LEVERAGING PROXIMITY:

WHY SPECIAL OPERATIONS FORCES' PHYSICAL PRESENCE IS THE MOST UNDERAPPRECIATED COMPONENT OF THE CYBER-SPACE-SOF TRIAD

By Maj. Dalton Fuss, 18A NATO Special Operations-A

Space and cyber are two of the three elements of the triad that draw the most attention, but the critical role of the last element—special operations forces' (SOF) physical proximity—is commonly overlooked.

An example demonstrating the vital role of physical proximity is reflected in a Russian case study. An exposed intelligence operation conducted by the Russian-speaking espionage organization, Turla Group, provides us with an unclassified example of how SOF can utilize space-based assets to enhance the operational security of cyber operations. This case study demonstrates that a small group of highly-trained personnel can leverage their physical location within a satellite's coverage area to exploit space-based assets. By taking advantage of unencrypted downlinks, Russian operatives were able to translate physical proximity into operational anonymity for a separate intelligence operation that was conducted in cyberspace. We should examine this case study closely to build upon these techniques and maximize the primary value proposition of SOF—the access and placement of perpetually deployed elements.

Photos provided by Adobe Stock

HOW DID THE OPERATION WORK?

Starting in 2007, cyber operatives from Turla Group began exploiting unencrypted downlinks from satellites.[01] The Russian-speaking attackers were operating within the coverage area of a satellite that was providing internet to ground-based computers through an unencrypted downlink. The coverage area, or "footprint," refers to the area on the Earth's surface that a satellite's signal covers.[02] By "listening" to downstream satellite traffic with a rudimentary antenna from within this footprint, the attackers collected metadata on the computers involved.[03] This action provided the attackers with the active IP addresses of those computers relying on the satellite. The attackers reconfigured their own server to mimic these IP addresses and trick the satellite into accepting the hacker's computer as the legitimate user. This process is known as "satlink hijacking."[04]

Critically, the attackers did not access the legitimate user's computer. Instead, they reconfigured their server so that the satellite would perceive it as the legitimate computer, thereby creating a clone that also received the information sent to the legitimate user. When the satellite sent data packets to the legitimate user's IP address, the attackers would also receive that information. After uncovering these active IP addresses within the satellite's footprint, Turla Group then configured their malware to transfer stolen data to these new IP addresses.[05]

HOW THE ATTACKS WORKED:

Attackers operate within the coverage area of a satellite that provides internet to ground-based computers through an unencrypted downlink.

The coverage area, or **"footprint,"** refers to the area on the Earth's surface that a satellite's signal covers.[02]

By **"listening"** to downstream satellite traffic with a rudimentary antenna from within this footprint, the attackers collected metadata on the computers involved.[03]

This action provided the attackers with the active IP addresses of those computers relying on the satellite. The attackers reconfigured their own server to mimic these IP addresses and trick the satellite into accepting the hacker's computer as the legitimate user. This process is known as **"satlink hijacking."** [04]

To spread this modified malware more efficiently, the Russians employed the worm called Agent.BTZ that has historically been used to infect American and European government computers.[06] In previous attacks, the worm quickly propagated across entire networks and exfiltrated information to a separate network, a malicious code known as spyware. Agent.BTZ was "not optimized for stealing data" with precision.[07] The spyware lacked the sophistication required to determine high-value information. To compensate for this shortfall, the malware exfiltrated mass amounts of information for later processing.

This malicious code was designed to clandestinely export data from the target network and then routed through satellites to IP addresses that were employing unencrypted downlinks for internet access—a Wi-Fi café in the Central African Republic, for example.[08] Agent.BTZ commanded the infected computer to send the files to a seldom-used or unopened port on the receiving end, which ensured that the legitimate user's computer did not notify the user of the inbound traffic.[09]

Russian operatives that were in the satellite's footprint, cloned the legitimate user's IP address, so they, too, would receive the stolen data without being detected.[10] To further hide their trail, they often used satellite internet connection providers located in countries like Afghanistan, Lebanon, Libya, Niger, Somalia, and Zambia, which helped hide the location of their command-and-control servers and avoid attribution.[11]

The Russian-speaking espionage organization hoped that no one would discover the malware. But, if the code were uncovered, forensic analysts attempting to reveal the perpetrator would only be able to track it to legitimate users employing satellite-based internet, not the Russian-speaking operatives.

