Annealed Cyber Resiliency

Cyber Discernment for the Launch Providers of Space Systems

Steve Chan
Decision Engineering Analysis Laboratory
San Diego, California
email: schan@dengineering.org

Bob Griffin
Tucson, Arizona
email: bobgriffin@me.com

***Abstract*—Out-of-the-box and outside-the-wire thinking is required to identify sophisticated synthetic aberrations, which would bypass prototypical cyber defense systems. The various tools and techniques are somewhat important within the ecosystem, but an assessment methodology that embodies diligence, persistence, and learning over time can be even more vital than the various tools and techniques. This paper posits that the depth and breadth of any cyber investigation foray can well be achieved by employing an approach that is termed Cyber Discernment. In Cyber Discernment, a methodological robust decision engineering framework, Karassian Netchain Analysis (KNA), among others, is utilized to understand Negative Influence Dominating Sets (NIDS) or areas of instability and Positive Influence Dominating Sets (PIDS) or islands of stability. By ascertaining PIDS and understanding how best to mitigate NIDS, a form of *annealed cyber resiliency, enhanced cyber security,* and *latent cyber stability* can be achieved, thereby mitigating against unintended consequences, undesired elements of instability, and "perfect storm" crises lurking within the system.**

Keywords-space systems; strategic infrastructure; critical infrastructure; advanced persistent threats; outside-the-wire.

I. INTRODUCTION

Generally speaking, systems residing within the "space" ecosystem constitute attractive "persistent targets" (for "Advanced Persistent Threats (APTs)" due to their serving as an "Achilles heel" or central point of failure for large-scale systems, their potential lack of stringently enforced cyber security regulation, and their relatively large and pervasive attack surface area. Considering that much of the world's strategic infrastructural and critical infrastructural systems rely upon space-based systems, it would seem axiomatic the attacks would be channeled in this direction. Technically, space systems do not require substantively different cyber security systems from that of other strategic and/or critical infrastructure; however, as these space systems often serve as underlying infrastructure for other strategic and/or critical infrastructural systems (hence, "outside-the-wire," which is military jargon for being beyond the relatively safe confines of a controlled environment), they are not necessarily construed to be intrinsic to the referenced strategic and/or critical infrastructural systems and, therefore, are not necessarily subject to the same cyber security standards.

Typically, space systems are relatively sophisticated pieces of equipment (e.g., hardening, compute capabilities, communications packages, etc.). Despite the involved sophisticated technology, cybersecurity standards for space system assets are not necessarily strictly regulated by any governing body; the relative lack of regulation segues to an arena, wherein space systems may lack common cybersecurity standards and may be subject to a myriad of cyberattacks. This is distinct from other domains, such as Industrial Control Systems (ICS), which are regulated by the Federal Energy Regulatory Commission (FERC) and subject to, on a voluntary basis, the electric utility industry's North American Electric Reliability Corporation (NERC), which is the successor to the North American Electric Reliability Council (also known as NERC). The United Nations International Telecommunication Union (ITU) regulates the assigned frequencies for satellite communications and registers the orbits of satellites, but apart from this aspect, there are relatively few standards at play, and cyber vulnerabilities remain a challenge [1].

While the seemingly lack of standards for such sophisticated systems is already of great concern, the recent trend of low-cost satellites — utilizing commercial-off-the-shelf (COTS) technology — being launched into orbit may be of even greater concern. These "cubesats" have a fairly low barrier to entry with regards to engineering from a technical standpoint and are relatively inexpensive to launch (less than $100K). Considering the COTS nature of the satellite, it is likely that open-source software (OSS) is used prevalently by the components with the concomitant associated vulnerabilities. As has been debated over time [2], there are advantages and disadvantages to OSS. First, the wide distribution of COTS products and its associated OSS means that many people have access to the code base, and an attacker can extensively analyze the paradigm for vulnerabilities. Second, COTS products and its associated OSS need to be actively maintained, patched, and upgraded, particularly as cyber attackers are becoming increasingly adept. Just as Managed Service Providers (MSPs) and Managed [Cyber] Security Service Providers (MSSPs) are leveraging early warning indicators, such as the National Vulnerability Database (NVD) and Sentient Hyper Optimized Data Access Network (SHODAN), cyber attackers are also leveraging these assets for exploitation opportunities and as attack accelerants [3]; security patches are often not applied, and software vulnerabilities or backdoors (which may have been intentionally embedded) persist.

