Emory Corporate Governance and Accountability Review

Volume 8 | Issue 1

2021

Cyber Conflicts in Outer Space: Lessons from SCADA Cybersecurity

Roy Balleste

CYBER CONFLICTS IN OUTER SPACE: LESSONS FROM SCADA CYBERSECURITY

Roy Balleste[*]

He captured strange and distant worlds in greater detail than ever before. They were beautiful, magnificent . . . full of awe and wonder. But beneath their sublime surfaces . . . there was nothing. No love or hate. No light or dark. He could only see what was not there . . . and missed what was right in front of him.

—Roy McBride[1]

INTRODUCTION

The story of cybersecurity begins in land. By land, a cyber operations expert would mean the land mass on the surface of the Earth. The great monuments to human achievement surround our daily lives, every hour of every day. These testaments to human ingenuity are not the usual ones known to be appreciated as works of art. The monuments of concern for cybersecurity include, among others, power plants, electrical substations, water dams, water processing plants, auto assembly factories, and satellite ground stations. On January 10, 2014, Australia's IT News reported that Russian researchers Sergey Gordeychik and Gleb Gritsai discovered vulnerabilities in industrial control systems that granted them "full control of systems running energy, chemical and transportation systems."[2] The researchers spent a year prying into the supervisory control and data acquisition (SCADA) systems that controlled critical national infrastructure and, in particular, noted vulnerabilities in the Siemens WinCC software for industrial control systems.[3] The Siemens SIMANTIC WinCC refers to one of the SCADA components. In this case, the WinCC serves as a human machine interface portal for the use of the operator to control remote operations.[4] Siemens

---

[*] Dr. Roy Balleste is Assistant Professor of Law and Director of the Dolly & Homer Hand Law Library, Stetson University College of Law. Balleste teaches and conducts research in cybersecurity law and policy and the crossroads of cybersecurity and international space law. He was the 2017 recipient of the space law Nicolas Mateesco Matte Prize at McGill University. Professor Balleste is currently a core expert and member of the editorial board of the Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS). Balleste earned a certificate in cybersecurity (the intersection of policy and technology) from the John F. Kennedy School of Government at Harvard University, Executive Education. He is a member of the International Institute of Air and Space Law. This Article is dedicated to his wife Enarda and daughter Arya.

[1] AD ASTRA (20th Century Fox 2019) (Astronaut Roy McBride is a fictional character in this 2019 American science fiction film).

[2] Darren Pauli, *Hackers Gain 'Full Control' of Critical SCADA Systems*, IT NEWS (Jan. 10, 2014), https://www.itnews.com.au/news/hackers-gain-full-control-of-critical-scada-systems-369200.

[3] *Id*.

[4] *Siemens SIMATIC WinCC Programming*, DMC, https://www.dmcinfo.com/services/manufacturing-

did eventually release security updates for its SCADA products to patch critical vulnerabilities.[5] One of the vulnerabilities would have allowed an attacker "to remotely execute arbitrary code on a Siemens SIMATIC WinCC SCADA server by sending specially crafted packets to it."[6] This vulnerability received a score of 10 in the Common Vulnerability Scoring System—the maximum—since it would have allowed a full system's compromise.[7]

SCADA systems are common to the daily life of every nation in the world, yet these remain seriously vulnerable. For this reason, this Article provides guidance on selected aspects of securing the SCADA systems and its effects for the commercial satellite industry. The challenge for those engaged in space activities is much more complex than in the early days of the Gemini and Apollo programs. It is in this emerging world of clandestine online maneuvers that industry stakeholders encounter the evolving conflict of cyberspace in outer space. There are legal considerations that intersect the role of SCADA systems in modern society. These systems offer the benefits of automation while operating without the trappings of human error.[8] Since these systems are autonomous by design, human operators expect that production outcomes will match real-time unique management mechanisms of accuracy.[9]

SCADA systems are utilized across various industry sectors. In the modern world of industries' cyberthreats, the potential for a cyberattack with devastating consequences is not out of the realm of possibilities. As a result, senior executives are encouraged to improve the security of their organizations' SCADA systems. Failure of performance in one of these systems—for example, the water infrastructure—would raise serious and somewhat unexpected concerns for the human operators and the general public counting on their services. On April of 2020, Israel's Water Authority, along with the National Cyber Directorate, advised the water companies of a cyberattack on their SCADA systems.[10] The hacker's main intention had been to direct the systems

automation-and-intelligence/hmi-and-scada-programming/siemens-simatic-wincc-programming (last visited Nov. 23, 2020).

[5] Lucian Constantin, *Siemens Patches Critical SCADA Flaws Likely Exploited in Recent Attacks*, CSO (Dec. 1, 2014), https://www.csoonline.com/article/2853436/siemens-patches-critical-scada-flaws-likely-exploited-in-recent-attacks.html.

