Anritsu

SIGINT Cyber Security: Importance of Signal Monitoring and Analysis

Application Note

Introduction

The conflict in Ukraine marks a pivotal moment as it unfolds across not only conventional battlegrounds but also within the intricate realms of cyber warfare. This engagement heralds the dawn of a novel era characterized by the convergence of Electronic Warfare (EW), Electronic Attack (EA), Signals Intelligence (SIGINT), and a host of other nascent technologies. This transformative landscape necessitates global military and governmental entities to adapt and evolve, safeguarding armed forces and civilian populations in the face of emerging threats.

In the evolving landscape of contemporary warfare, the battlefield is undergoing a digital and virtual transformation, giving rise to a new form of weaponry – cyber attacks. These cyber-threats transcend the conventional boundaries of IT networks and computers, extending their reach to encompass critical aspects such as machinery control, weaponry, and various battle systems. Comprehensive cyber security measures are paramount to ensure the triumph of missions and safeguard armed forces, naval fleets, military bases, and other strategic installations. These measures are crucial at every echelon – from the micro to the macro. Among these measures, signal monitoring and analysis are pivotal operations that demand immediate attention.

Through these operations, the military can glean critical insights into communication landscapes for early threat detection and safeguarding the environment of legitimate transmissions. Communications between command centers and field troops must be done in near-real-time. Weapons also rely more on radar and advanced signal technologies for mission success. Adversaries will inject signals to cause interference and unreliable connections and/or deliberately transmit misinformation to disrupt and deter such acts.

By adopting a proactive approach through rigorous signal monitoring and analysis, armed forces bolster their capacity to anticipate and counter potential threats. The result is improved operational readiness and fortified defensive prowess.

For the U.S. Department of Defense (DoD), cyber security is a top priority, as cyber attacks are one of the biggest threats to the safety of armed forces and civilians. More than 12,000 cyber incidents against military systems have been recorded by the DoD since 2015 (figure 1). To defend against such offensives, two processes have been implemented by the DoD. One set of procedures is for critical attacks, and the second is for all incidents.

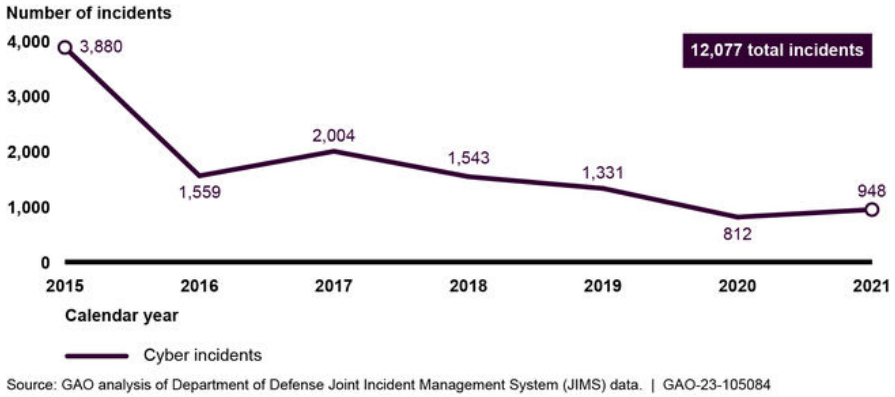

Figure 1: *Over 12,000 cyber incidents related to defense systems have occurred since 2015.*

SIGINT Importance

In this new world, SIGINT has taken on greater importance. It collects and analyzes information on a growing and more diverse network of foreign powers, international terrorists, organizations, and other interest groups. Intelligence agencies globally rely on advanced SIGINT technologies to monitor and intercept digital communications, thwarting attempted attacks by non-state actors. To this end, data acquired using SIGINT is being shared by nations. One example is the Five Eyes Alliance formed by the United States, United Kingdom, Canada, Australia, and New Zealand.

To efficiently collect, analyze, and disseminate data, governmental entities, and military organizations must stay abreast of the rapid developments in today's high-speed, multifunctional technologies. The constant growth in the quantity and diversity of signals adds complexity to generating pertinent and timely intelligence, posing a more significant challenge for military commanders and national policymakers.