While the National Institute of Standards and Technology (NIST) Cybersecurity Framework is well-documented and

 ISBN: 978-1-61208-743-6

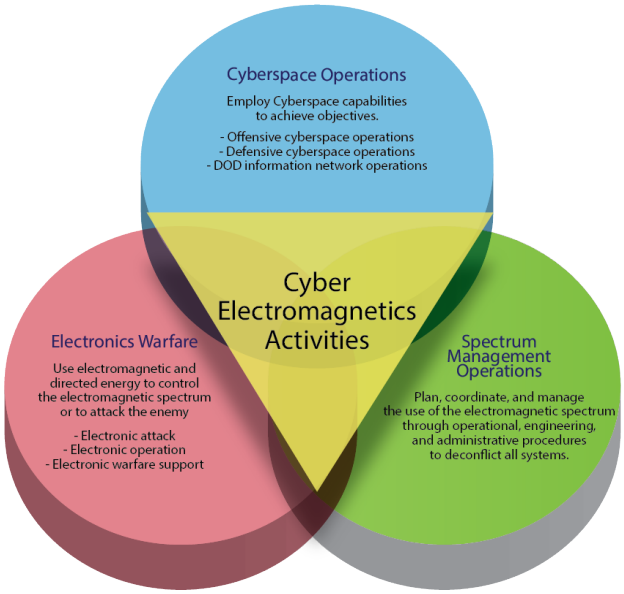
widely adopted on a voluntary basis, currently, there is no mandatory reporting, via the Code of Federal Regulations for the Department of Defense-Defense Industrial Base Cybersecurity Activities (32 CFR Part 236). In other words, there is no mandatory reporting of cyber incidents by space systems organizations, which are responsible for space systems that enable other strategic and/or critical infrastructures.

Section I provided an introduction to the paper. Section II presents the criticality of time synchronization for event correlation. Section III delineates the cyber risks and responsibilities within an exemplar satellite launch project. Section IV posits a robust decision engineering framework for addressing cyber in a defense-in-depth fashion. Section V summarizes the paper and alludes to future work.

II. THE CRITICALITY OF TIME SYNCHRONIZATION FOR EVENT CORRELATION

Among the various cyber-attack vectors, the criticality of Assured, Position, Navigation, and Timing is affirmed by the legislative direction of the National Defense Authorization Act for Fiscal Year 2019. In essence, it recognizes that "strategic high-end competitors possess the capability to disrupt systems that depend on [Global Positioning System] GPS which could pose an unacceptable level of risk … in GPS-denied environments." Accordingly, a paradigm of "cyber-robust[ness]" is being emphasized by the U.S. Army's Program Executive Office, Missiles and Space to "counter emerging threats."

At the core of the GPS issue is the fact that GPS-based clocks have become foundational to critical infrastructural systems (some are construed as mission-critical strategic infrastructural systems). Yet, despite this criticality, GPS-based clocks are susceptible to a variety of issues and represent a potential cyber "Achilles heel" for the modern-day mission-critical strategic infrastructural and critical infrastructural systems. Along this vein, the term of art "cyber," particularly within the context of the discussed case of the GPS-based clock, should be more clearly delineated. Among a variety of sources, the U.S. Army Cyber Warfare Field Manual (FM) 3-38 [4], "Cyber Electromagnetic Activities" (supplanted by FM 3-12 "Cyberspace and Electronic Warfare") contends that "Cyber Electromagnetic Activities" encompass not only conventional cyber activities (e.g. Distributed Denial-of-Service or DDoS attack, which is an attack by which multiple compromised computer systems attack a targeted resource, such as a GPS-based clock. The torrent of incoming messages, connection requests force the targeted resource to slow down or shut down, thereby denying service for legitimate use), but also activities involving electronic warfare (e.g., GPS jamming, GPS spoofing, etc.) and spectrum management operations. Professor Todd Humphreys at the University of Texas, Austin demonstrated in 2012 that a software-defined small-scale spoof attack might be quite inexpensive to build and execute [5], and the U.S. Maritime Administration noted in 2017 that a large-scale spoof attack occurred in the Black Sea (a body of water and marginal sea of the Atlantic Ocean between the Balkans, Eastern Europe, the Caucasus, and Western Asia) against 20 ships [6]. Spectrum management operations refers to the management of the spectrum. By way of example, the U.S. spectrum is managed by the Federal Communications Commission (FCC) for non-governmental applications as well as by the National Telecommunications and Information Administration (NTIA) for governmental applications. Spectrum management is a burgeoning problem due to the growing number of spectrums uses, such as over-the-air broadcasting, government and research uses (e.g. defense, public safety), commercial services to the public (e.g. wireless broadband), and industrial, scientific, as well as medical services. This is delineated in Figure 1 below.



Source: FM 3-38, p 1-2.

