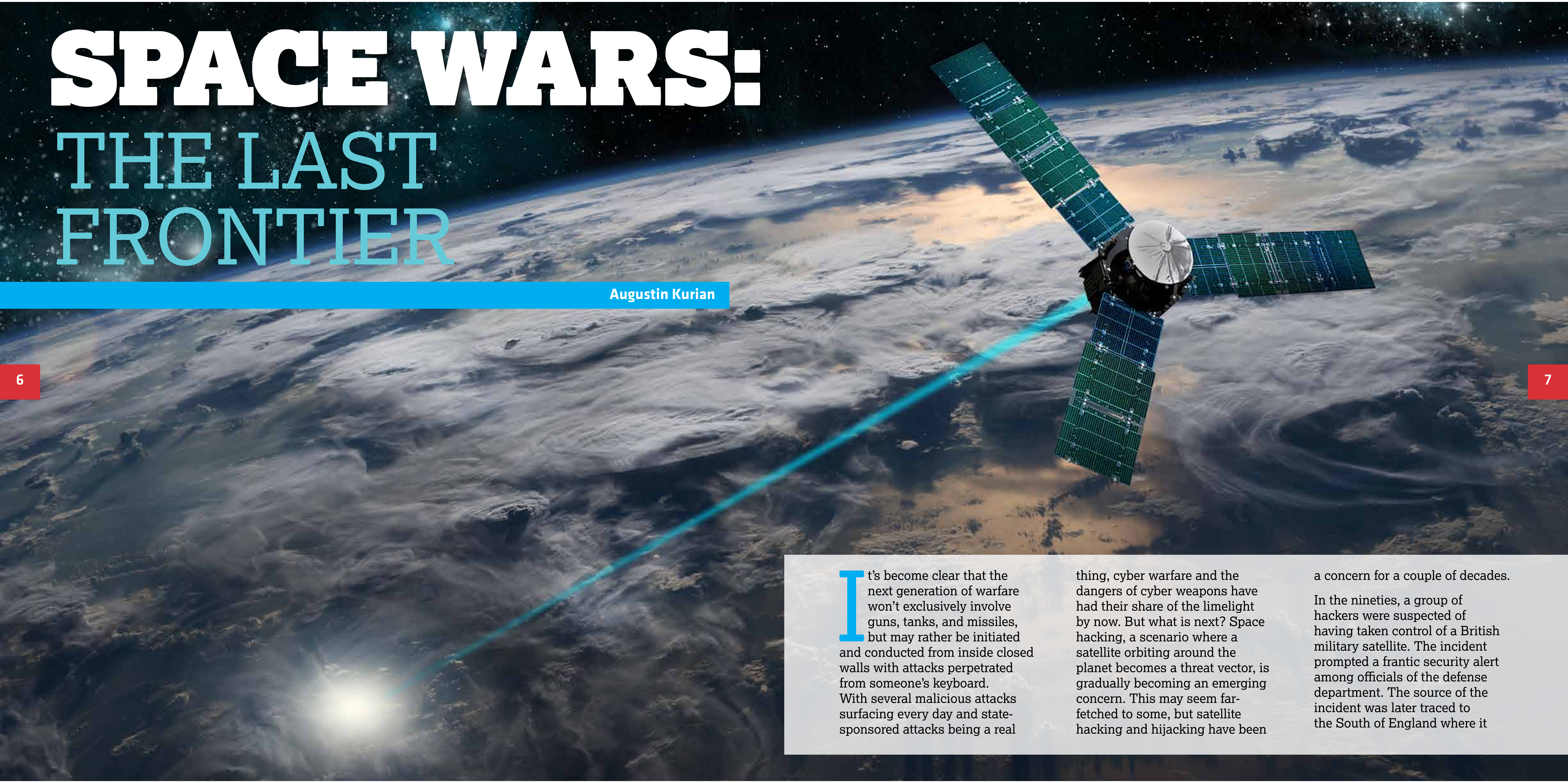
Marketing Manager
Jinu Francis
jinu.francis@eccouncil.org

Sales Manager - India
Basant Das
basant.das@eccouncil.org

Sales Manager - North America
Jessica Johnson
jessica.johnson@eccouncil.org

Technology
Director of Technology
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Rahul Arora.



SPACE WARS: THE LAST FRONTIER

Augustin Kurian

It's become clear that the next generation of warfare won't exclusively involve guns, tanks, and missiles, but may rather be initiated and conducted from inside closed walls with attacks perpetrated from someone's keyboard.

With several malicious attacks surfacing every day and state-sponsored attacks being a real thing, cyber warfare and the dangers of cyber weapons have had their share of the limelight by now. But what is next? Space hacking, a scenario where a satellite orbiting around the planet becomes a threat vector, is gradually becoming an emerging concern. This may seem far-fetched to some, but satellite hacking and hijacking have been a concern for a couple of decades.

In the nineties, a group of hackers were suspected of having taken control of a British military satellite. The incident prompted a frantic security alert among officials of the defense department. The source of the incident was later traced to the South of England where it

was found that hackers found a way to control the satellites and change "the characteristics of channels used to convey military communications, satellite television and telephone calls."