Propelled mainly by these endeavors, the worldwide SIGINT market is experiencing expansion. The year 2022 saw approximately $14.09 billion allocated to SIGINT efforts. This expenditure is projected to increase to $14.7 billion in 2023 and is anticipated to further escalate to $17.93 billion by 2027.

Emerging SIGINT Systems

These investments fuel the initiation of many fresh endeavors within SIGINT, introducing cutting-edge concepts such as artificial intelligence (AI) and machine learning (ML). The success of SIGINT no longer solely revolves around the accumulation of vast amounts of data; the swiftness of processing and analysis has taken precedence. In this endeavor, the pivotal roles of AI and ML come to the fore, driving the efficiency of these operations.

Another prominent trajectory within SIGINT pertains to the advancement of encryption techniques. The landscape has never presented a more formidable challenge for intelligence and military agencies in their pursuit of intercepting and decoding communications. Innovations are being engineered, giving birth to new technologies and tools designed to gather, decipher, and meticulously scrutinize transmissions.

Already underway, the integration of sophisticated SIGINT capabilities into military endeavors by the U.S. armed forces is evident. The U.S. Terrestrial Layer System-Brigade Combat Team (TLS-BCT) represents the Army's forthcoming generation of tactical vehicle-based systems. A seamlessly integrated suite of SIGINT, EW, and Cyberspace Operations capabilities defines TLS-BCT, bolstering the prowess of the Joint All Domain Operational (JADO) Capable Force. Initially mounted on Stryker combat vehicles, as depicted in figure 2, TLS-BCT is poised to evolve into an infantry-packable solution, thus amplifying its versatility and impact.

Figure 2: *The U.S. Army TLS-BCT has an integrated suite featuring SIGINT, EW, and Cyberspace Operations. (Photo credit: U.S. Army).*

The U.S. Navy is also making significant strides. The Naval Information Warfare Systems Command (NAVWAR) has initiated the Spectral mission, aimed at swiftly enhancing capabilities for tactical mission operations. Through the Spectral suite encompassing shipboard SIGINT, EW, and information operations (IO), carrier and expeditionary strike groups within the U.S. Navy will attain the ability to gather and utilize SIGINT across an extensive RF spectrum effectively. This suite will facilitate indications and warnings, targeting, ship self-defense, and analogous missions.

Emerging Digital Technologies

Advanced SIGINT used in these systems relies on emerging technologies, such as the Internet of Military Things (IoMT) and the Internet of Battlefield Things (IoBT), as well as cloud computing and 5G. IoMT and IoBT are vital for military success, as they communicate data swiftly. Protecting these digital networks from cyber attacks is critical for missions to be successful, as they are being used as a central hub for emerging warfare tactics.

Equipped with cameras and sensors, unmanned aerial drones have the ability to rapidly and efficiently survey battlegrounds, utilizing IoMT and IoBT technologies to provide enhanced situational awareness on the battlefield. The data collected by these drones is promptly relayed to a central command center, granting mission specialists access to live imagery, terrain tracking, and enemy positioning in real time. This advancement significantly enhances the decision-making process. Further, IoT-based networks can monitor soldier health and facilitate real-time management of equipment and vehicles.

Likewise, IoMT and IoBT technologies enhance the security of military bases and borders, deterring unauthorized access by malicious individuals. By leveraging these technologies, the risk of infiltrators using stolen or forged credentials to breach borders or military installations is significantly reduced. Active and passive IoT sensors play a pivotal role in gathering biometric data such as fingerprints and iris scans. This comprehensive biometric approach accurately identifies individuals who could pose potential threats.

As such, IoMT and IoBT technologies are susceptible to targeting due to the prevalence of IoT networks utilizing edge architectures, which feature numerous connections vulnerable to infiltration and software vulnerabilities. The government is adopting a range of cybersecurity protocols to counter clandestine activities. Spectrum monitoring tools are also employed to safeguard against unauthorized signals that could disrupt crucial transmissions or intercept sensitive communications.

Cloud technology is finding applications across all sectors of defense and government institutions, offering the essential capabilities of processing power, data throughput, and storage capacity. Moreover, it leads to more efficient workflows. One notable illustration is the incorporation of cloud technologies within the Joint All-Domain Command and Control (JADC2) framework, which interlinks sensors, weaponry, and associated communications across every branch of the U.S. military. The integrity of these networks is crucial, necessitating robust resilience and the deployment of cutting-edge cybersecurity measures due to the persistent risk of cyber attacks.