Figure 1. Cyber Electromagnetic Vulnerabilities

As can be seen by way of various vulnerability databases (e.g. NVD), such as that produced by the National Cybersecurity and Communications Integration Center (NCCIC) Cyber Emergency Response Team (ICS-CERT), there exists several GPS clock vulnerabilities that can affect the accuracy of the clock. This is unacceptable as correct correlation of data (i.e. event correlation) [7] to time (i.e., accurate timestamping) [8] is needed to establish a meaningful baseline against which anomalies can be detected. To rearticulate this matter, by way of example, logs are predicated upon timestamps, as can be seen in Figure 2. If these timestamps are manipulated, then the sequencing of the log entries would be incorrect; any subsequent utilization of detection methodologies [9][10] for forensic investigation would be greatly inhibited.

 ISBN: 978-1-61208-743-6

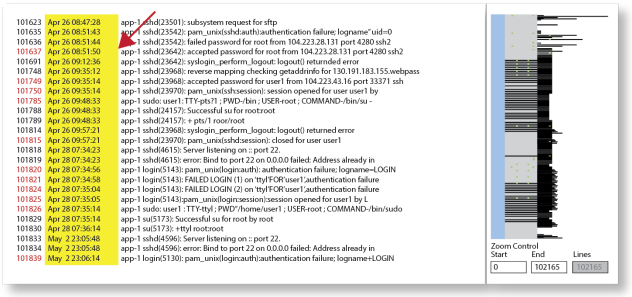


Figure 2. Exemplar Log for Forensic Investigation

There have been a variety of attacks against space systems, and interestingly, the attackers' interest has not necessarily focused upon the space system itself, but rather upon the technology, which was enabled by the space system. For example, Kaspersky Labs discovered that Turla, a Russia-based cyber-espionage group, had compromised a satellite internet provider and obfuscated their ensuing cyber-espionage operations against countries ranging from the U.S. to various former Eastern Bloc countries [11]. By using a ground antenna, Turla could detect Internet Protocol (IP) addresses from satellite internet users and proceed to initiate a Transmission Control Protocol/Internet Protocol (TCP/IP) connection from the compromised IP address. This type of attack is not easily discernable, as it does not perceivably impact a satellite internet user's performance (which depends upon whether the attacker and legitimate satellite internet users are using the IP address concurrently), and it is unlikely to be flagged by conventional intrusion detection systems (IDS).

III. CYBER SECURITY RISKS AND RESPONSIBILITIES WITHIN AN EXEMPLAR SATELLITE PROJECT

Unfortunately, the expanding ecosystem of cyber electromagnetic spectrum cyber vulnerabilities presents a dilemma for those involved in satellite projects. Satellite projects were technologically challenging enough from just a capabilities perspective (e.g., Ka-band systems are susceptible to weather due to signal absorption by moisture in the air and by wetness on antenna surfaces [12], [13]), but the spectrum of cyber-attack pathways given the growing complexity of systems [14] and the vulnerability to cyber manipulation [15] greatly exacerbate the situation.

As an exemplar, the Iridium satellite constellation provides L-band voice and data coverage to integrated receivers, satellite phones, and pagers. Originally, the Iridium satellite owners had asserted that "the complexity of the Iridium air interface makes the challenge of developing an Iridium L-Band monitoring device very difficult and probably beyond the reach of all but the most determined adversaries." However, at the Chaos Communication Camp, held in Zehdenick, Germany during August 2015, the conference organizers distributed 4,500 software-defined rad1o badges (a.k.a. HackRF), which were sensitive enough to intercept satellite traffic from the Iridium communications network (Iridium pager traffic is, by default, sent in cleartext, and most pager traffic remains unencrypted). Other vulnerabilities, such as in the firmware (digital "backdoors" embedded within the computer code as well as "hardcoded credentials") have been cited in reports related to satellite communications (SATCOM) security.

However, similar to other industries (e.g. automotive industry, ICS industry), space technology designers, manufacturers, and industry providers have progressed slowly in their efforts toward enhancing cyber security. Perhaps, it is due to the distributed responsibility. By way of example, as is delineated in Figure 3 below, A may commission the development of a satellite with B, which then assumes the cybersecurity responsibility of the satellite. B then outsources the satellite development to (and/or sources components from) to C and D, who each maintain their own cybersecurity responsibility for their respective components. When B completes the development of the satellite and delivers it to A, E is contracted to manage the operations of the satellite; at this point, E assumes cybersecurity responsibility for the satellite. Then, E commissions F to launch the satellite into space; at this point, F assumes cybersecurity responsibility during the launch process. The liability for this cybersecurity responsibility is often displaced to G, an insurance underwriter. Once the satellite is in orbit and is operational, E resumes cybersecurity responsibility for the operations of the satellite. Oftentimes, A will want to maximize profitability and will proceed to lease bandwidth and/or the processing capability of the satellite to other companies, such as H and I. Depending upon the usage (e.g. ICS), H and I will now have cyber liability as well. Due to the complex ecosystem of owner, developer, operator, and user cybersecurity responsibilities, there are a myriad of attack vectors along the cyber-physical supply chain.