After the operation, investigators obtained a sample of Agent.BTZ from a government computer. Digital forensic analysts at the Moscow-based Kaspersky Labs dissected this malware through dynamic analysis in an isolated environment. Fortunately, because the operatives employed poor tradecraft and reused the same techniques and procedures from previous operations, Kaspersky Labs concluded that Turla Group was responsible for this attack. Analysts recognized programming patterns that were consistent with Turla Group's previous attacks. Even with this information, investigators were unable to identify the exact location of the attacker's servers. All they knew for sure was that the attackers were operating somewhere within the satellite's footprint.

EXPLOITING THE ADVERSARY: WHAT CAN WE STEAL FROM THE RUSSIANS?

Detailed lessons from this operation need to be discussed through classified channels. However, at the unclassified level, it is possible to identify ways to leverage physical proximity to create options for decision-makers and generate dilemmas for adversaries.

EMPHASIZE HOW PHYSICAL PROXIMITY CAN ENHANCE SOF'S ROLE IN THE TRIAD IN COURSES LIKE THE ARMY'S SPACE CADRE BASIC COURSE.

Classified case studies in this course should demonstrate how space assets can support SOF in semi-permissive or denied environments. For example, multidomain operations require SOF to operate in areas where the electromagnetic spectrum is contested and vulnerable. In this environment, space assets can obfuscate the exact location of the SOF element in the same way that the Turla attackers could remain hidden anywhere within a satellite's footprint. In the same way, a SOF unit could receive unencrypted messages from anywhere within a satellite's footprint.

WITHIN ARMY SPECIAL OPERATIONS FORCES, INCREASE THE NUMBER OF BILLETS FOR THE ARMY SPACE CADRE ADDITIONAL SKILL IDENTIFIER.

The Turla Group only has a small number of qualified attackers with the technical skills needed to conduct the attacks described above. SOF must ensure that it has enough qualified personnel to perform these tasks. At a minimum, the special operations community should cultivate proficiency in space operations. Even a rudimentary understanding of orbital mechanics, GPS constellations, and electromagnetic spectrum fundamentals will make SOF personnel more effective by encouraging a more integrated approach to responding to threats. Courses like the Army's Space Cadre Basic Course provide overviews of these technical competencies. Commanders can institutionalize the technical knowledge of space operations within their formations by coding these SOF personnel billets as Space Cadre. This additional skill identifier can be designated at the O-6 (colonel) level in coordination with the Army's Space and Missile Defense Command. While this is a small step to building the required skillset within SOF, this credential will encourage service members to attend the schools needed to perform their assigned roles.

SEND A SPECIAL OPERATIONS EXPERT TO LECTURE AT SPACE AND CYBER PROFESSIONAL MILITARY EDUCATION COURSES TO OUTLINE HOW SOF CONTRIBUTES TO THE TRIAD OPERATIONALLY.

Discussions about the triad frequently center on technical solutions and specialized devices that drive operational outcomes without adequately emphasizing the human dimension. The United States Special Operations Command (USSOCOM) should send lecturers to space and cyber professional military education courses to address this gap. This program would allow SOF personnel to articulate their roles and responsibilities within the triad explicitly. Enhanced comprehension regarding SOF's role in irregular warfare, especially among space and cyber experts, could significantly clarify how their contributions support SOF units in the field.

CONCLUSION

The Russian Turla group leveraged unencrypted satellite communications to obfuscate their location and intercept critical data. This provides a clear example of how physical proximity within a satellite's footprint can be transformed into a tool for anonymity and operational security. This Russian operation also demonstrates the potential for SOF to conduct similar operations with only basic equipment. SOF should replicate this capability of hijacking satellite downlinks with equipment that reduces their digital signature, such as a locally sourced laptop, a portable antenna, and necessary cables. Adopting this approach would necessitate a shift towards greater autonomy and reliance on mission command principles, allowing SOF units to operate independently without direct oversight or constant communication. This strategy would transform geographical location and satellite proximity into operational assets, enhancing the effectiveness of the SOF-Space-Cyber Triad in national security efforts. The strategy would suggest a leaner, more agile operational model that maximizes stealth and minimizes detection risk.