During an interview with *NBC News*, Jeff Matthews, Director of Venture Strategy and Research at the Space Frontier Foundation, said, "Space allows for some very unique business-use cases and opportunities, and when done right, can really go a long way to protecting communication interests and national infrastructure. However, we have to be very aware about the information security side up in space and down here."

> "Space allows for some very unique business-use cases and opportunities, and when done right, can really go a long way to protecting communication interests and national infrastructure. However, we have to be very aware about the information security side up in space and down here."

A recent Chatham House paper pointed out that cybersecurity in space has remained unrecognized as a potential vulnerability. According to the paper, there is an "increasingly blurred line between 'offensive' and 'defensive' activities in cyber and space, given that, technologically, the offence is easier and more cost-effective than defence." It further stated, "More advanced countries are increasingly vulnerable to attack from less developed states, and from terrorist groups and other actors such as organized criminals. In addition, the technologies for the space sector are developed and sourced from all over the world; the space supply chain can, therefore, be considered a truly internationalized business environment that is not yet well regulated with cybersecurity in mind."

While the approach of many governments to cybersecurity is becoming more effective, the paper warned that "the conjunction of cyber and space remains vulnerable to exploitation in the context of complex and internationalized supply chains and space-related infrastructure."

Reports have also suggested that hacking a satellite is a rather easy task. At the Chaos Communication Camp (a security conference) in 2015, hackers Sec and Schneider demonstrated "how to eavesdrop on Iridium pager traffic using the Camp badge" in their presentation titled 'Iridium Hacking: please don't sue us.' The Iridium satellite network, developed by Motorola, consisted of 66 active satellites in low Earth orbit and was a highly vulnerable vector. The hackers said "The problem isn't that Iridium has poor security. It's that it has no security. With just the radio and an onboard PCB antenna, you can collect 22 percent of all the packets you can receive with a proper Iridium antenna. You just load the software on your PC, you attach the radio and you can start receiving Iridium pager messages." They also pointed out that the largest user of the Iridium network was the Pentagon.

Satellite hacking has caused enough uproar that former Chief Information Security Officer of NASA, Jeanette Hanna-Ruiz, prioritized cyber attacks as one of the agency's top concerns. "It's a matter of time before someone hacks into something in space. We see ourselves as a very attractive target," she stated in an interview with *Bloomberg*.

Among her key concerns was a rogue agency or a hacker group trying to disrupt communication between NASA and its spacecraft that transmits research data. "There could be a company that wants it, there could be a nation-state that wants it," Hanna-Ruiz said. The challenge, she said, is, "How do I harden these streams and communications flows?" She was clearly worried about a direct cyber attack on a satellite that would allow adversaries to commandeer the controls of the satellites. The apprehension is also among the military. Even though the U.S. Air Force and Missile Systems Center is confident that its own spacecraft are securely encrypted, its major concerns are about the "vulnerability of commercial satellites that host military payloads."

The agencies have also contracted Innoflights, a company that specializes in information security for spacecraft. Innoflights have subcontracted with commercial satellite firm SSL to "develop a high-fidelity simulation environment for testing the security of hosted payloads on commercial satellites," as reported by *Spacenews*.

According to Al Tadros, Vice President of Space Infrastructure and Civil Space at SSL, the project might be a major opportunity for the government to increase the deployment of commercial space technology as well as meeting with the standards of military-level cybersecurity. "The government wants a level of security for payloads that are hosted on commercial satellites. It's a reasonable thing. But it hasn't been developed previously," Tadros said. "Security is one element of resilience, and hosted payloads are part of the solution for increased resilience."

According to experts, the main problem is that space observers often assume that the threat to satellites comes from a direct kinetic attack. But the most probable assault would be through jamming satellite signals. This brings us to the next challenge in space warfare: Global Positioning System (GPS). This technique came to fore after reports emerged that Russia might be testing systems that can interfere with GPS signals by overriding them with fake ones.

It all began on June 22, 2017 when the master of a ship off the Russian port discovered that his GPS had pointed him 25 nautical miles inland near Vnukovo Airport. He reported to the U.S. Coast Guard Navigation Center. When the coast guard contacted other nearby ships, it was found that all their automatic identification system (AIS) pointed to the same location at the Vnukovo Airport, affecting nearly 20 ships traversing the Black Sea.

This was not the first time when GPS spoofing was effectively deployed. In 2013, students of University of Texas sent an $80 million yacht off course by using a custom-built GPS spoofer. The students, with owner's permission, misdirected the yacht by mimicking the GPS signal. "The yacht's on-board navigation system detected the (fake) signal and used it as a triangulation point; no alarms were triggered, and the crew obeyed their computer and changed course," stated a report in *The Verge*.

At present, space may seem like an untouchable realm. But what many fail to understand is that the systems that we have in place are outdated, and that means they are increasingly vulnerable to cyber threats.

Hackers are evolving their methodologies, creating a future in which the possibility of hacking a satellite and crashing into specific targeted locations is a real threat. It's an urban legend that if you drop a penny from the top of The Empire State Building it can kill a person below, but a three-ton satellite crashing down from outer space could become a very real scenario. It would be nothing short of a weapon. For now, that may seem implausible, but there is an impending threat and it needs to be addressed.

FEW MINUTES WITH KEVIN O'LEARY, CMO, GE CHINA