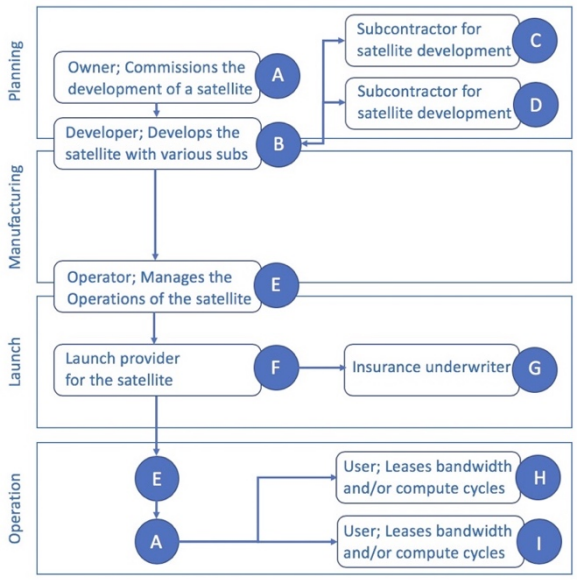


Figure 3. Cybersecurity Responsibilities for an Exemplar Satellite Project [16]

From a certain vantage point, the cyber rationale might seem quite robust given the seemingly "logical" delineation of responsibilities, but given the lesson learned from the NASA Space Shuttle Challenger (Orbiter Vehicle or OV-99) explosion in 1986, metaphorically, all it takes is one "O-Ring" (the primary and secondary O-rings, which were designed to prevent a leakage of hot gases were incapable of properly sealing the gaps between the Solid Rocket Booster (SRB) joints in extremely cold weather) for catastrophic (in this case, cyber) failure of the system as a whole.

A. Cyber-Physical Supply Chain Issues at Boeing and Elsewhere

As demonstrated by the July 2007 unveiling of Boeing's Dreamliner or Boeing 787 (a.k.a. "B787"), supply chain structures are becoming increasingly multi-layered and complex. Along this vein, for the first time in its history, Boeing (the world's largest aerospace company) outsourced its engineering of — and integration for — its aircraft parts. In it of itself, this particular fact may not raise any eyebrows until it is realized that more than 90% of the Dreamliner program was outsourced to a variety of supply chain partners across the globe [17]. Interestingly, for these partners to participate in the Dreamliner program, they were obligated to finance and oversee the development of — and assimilation for — the assigned outsourced specific part based upon very granular technical specifications provided by Boeing.

While Boeing did indeed reduce its own upfront developmental costs, and its Vice President for Global Supply Partners, Steven Schaffer, was feted as the "Supply Chain Manager of the Year" in 2007 by *Purchasing Magazine*, the back-story, according to Stan Sorscher, Legislative Director at the Society for Professional Engineering Employees in Aerospace (SPEEA) (a union representing over 20,000 scientists, engineers, technical and professional employees within the aerospace industry), was that Boeing was shocked when it was confronted by a rather opaque supply chain and realized that it no longer had a crystal-clear vantage point as to what went into the detailed designs of its own aircraft sections. After all, since the suppliers spent their own funds to design and develop the various assigned parts, they also, naturally, retained these precious designs as intellectual property. Also, because Boeing had selected, principally, those suppliers, who had the financial wherewithal to both proffer the initial capital expenditure (for the specialized research and development of the specific part), as well as instantiate the cash flow necessary to accommodate the need for Boeing to sell an aircraft before the supplier received any payment, it turned out that the performance metric of technical capability of the supplier came, for the most part, second to the performance metric of financial capacity. Therefore, from a product development vantage point, numerous Boeing suppliers may have been sub-optimally selected, and in turn, these financially minded subcontractors outsourced a myriad of tasks to a further network of, potentially, lowest bid sub-suppliers. Suffice it to say, not all the actors within this intricate sub-supplier fabric were commensurate with Boeing's high standards for excellence, and an exemplar of a quality assurance/quality control (QA/QC) issue includes the Federal Aviation Administration (FAA) asserting, in January 2011, that the code written by an Indian software company, HCL Technologies, for the Dreamliner's electrical systems, was so low in quality that it had to be redone [18]. Other commensurate situations include aircraft parts — being delivered to Boeing — that were simply unfinished. These shocking citations merely depict the proverbial tip of the iceberg as to what can go awry when transparency in the cyber-physical supply chain does not run deep; this further begets the question of how the cybersecurity protocols fared, if even the contracted core competencies were in disarray.