[6] *Id*.

[7] *Id*.

[8] *Id*.

[9] *Id*.

[10] Benjamin Kerstein, *Israel Thwarts Major Coordinated Cyber-Attack on Its Water Infrastructure Command and Control Systems*, THE ALGEMEINER (Apr. 26, 2020), https://www.algemeiner.com/2020/04/26/israel-thwarts-major-coordinated-cyber-attack-on-its-water-infrastructure-command-and-control-systems/.

to dump larger amounts of chlorine in the water.[11] There was a larger implication in this real scenario. While an attack against a water system may have been low profile, it presented high impact consequences.[12] The fact that malicious actors were willing to interfere with a water system, even during a pandemic, highlighted the security risks that management executives and operators must navigate.[13]

The lawyers of the twenty-first century have challenges beyond those of their counterparts in the twentieth century. Today's lawyers work within five domains that intersect technology: land, sea, air, outer space, and cyberspace. The role played by the lawyer vis-à-vis the chief information security officer (CISO) of an organization and the responsibilities associated with this role has become critical. The challenges at hand are those cyber conflicts that threaten the peaceful utilization of cyberspace. With the increasing proliferation of mobile technologies and the growing real-time borderless exchange of information, satellite networks have become a vital tool with international connotations requiring a global approach. It is in outer space where the next adventure begins. The exploration of outer space fills the imagination of many individuals. The idea of colonizing distant places of our solar system, and beyond, offers some tantalizing possibilities. This idea, in many ways, seems to border the imaginary. Indeed, the story of Astronaut Roy McBride, in the sci-fi film *Ad Astra*, compels us to consider the future possibilities of space exploration, while also reminding us of the fragile human existence:

> Vehicle system: "Trajectory, Earth. two point seven one four billion miles."
> Roy McBride: "I am looking forward to the day my solitude ends, and I'm home."

And with just a few words, McBride sparks our imagination about the solitude encountered in the immeasurable universe.[14] He helps us understand that future space travel will be challenging, where extraordinary events will intersect ordinary moments. As nations seek ways to protect their national critical infrastructure sectors, the international community wrestles with extraordinary legal challenges associated with ordinary vulnerabilities identified by malicious online attacks. Commercial activities in outer space, by default, will require

---

[11] *Id*.

[12] Cynthia Brumfield, *Attempted Cyberattack Highlights Vulnerability of Global Water Infrastructure*, CSO (May 7, 2020), https://www.csoonline.com/article/3541837/attempted-cyberattack-highlights-vulnerability-of-global-water-infrastructure.html.

[13] *Id*.

[14] AD ASTRA (20th Century Fox 2019).

some degree of cyberspace utilization. The applicability of international cyber law to space activities intersects, for example, with Article III of the Outer Space Treaty (OST), highlighting activities in outer space that could involve hacks of "the landlines that connect ground stations to terrestrial networks."[15] The applicability of international law finds it footing with Article III of the Outer Space Treaty:

> States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding.[16]

As a result, and by extension, Article III of the Outer Space Treaty provides part of the legal context for the application of international law to cyber operations in outer space. The concerns over cyber vulnerabilities have steadily become a matter of international priority and relevant to space activities. Michel Bourély, former General Counsel of the European Space Agency, explains that "[f]rom the moment when humanity began undertaking certain activities in space, the international community was conscious of the need to organize them by adopting, as early as possible, a means of regulation."[17] This was the first clue: new law would be needed to tackle future and emerging space activities. Indeed, he also notes that "by their very nature, space activities have no respect for national boundaries. . . ."[18] Thus, this lack of respect, if considered from the opposite point of view, opens up new challenges and new opportunities. This has been the essence of space, and interestingly, also of cyberspace. Cyberspace was invented for a military purpose, and this purpose has evolved over time. Despite its promising future, the complexities of Internet communications have become tied to the emergent space activities of nation-states and the commercial industry. The interconnection of cyberspace via ground stations and space via satellites have opened potential risks and actions of dubious motivations organized by malicious actors.[19]

---

[15] Todd Harrison et al., *Space Threat Assessment 2018*, CTR. FOR STRATEGIC & INT'L STUDIES (2018), https://aerospace.csis.org/wp content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf.

[16] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies art. III, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 (entered into force Oct. 10, 1967) [hereinafter Outer Space Treaty].

[17] Michel Bourély, *Space Commercialization and the Law*, 4(2) SPACE POLICY 131, 132 (1988).

[18] *Id*.

[19] *See generally* CLAY WILSON, CONG. RSCH. SERV., RL32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 24 (2008), https://fas.org/sgp/crs/terror/RL32114.pdf.