This collaborative approach among academia, the private sector, and the military is crucial, given that numerous technologies are already extensively employed in commercial contexts. Consequently, a multitude of cybersecurity challenges have been thoroughly assessed and resolved through practical, real-world experiences.

Having the capability to observe and manage the virtual battlefield is imperative for the successful execution of military operations and the minimization of casualties. Adversarial forces employ diverse tactics within contemporary SIGINT practices, necessitating countermeasures to ensure the safety of troops and civilians.

Importance of Signal Monitoring and Analysis

Protocols regarding hardware and software, alongside the management of physical access to military installations and command centers, constitute crucial steps – albeit not the sole ones. In the realm of contemporary SIGINT, signal monitoring and analysis hold equal significance, given the incessant efforts of malicious entities to manipulate signal transmissions.

Deploying essential tools and procedures for signal monitoring and analysis establishes a pivotal stratum of cybersecurity. This proactive approach can thwart adversaries from achieving the following objectives:

- **Intercepting Transmissions** – SIGINT commonly intercepts a wide range of electronic communications from an adversary to gather information on deployments, missions, and other military data. The closer the SIGINT system is to the enemy base or other facility, the easier it is to intercept signals due to less signal loss and delay.

- **Signal Jamming** – Radio noise or signals are used to interfere with transmissions intentionally. Jammers radiate interfering signals toward an opponent's radar, blocking the receiver with highly concentrated energy signals. Noise and repeater techniques are commonly used to jam signals.

- **Hidden Communications** – Often, signal jamming relies on lower-level signals "hiding" in larger signals. Hidden signals are also used by armies and terrorist groups to communicate during stealth operations.

Real-time Spectrum Analysis

Effective testing and monitoring systems serve as a countermeasure against increasingly prevalent covert and intentional activities. Furthermore, these systems can also be employed for offensive operations to gather intelligence from adversary transmissions.

A pivotal tool in safeguarding and overseeing the spectrum is a handheld real-time spectrum analyzer (RTSA), which outperforms a vector signal analyzer (VSA) when identifying rogue signals during interference detection. Conventional VSAs gather analog-to-digital converter (ADC) samples over specific intervals, potentially missing critical malicious transmissions while undergoing signal processing. In contrast, an RTSA, such as the Field Master™ Pro series (figure 3), captures and simultaneously analyzes signal data during acquisition, ensuring no signals go unnoticed.

Furthermore, an RTSA excels in uncovering signals attempting to conceal themselves within larger transmissions. It proves highly adept at locating signals with a low probability of interception. Consequently, field operatives can employ an RTSA to monitor frequency hopping utilized in military radios and drones, as well as other missions reliant on short-range directional signals for communication.

Figure 3: *Field Master™ Pro Series – MS2090A, MS2080A, MS2070A*

Advanced Display and Analysis – A power spectral density display shows the relative time that RF power is present at all levels and frequencies within the capture span. A highly effective tool, it allows SIGINT troops to find interfering signals hiding within the same band as known/wanted signals.

IQ Capture and Analysis – IQ capture and streaming enable comprehensive offline processing of IQ data so command officers can gain critical insight into RF signals captured in the field. An RTSA with high capture bandwidth, a large internal memory, or the ability to continuously stream over a high-speed digital interface allows for more efficient post-processing of elusive signals. As a result, hunting and identifying such signals can be done much more effectively.

Pulse Analyzer – Pulse analysis is critical to identify and eliminate nefarious signals before they impact mission success. It is particularly effective in protecting airborne platforms with multiple radars, such as surveillance, target tracking, and threat detection; missile guidance; and for surveillance and threat detection of ship radar.

Remote Spectrum Monitoring

Specialized spectrum monitoring solutions offer continuous and uninterrupted surveillance of signal transmissions around the clock. A spectrum monitoring system, depicted in figure 4, simplifies detecting and eliminating unauthorized or unlicensed interference signals. Through constant spectrum monitoring, problematic signals can be promptly recognized and addressed in real-time as they emerge.