In a similar fashion, the re-use, modification of open-source software (OSS) code published by the National Aeronautics and Space Administration (NASA) and other space agencies have, over time, segued to "commercial offerings," via wrappers around the OSS; this has muddied the waters of the cyber-physical supply chain with regards to its provenance and overall transparency. By way of example, sometimes, commercial solutions may quickly advance to the forefront, but in some cases, many are overtaken by various OSS projects. Among various reasons, innovation, particularly as pertains to the commercial offerings, may decrease after the product reaches a certain level of maturity. In several other cases, the more successful commercial solutions are comprised of either the original or variants of OSS projects. Accordingly, it is becoming increasingly complex to distinguish what was originally "proprietary" and what is a derivative work product. In either case, cybersecurity vulnerabilities abound and need to be addressed.

B. Cyber Issues at NASA and Elsewhere

In Fiscal Year (FY) 2015, an audit at NASA revealed the need for a revamping of cybersecurity standards and protocols. The audit cited several attacks on NASA space assets, which were not publicly disclosed [19]. Previously, the Office of the Chief Information Officer (OCIO) was responsible for cybersecurity across all of NASA. However, OCIO teams could not fully contend with both the infrastructural security of NASA's various laboratories as well as the various attack vectors of its complex mission systems (let alone the emergent threats of the cyber electromagnetic spectrum). To contend with these issues, NASA's Jet Propulsion Laboratory (JPL) instantiated the Cyber Defense Engineering and Research Group (CDER), whose goal is to specifically to address mission systems, which may have unique cybersecurity requirements; in June 2019, a report published by the NASA Office of the Inspector General (OIG) revealed that in April 2018, attackers had breached NASA's network and exfiltrated approximately 500MB of data related to its Mars missions [20].

 ISBN: 978-1-61208-743-6

IV. ROBUST DECISION ENGINEERING FRAMEWORK FOR CYBER SECURITY

One mitigating cyber framework centers upon a [Big Compute] approach, as it is a blend of complexity science, cyber-physical supply chain science, network science, and decision engineering — "Cyber Discernment." Cyber Discernment shows promise, as it works for a fairly straightforward reason: it embodies the characteristics of how the world actually works. To analyze complex real-world relationships, the utilized methodological framework — "karassian netchain analysis" (KNA) — is utilized [21]. This framework differs from traditional netchain analysis (network and supply chain analysis) in three critical ways: (1) it adequately considers the network of dotted-line relationships that are not codified elsewhere; (2) it expands the observational space to include the interactions among heterogeneous actors within a given "horizontal" layer of a supply chain; and (3) it captures the latent potential for actors within the horizontal and/or vertical layers to deviate significantly from the average behavior, which may have ensuing dramatic effects. Furthermore, through KNA, it is possible to identify specific local community structures within the cyber-physical supply chain, via discernible "shapes" (i.e. morphology) that correspond to specific conditions and/or adaptations amidst various pressure sensitivities. The identification of these morphological motifs are crucial for mitigating against exfiltration, such as of the Mars mission data previously delineated.

While the social and physical sciences have traditionally tackled problems by breaking them into constituent parts and simplifying interactions between them, it is now clear within the context of the Challenger explosion that for the arena of space systems, the emergent patterns that beget predictions will appear only when problems are considered in their full complexity and local context. This approach vector will better illuminate cyber-physical supply chains and pertinent local community structures that must be: (1) orchestrated to achieve *annealed cyber resiliency*, (2) leveraged to secure pathways for *enhanced cyber security*, and (3) amalgamated to serve as the backbone of *latent cyber stability*.

The concept of "islands of stability," such as for KNA, is exemplified by the "sandpile effect" (more formally, the Bak-Tang-Wiesenfield sandpile model of non-equilibrium systems [22]) in which sand is dropped, one grain at a time, onto the same spot on a flat surface, until the addition of one more grain of sand causes an avalanche to slide down the slopes of the growing sandpile. In 1987, physicists Per Bak, Chao Tang, and Kurt Wiesenfield investigated the "sandpile effect" by using a computer to color the sandpile according to steepness—the steepest regions of the pile were colored in red, and the flattest, green; they discovered that a single grain of sand falling onto a red region would instigate an avalanche, which not only caused certain green regions to become red, but also compounded into a cascading series of avalanches that grew in size and intensity as it disturbed other red regions (i.e. cascading failure). Restated in terms of KNA, instability (e.g. a compromised component, such as an "O-ring") can spread throughout the entire network, via islands of potentially unstable nodes; these small sets of nodes with the power to influence the entire network are known as *Influence Dominating Sets (IDS)*. Just as a sandpile avalanche can create instability in previously stable areas, real-world phenomena (e.g. a compromised sub-system) can originate at just a few nodes (an occurrence of IDS) and eventually permeate an entire large-scale system. Identifying Negative Influence Dominating Sets (NIDS) in a given network requires a detailed knowledge and sophisticated analysis of the involved network so as to uncover the harbingers of instability and "perfect storm" crises lurking within a network, and, on the positive side, to identify opportunities to infuse *latent cyber stability, enhanced cyber security,* and *cyber resiliency* throughout the network by cultivating and/or influencing PIDS. One goal is to understand fundamental patterns and constraints that arise from those interactions, based upon the preliminary hypothesis that successful, sustainable coordination arises most readily out of PIDS, which can anneal a system and reduce brittleness.