The status of security requires that cyberspace be understood as "an inherently adaptive, iterative and interactive domain."[20] Cyberspace, thus, is a landscape where nation-states and other actors remain in constant interactions and is a domain where conflict cannot be contained to specific areas.[21] In this landscape of threats, new space executives need to maintain the initiative—and anticipate that vulnerabilities will pose a danger to their operational outcomes.[22] One anticipated vulnerability is the tampering of data integrity or seeking to affect data availability.[23] Indeed, malicious code can be used to create a cyberattack aimed against computer instruction logic or data.[24] A malicious code can exploit vulnerabilities in computer software or security practices of an organization that, in turn, would disrupt data access.[25] These and relevant aspects of the security systems need to be understood and addressed by industry executives and SCADA operators.

The desire to resolve the challenges associated with SCADA systems has concentrated in surveying the vulnerabilities, understanding these, and proposing a solution. This Article seeks to add a new assessment process aided by existing standards. The Article offers guidance to understand selected aspects of the SCADA systems, including relevant information for the benefit of satellite industry executives, SCADA operators, and engineers. The Article identifies known threats and vulnerabilities. It also explains the consequences of significant cyberattacks that result in substantial damage or impairment to an organization. The Article also addresses recommended solutions to mitigate the associated risks. In particular, the following:

I. A Landscape of Conflict
II. Supervisory Control and Data Acquisition Systems
III. Conflict in Estonia
IV. Security Design and Legal Perceptions
V. A Cyberwar in Ukraine?
VI. Recommendations for the industry

---

[20] Robert J. Bebber, *Treating Information as a Strategic Resource to Win the "Information War,"* 61(3) ORBIS 394, 396 (2017).

[21] *Id*.

[22] *Id*.

[23] *See* Wilson, *supra* note 20, at 25.

[24] *Id*.

[25] *Id*.

I. A LANDSCAPE OF CONFLICT

In 2011 the US Air Force struggled to give meaning to the word "cyberspace."[26] These military experts struggled at the time—indeed not long ago—because this environment was defined as "a man-made domain, and therefore unlike the natural domains of air, land, and maritime."[27] However, if this was the case, then it represented a problem and one in which it gave "the impression that this domain [was] not connected with the real world."[28] Along these findings, it could be expected to infer that cyberspace defies imitations of capabilities. It would be better to redefine "the conceptualization of cyberspace [to] allow for its demystification and a closer alignment within the physical world."[29] If cyberspace was indeed to be seen as another domain in equal standing with land, sea, and air—it could be deduced—that another challenge would inevitably complicate the cyberthreat landscape. The problem would be to notice that "malicious cyber actors exploit gaps in international cybersecurity cooperation to launch multistage, multijurisdictional attacks."[30] As nations prepare to enter the next space age, and despite the clarity of the benefits offered by commercial space activities, the specific circumstances of cyber activities are likely to implicate other considerations regarding prohibited acts thereunder in accordance with international space law or international cybersecurity principles, and national laws. In addition, the nature of cyber operations involves a diverse group of stakeholders: nation-states, commercial organizations and international organizations.

The landscape that a senior executive must face is one of management decisions, while preparing for activities online that utilize cyberspace capabilities to "achieve objectives in or through cyberspace."[31] These capabilities also enable and achieve military objectives.[32] These cyberspace capabilities could be understood as a device, a computer program, or a technique, designed to create a particular effect.[33] These capabilities, for

---

[26] *See* PANAYOTIS YANNAKOGEORGOS & LYNN MATTICE, ESSENTIAL QUESTIONS FOR CYBER POLICY 1 (Air Univ. Press 2011), https://permanent.fdlp.gov/gpo57008/Essential_Questions_for_Cyber_Policy.pdf.

[27] *Id*.

[28] *Id*.

[29] *Id*.

[30] *Id* at 3.

[31] U.S. JOINT CHIEF OF STAFFS, JOINT PUBLICATION 3-0, JOINT OPERATIONS, at GL-8 (Jan. 17, 2017), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf.

[32] *See* UK MINISTRY OF DEF., JOINT DOCTRINE PUBL'N (JDP) 0-01.1., TERMINOLOGY SUPPLEMENT TO NATOTERM (A ed. 2019), https://www.gov.uk/government/publications/jdp-0-01-1-united-kingdom-supplement-to-the-nato-terminology-database.