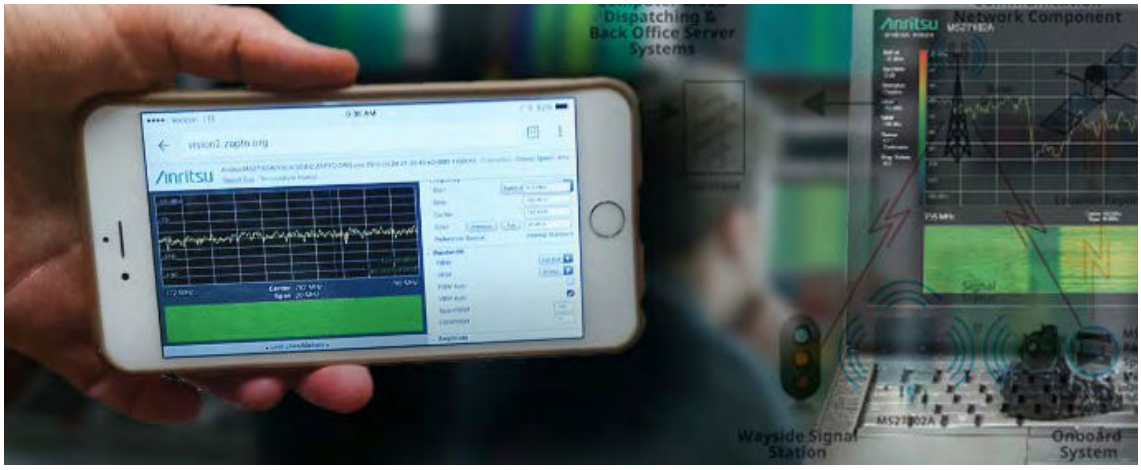

Figure 4: *Spectrum monitoring solutions can locate nefarious signals continuously.*

Undesirable signal patterns can also be analyzed, offering an effective approach to categorizing and pinpointing the origin of interference issues. Consistent and dependable communication is of utmost importance, supporting military endeavors and the testing of advanced systems dependent on wireless command and control. Uninterrupted and distortion-free communication is essential for security at military installations, national borders, and potential high-value sites like power grids and airports. Ensuring unobstructed and clear communication is paramount for the safety and effectiveness of military personnel and civilian populations. Spectrum monitoring plays a pivotal role in achieving this goal.

Conclusion

In the modern landscape of digital warfare, SIGINT emerges as a pivotal weapon that holds the potential to shape the outcome of conflicts and operations. With the intricate interplay of technology and information in today's battlespace, effectively utilizing SIGINT becomes essential for gaining a strategic edge.

To wield this weapon adeptly, the implementation of advanced signal monitoring and analysis tools takes center stage. These tools act as sentinels, vigilantly guarding against unwanted interference and ensuring signal transmissions' security from adversaries' prying eyes. By bolstering the encryption and safeguarding of signals, these tools play a crucial role in preventing unauthorized interception and maintaining the confidentiality of critical communications.

For more information on Anritsu's products, please visit www.anritsu.com or contact the Anritsu sales and support team.

Anritsu
Advancing beyond

Specifications are subject to change without notice.

• **United States**
Anritsu Company
450 Century Pkwy, Suite 109,
Allen, TX, 75013 U.S.A.
Toll Free: 1-800-267-4878
Phone: +1-972-644-1777
Fax: +1-972-671-1877

• **Canada**
Anritsu Electronics Ltd.
700 Silver Seven Road, Suite 120,
Kanata, Ontario K2V 1C3, Canada
Phone: +1-613-591-2003
Fax: +1-613-591-1006

• **Brazil**
Anritsu Electrônica Ltda.
Praça Amadeu Amaral, 27 - 1 Andar
01327-010 - Bela Vista - Sao Paulo - SP - Brazil
Phone: +55-11-3283-2511
Fax: +55-11-3288-6940

• **Mexico**
Anritsu Company, S.A. de C.V.
Av. Ejército Nacional No. 579 Piso 9, Col. Granada
11520 México, D.F., México
Phone: +52-55-1101-2370
Fax: +52-55-5254-3147

• **United Kingdom**
Anritsu EMEA Ltd.
200 Capability Green, Luton, Bedfordshire LU1 3LU, U.K.
Phone: +44-1582-433280
Fax: +44-1582-731303