A. *Utilization of Artificial Intelligence for Cyber Diagnosis within a System*

Without having conducted an interview or on-site investigation, it is difficult to assert what cyber paradigm should be implemented. However, the utilization of an apropos Artificial Intelligence (AI) paradigm, such as via a Convolutional Neural Network (CANN), for a preliminary diagnosis within a system has been successfully utilized, within a cyber context, to provide certain insights (particularly those at machine speed). An exemplar CANN is shown in Figure 4 below.

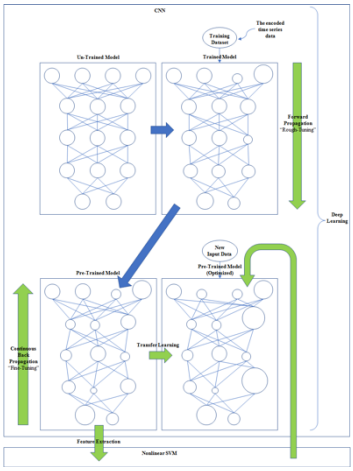


Figure 4. Hybrid Model involving various CNNs and a Nonlinear SVM, which segue to a [Deep Learning] Convolutional [Generative] Adversarial Neural Network (CANN) Paradigm to provide certain cyber insights (particularly those at machine speed) [23].

B. *Exemplar Posited Hybridized Solution Stack for Cyber*

Generally speaking, variants of an apropos AI CANN operating atop a hybridized solution stack to address cyber in a defense-in-depth fashion have successfully provided certain insights into the degree of cyber uncertainty and/or ambiguity

 ISBN: 978-1-61208-743-6

in the system. An exemplar hybridized solution stack in shown in Figure 5 below.

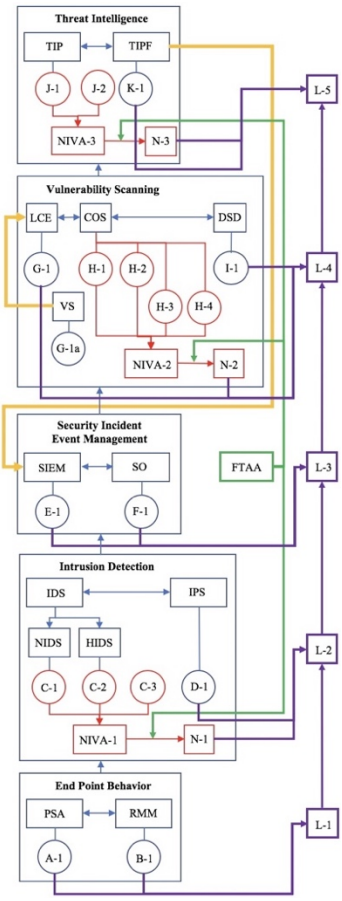


Figure 5. Hybridized Cyber Stability/Security/Resiliency Solution Stack to provide certain insights into the degree of cyber uncertainty and/or ambiguity in the ecosystem [24].

As can be seen in Fig. 5, there are groupings at different levels: (1) End Point Behavior Monitoring (EPBM) (comprised of Professional Services Automation [PSA] and Remote Monitoring and Management [RMM] tools); (2) Intrusion Detection Systems (IDS) (comprised of Network Intrusion Detection Systems [NIDS] and Host Intrusion Detection Systems [HIDs]), as well as Intrusion Prevention Systems (IPSs); (3) Security Information and Event Management (SIEM) and Security Orchestration (SO); (4) Vulnerability Scanning (VS) (comprised of a Log [Analysis] and Correlation Engine [LCE] as a Monitoring Strategy, Container-Orchestration System [COS], and Dynamic Service Discovery [DSD]); and (5) Threat Intelligence (TI) (comprised of Threat Intelligence Platforms [TIPs] and a Threat Intelligence Processing Framework [TIPF]). Each set of groupings pass their outputs to a N-Input Voting Algorithm (NIVA), which acts in concert with a Fault Tolerant Averaging Algorithm (FTAA), via ensemble method Machine Learning (ML). For Intrusion Detection, C-1, C-2, and C-3 passed their outputs to NIVA-1, whose output was refined by FTAA and the resultant was N-1 (red pathway). For VS, H-1, H-2, H-3, and H-4 passed their outputs to NIVA-2, whose output was refined by FTAA and the resultant was N-2 (red pathway). For TI, J-1 and J-2 passed their outputs to NIVA-3, whose output was refined by FTAA and the resultant was N-3 (red pathway). The FTAA refinement pathways are illuminated (green pathway). The various interim steps were as follows: (A-1)&(B-1)->(L-1), (N-1)&(D-1)->(L-2), (E-1)&(F-1)->(L-3), (G-1)&(N-2)&(I-1)->(L-4), and (K-1)&(N-3)->(L-5). Each layer of the solution stack passed its output to the layer above; hence, EPBM (L-1) -> IDS (L-2) -> SIEM (L-3) -> VS (L-4) -> TI (L-5) (purple pathway). Of course, the TIPF fed its output back to the SIEM, and the VS repertoire fed its output to the LCE (orange pathway).