[01] Lucian Constantin. "Turla Cyberespionage Group Exploits Satellite Internet Links for Anonymity: The group routes traffic to their command-and-control servers through hijacked DVB-S Internet connections." PC World. 9 September 2015. (Accessed on 9 February 2024 at https://www.pcworld.com/article/423504/turla-cyberespionage-group- exploits-satellite-internet-links-for-anonymity.html).

[02] Marcin Frackiewicz. "What is the Footprint? Glossary of Satellite Terms." TechnoSpace2. 4 September 2023. (Accessed on 9 February 2024 at https://ts2.com.pl/en/what-is-the-footprint-glossary-of-satellite-terms/).

[03] Mike Lennon. "Russian-Speaking Turla Attackers Hijacking Satellite Internet Links." Security Week: Cybersecurity News, Insights & Analysis. 9 September 2015. (Accessed on 3 February 2024 at

https://www.securityweek.com/russian-speaking-turla-attackers-hijacking-satellite-internet-links/).

[04] Oleg Gorobets. "Satellite Turla: Still Alive and Hiding in the Sky." Kaspersky Daily. 9 September 2015. (Accessed on 3 February 2024 at https://www.kaspersky.com/blog/satellite-turla/15098/).

[05] Kaspersky Labs. "How Turla and "Worst Breach of U.S. Military Computers in History" are Connected ." Kaspersky. 12 March 2014. (Accessed on 12 February 2024 at https://usa.kaspersky.com/about/press-releases/2014_how- turla-and--worst-breach-of-u-s-military-computers-in-history-are-connected).

[06] Mike Lennon. "Russian-Speaking Turla Attackers Hijacking Satellite Internet Links." Security Week: Cybersecurity News, Insights & Analysis. 9 September 2015. (Accessed on 3 February 2024 at https://www.securityweek.com/russian-speaking-turla-attackers-hijacking-satellite-internet-links/). Kim Zetter. "The Return of the Worm That Ate the Pentagon." Wired. 9 December 2011. (Accessed on 12 February 2024 at https://www.wired.com/2011/12/worm-pentagon/).

[07] Jim Finkle. "Agent.BTZ Spyware Hit Europe Hard After U.S. Military Attack: Security Firm." Reuters. 12 March 2014. (Accessed on 12 February 2024 at https://www.reuters.com/article/us-russia-cyberespionage/agent-btz-spyware-hit-europe-hard-after-u-s-military-attack-security-firm-idUSBREA2B25R20140312/).

[08] John Leyden. "State Cyberspies Wriggle Into Satellites For Super-Duper Sneaky Ops." The Register. 9 September 2015. (Accessed on 3 February 2024 at

https://www.theregister.com/2015/09/09/turla_apt_satellite_stealth/#:~:text=A%20Russian-speaking%20cyber- espionage%20group%20which%20exploits%20the%20Turla,global%20satellite%20networks%20as%20part%20of% 20its%20tradecraft).

[09] Stefan Tanase. "Satellite Turla: APT Command and Control in the Sky." SecureList (By Kaspersky). 9 September 2015. (Accessed on 9 February at https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/).

[10] Kim Zetter. "Russian Spy Gang Hijacks Satellite Links to Steal Data." Wired. 9 September 2015. (Accessed on 3 September 2024 at https://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections- to-steal-data/).

[11] Kaspersky Lab. "Turla Hiding in the Sky: Russian Speaking Cyberespionage Group Exploits Satellites to Reach the Ultimate Level of Anonymity." Kaspersky Lab. 9 September 2015. (Accessed on 3 February 2024 at https://media.kaspersky.com/pdf/Kaspersky_Lab_press_release_Satturla_eng_final.pdf).Ullaboritium aborera eperum resciuntius doloreprae et labore peliquia quis quide sus es res es et autemodi alicipiet eturem. Cient.