• **France**
Anritsu S.A.
12 avenue du Québec, Batiment Iris 1-Silic 612,
91140 Villebon-sur-Yvette, France
Phone: +33-1-60-92-15-50
Fax: +33-1-64-46-10-65

• **Germany**
Anritsu GmbH
Nemetschek Haus, Konrad-Zuse-Platz 1
81829 München, Germany
Phone: +49-89-442308-0
Fax: +49-89-442308-55

• **Italy**
Anritsu S.r.l.
Via Elio Vittorini 129, 00144 Roma Italy
Phone: +39-06-509-9711
Fax: +39-06-502-2425

• **Sweden**
Anritsu AB
Kistagången 20B, 164 40 KISTA, Sweden
Phone: +46-8-534-707-00
Fax: +46-8-534-707-30

• **Finland**
Anritsu AB
Teknobulevardi 3-5, FI-01530 VANTAA, Finland
Phone: +358-20-741-8100
Fax: +358-20-741-8111

• **Denmark**
Anritsu A/S
Kay Fiskers Plads 9, 2300 Copenhagen S, Denmark
Phone: +45-7211-2200
Fax: +45-7211-2210

• **Russia**
Anritsu EMEA Ltd.
Representation Office in Russia
Tverskaya str. 16/2, bld. 1, 7th floor.
Moscow, 125009, Russia
Phone: +7-495-363-1694
Fax: +7-495-935-8962

• **Spain**
Anritsu EMEA Ltd.
Representation Office in Spain
Edificio Cuzco IV, Po. de la Castellana, 141, Pta. 5
28046, Madrid, Spain
Phone: +34-915-726-761
Fax: +34-915-726-621

• **United Arab Emirates**
Anritsu EMEA Ltd.
Dubai Liaison Office
P O Box 500413 - Dubai Internet City
Al Thuraya Building, Tower 1, Suite 701, 7th floor
Dubai, United Arab Emirates
Phone: +971-4-3670352
Fax: +971-4-3688460

• **India**
Anritsu India Pvt Ltd.
2nd & 3rd Floor, #837/1, Binnamangla 1st Stage,
Indiranagar, 100ft Road, Bangalore - 560038, India
Phone: +91-80-4058-1300
Fax: +91-80-4058-1301

• **Singapore**
Anritsu Pte. Ltd.
11 Chang Charn Road, #04-01, Shriro House
Singapore 159640
Phone: +65-6282-2400
Fax: +65-6282-2533

• **P. R. China (Shanghai)**
Anritsu (China) Co., Ltd.
27th Floor, Tower A,
New Caohejing International Business Center
No. 391 Gui Ping Road Shanghai, Xu Hui Di District,
Shanghai 200233, P.R. China
Phone: +86-21-6237-0898
Fax: +86-21-6237-0899

• **P. R. China (Hong Kong)**
Anritsu Company Ltd.
Unit 1006-7, 10/F., Greenfield Tower, Concordia Plaza,
No. 1 Science Museum Road, Tsim Sha Tsui East,
Kowloon, Hong Kong, P. R. China
Phone: +852-2301-4980
Fax: +852-2301-3545

• **Japan**
Anritsu Corporation
8-5, Tamura-cho, Atsugi-shi,
Kanagawa, 243-0016 Japan
Phone: +81-46-296-6509
Fax: +81-46-225-8359

• **Korea**
Anritsu Corporation, Ltd.
5FL, 235 Pangyoyeok-ro, Bundang-gu, Seongnam-si,
Gyeonggi-do, 13494 Korea
Phone: +82-31-696-7750
Fax: +82-31-696-7751

• **Australia**
Anritsu Pty Ltd.
Unit 20, 21-35 Ricketts Road,
Mount Waverley, Victoria 3149, Australia
Phone: +61-3-9558-8177
Fax: +61-3-9558-8255

• **Taiwan**
Anritsu Company Inc.
7F, No. 316, Sec. 1, Neihu Rd., Taipei 114, Taiwan
Phone: +886-2-8751-1816
Fax: +886-2-8751-1817

10-2023 SIGINT Cyber Security: Importance of Signal Monitoring and Analysis