C. *Assessment Methodology*

The learnings behind Figure 4 were that certain cyber insights (particularly those at machine speed) are necessary to understand the IDS described for KNA. The learnings behind Figure 5 were that certain cyber insights (particularly to identify the degree of uncertainty and/or ambiguity at each level in the ecosystem) are also necessary to contextualize the PIDS and NIDS as part of KNA.

The various tools and techniques are somewhat important within the ecosystem, but an assessment methodology that embodies diligence, persistence, and learning over time can be even more vital than the various tools and techniques. Figure 6 shows a common motif to intentional skewing of timestamping so as to adversely impact the timestamping (in this case, GPS-based timestamping paradigm for the Phasor Measurement Units [PMUs] of an ICS ecosystem was affected) paradigm for pertinent logs. It is emblematic of the outside-the-wire and out-of-the-box thinking required to identify sophisticated synthetic aberrations, which would bypass prototypical cyber defense systems.

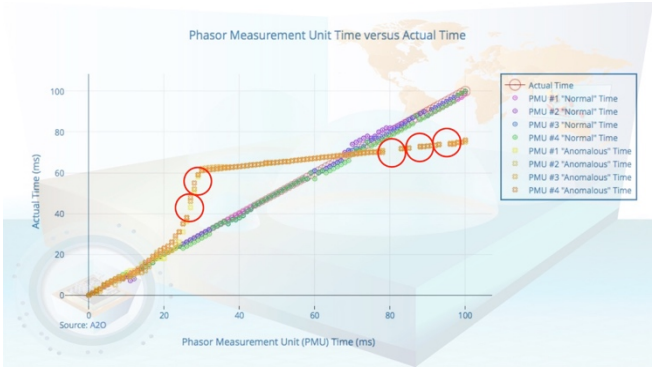


Figure 6. The Diligence and Persistence of Baselining Data over Time so as to identify Aberrations within the Timestamping Paradigm.

V. CONCLUSION

The public has already raised the specter of cybersecurity to space technology designers, manufacturers, and providers, such as SpaceX [25]. The dialectic is growing with intensity. As can be gleaned from the Boeing case study, there is a dilemma with

regards to driving down production costs amidst the ever-increasing complexity of the cyber-physical supply chain; global supply chains exacerbate this dilemma. From our longitudinal research within this arena, we posit that the depth and breadth of any cyber investigation foray can well be achieved by employing an approach that we term Cyber Discernment. In Cyber Discernment, a methodological robust decision engineering framework, karassian netchain analysis (KNA), among others, is utilized to understand Negative Influence Dominating Sets (NIDS) or areas of instability and Positive Influence Dominating Sets (PIDS) or islands of stability. By understanding both heuristics and algorithmics for cyber at machine speed and ascertaining PIDS as well as understanding how best to mitigate NIDS, a form of *annealed cyber resiliency, enhanced cyber security,* and *latent cyber stability* can be achieved, thereby mitigating against unintended consequences, undesired elements of instability, and "perfect storm" crises lurking within the system. Future work will provide further anonymized case studies beyond those presented thus far.

ACKNOWLEDGMENT

The authors would like to thank I. Oktavianti and O. Prafito for their invaluable assistance with completing this paper. Without their ongoing assistance, the production of this paper would have been delayed. The authors would also like to thank the Decision Engineering Analysis Laboratory for the support in completing the requirements for this paper.

REFERENCES

[1] S. Chan, Chapter 5, "Measuring the Information Society, 150th Anniversary Edition" United Nations International Telecommunication Union (ITU), pp. 147-185, 2015.

[2] R. Spousta and S. Chan "Milk or Wine: Are Critical Infrastructure Protection Architectures Improving with Age?" Journal of Challenges, vol. 2, no. 1, pp. 1-13, 2015.

[3] S. Chan, "Prototype Orchestration Framework as a High Exposure Dimension Cyber Defense Accelerant Amidst Ever-Increasing Cycles of Adaptation by Attackers: A Modified Deep Belief Network Accelerated by a Stacked Generative Adversarial Network for Enhanced Event Correlation," The Third International Conference on Cyber-Technologies and Cyber-Systems, pp. 28-38, 2018.

[4] "U.S. Army Cyber Warfare Field Manual (FM) 3-38," *Department of the Army*, February 2014.

[5] "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea," UT News, The University of Texas at Austin, July 2013.

[6] Maritime Administration (MARAD), "2017-005A-GPS Interference-Black Sea," U.S. Department of Transportation. 2017.

[7] S. Chan, "Quality Assurance/Quality Control Engine for Power Outage Mitigation: The Challenge of Event Correlation for a Smart Grid Architecture Amidst Data Quality Issues," Advances in Intelligent Systems and Computing.

[8] S. Chan, "A Potential Cascading Succession of Cyber Electromagnetic Achilles' Heels in the Power Grid: The Challenge of Time Synchronization for Power System Disturbance Monitoring Equipment in a Smart Grid Amidst Cyber Electromagnetic Vulnerabilities," Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), vol. 2, pp. 912-935, 2019.

[9] R. Spousta and S. Chan, "Electrical Islanding Detection based on the Integration of Synchronized Phasor Measurements," IEEE Future Technologies Conference (FTC) 2016, pp. 68–73, December 2016.

[10] S. Chan, "Methods and Apparatus for Detecting and Correcting Instabilities within a Power Distribution System," U.S. Patent Trademark Office (PTO), August 2016.

[11] Kaspersky's Global Research and Analysis Team (GReAT), "The Epic Turla Operation," SecureList, August 2014.

[12] S. Sala, et al., "Mitigation of Rain-Induced Ka-Band Attenuation and Enhancement of Communications Resiliency in Sub-Saharan Africa," Proceedings Annual Workshop of the AIS Special Interest Group for ICT in Global Development, December 2013.

[13] R. Spousta, S. Chan, and B. Griffin, "Space 2.0: Expanding Global Internet Accessibility," The Fourth International Conference on Data Analytics, pp. 17-24, 2015.

[14] S. Chan and S. Sala, "Sensemaking and Robust Decision Engineering: Synchrophasors and their Application for a Secure Smart Grid," 7th IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp. 102-107, July 2013.

[15] R. Spousta and S. Chan, "Ocean Data Vulnerability to Cyber Manipulation and Consequences for Infrastructural Resilience," IEEE Future Technologies Conference (FTC), pp. 672-680, December 2016.

[16] "Insuring Space Activities," Aon Risk Solutions, October 16.

[17] R. Preston, "Sorry, But Outsourcing Isn't Evil," InformationWeek, 3 August 2012.

[18] P. Cohan, "Is the Boeing 787's electrical system working?" Daily Finance, 20 August 2009.

[19] P. Martin, "NASA's Management of the Deep Space Network," NASA Office of Audits, pp. 1-42, March 2015.

[20] P. Martin, "NASA Cybersecurity: An Examination of the Agency's Information Security," Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, pp. 1-9, February 2012.

[21] S. Chan, "Robust Decision Engineering: Collaborative Big Data and its Application to International Development/Aid," 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), pp. 597-604, December 2011.

[22] P. Bak, C. Tang, and K. Wiesenfeld, "Self-Organized Criticality," Physical Review, vol. 38, no. 1, pp. 364-375, July 1988.

[23] S. Chan, I. Oktavianti,1 V. Puspita, and P. Nopphawan, "Convolutional Adversarial Neural Network (CANN) for Fault Diagnosis within a Power System: Addressing the Challenge of Event Correlation for Diagnosis by Power Disturbance Monitoring Equipment in a Smart Grid," The 2nd IEEE International Conference on Information and Communications Technology (2nd ICOIACT 2019), July 2019.

[24] S. Chan, "Prototype Open-Source Software Stack for the Reduction of False Positives and Negatives in the Detection of Cyber Indicators of Compromise and Attack: Hybridized Log Analysis Correlation Engine and Container-Orchestration System Supplemented by Ensemble Method Voting Algorithms for Enhanced Event Correlation," The Third International Conference on Cyber-Technologies and Cyber-Systems, pp. 39-48, 2018.

[25] Z. Abbany, "SpaceX's Starlink satellite internet: It's time for tough talk on cyber security in space," Deutsche Welle, 2018, [Online]. Available from: https://www.dw.com/en/spacexs-starlink-satellite-internet-its-time-for-tough-talk-on-cyber-security-in-space/a-42678704/ 2019.05.27

 ISBN: 978-1-61208-743-6