[33] OFF. OF THE GEN. COUNSEL, U.S. DEP'T OF DEF., LAW OF WAR MANUAL §16.1.2 (2015), https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20

example, may also involve "computers, software tools, or networks."[34] Once a vulnerability is identified, the affected organization must endeavor to determine the level of risk associated with it and the tolerance for that risk.[35] Excellent communication amongst all organization stakeholders is the best step in designing a solution.[36]

The borderless nature of cyberspace has turned it into the potential domain of choice for surreptitious activities that now threaten to enter outer space. This is why future cyber operations involving space activities will demand that "the statesman and the jurist . . . know the extent to which a State has the acknowledged right to control all activity in the areas of space above its surface territory."[37] Space law experts Jackson and Freeland observe how States have been approaching activities in outer space that increasingly consider these "as part of active engagement in the conduct of armed conflict."[38] If States eventually manage to adopt new rules for cyber operations in space, it may be because scientific discoveries will enhance SCADA industries to gain greater security for space ventures. It is inspiring and impressive to look at the images of our planet shared with us by the National Aeronautics and Space Administration. It is from this vantage point that borders cannot be observed, nor can they be enforced. Neil Armstrong recalled that it suddenly struck him "that that tiny pea, pretty and blue, was the Earth."[39] The ongoing activities in outer space are an evolving global evolution. Human beings have once again stepped into the void of outer space supported by technological innovation.

Today, information-driven organizations and the consumers they serve live in an intriguing time of new space ventures. These ventures are intertwined with cyber operations. Article I, paragraph 2 of the Outer Space Treaty states that "Outer space . . . shall be free for exploration and use by all States. . . . "[40] The phrase "outer space should be used for peaceful purposes only" was recognized at the beginning of the preamble of the General Assembly Resolution on the

---

Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

[34] *Id*.

[35] *See* U.S. DEP'T OF HOMELAND SEC., NAT'L CYBER SEC. DIV., RECOMMENDED PRACTICE FOR PATCH MANAGEMENT OF CONTROL SYSTEMS 5 (2018), https://us-cert.cisa.gov/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf.

[36] *See id*. at 10.

[37] John C. Cooper, *High Altitude Flight and National Sovereignty*, 4 INT'L & COMP. L.Q. 411, 411, 418 (1951).

[38] Jackson Maogoto & Steven Freeland, *The Final Frontier: The Laws of Armed Conflict and Space Warfare,* 23 CONN. J. INT'L L. 165, 169 (2007).

[39] COLIN BURGESS, FOOTPRINTS IN THE DUST: THE EPIC VOYAGES OF APOLLO, 1969-1975, at 405 (2010).

[40] *See* Outer Space Treaty, *supra* note 17, at art. I.

Question of the Peaceful Use of Outer Space.[41] The resolution recognized the need for cooperation to promote mutual understanding and the strengthening of friendly relations to reach the goal of peaceful activities in outer space.[42] It is reasonable to infer that activities in cyberspace are included in the "use" of outer space. The ultimate goal is to highlight the need to protect space assets from malicious intruders. In the cyberspace realm, these dangers embody a complex set of connections involving people, networks, facilities, space objects, and information. The present-day world arena has become a theater of combat with nation-states "armed with weapons to devastate the globe launched through the medium of outer space."[43] This environment must be understood from the numerous nation-states with their respective claims.[44] These claimants or stakeholders represent a decision development process, in which, as noted:

> the factor of greatest significance affecting claims is the lack of a centralized political authority possessing sufficient control of force, military and other, to support, with whatever dispatch and comprehensiveness may be required, the general community efforts to minimize unauthorized coercion.[45]

This is the case given that these claimants are not homogeneous in their goals for deploying their activities in cyberspace. SCADA industry stakeholders must recognize that cyber operations will be a threat to conducting space activities. The intersection of space activities and cyber operations raises a sense of nostalgia about the long-gone days of online innocence and safety. Whether hackers utilize malicious code or other techniques, these cyber operations directly affect the day-to-day life of the general public.[46] For these reasons, the information used for the functioning of the SCADA systems should be designated a valuable asset under the protection and due diligence of the organizations that manage it. "Treating information as a strategic resource requires rethinking assumptions in the economic, political, informational, military, and other domains.[47]" It has been suggested that cyberspace should not be understood as a space for deterrence, but as "an offense-persistent

---

41 G.A. Res. 1348 (XIII), U.N. Doc. A/4009 para. 1 (Dec. 13, 1958), *available at* https://www.unoosa.org/pdf/gares/ARES_13_1348E.pdf.

42 *See id*.

43 MYERS S. MCDOUGAL, HAROLD D. LASWELL & IVAN A. VLASIC, LAW AND PUBLIC ORDER IN SPACE 17 (1963).

44 *Id.* at 87.

45 *Id.* at 93–94.

46 Wilson, *supra* note 20, at 15.

47 Bebber, *supra* note 21.

environment."[48] In other words, to protect organizational assets, security measures alone will not suffice.[49]

Outer space is now the new landscape of cyber operations that directly threatens the organizations' security environment. Security managers will be successful if guided by a basic recognition that for a profitable and secure environment of their space-based technologies, these information-driven organizations must acknowledge that cyberattacks will occur anywhere with unfortunate consequences. As noted in CNN, a survey by PwC revealed that only 39% of business executives "weighed the impact of a cyberattack on their brand image."[50] Organizations such as SpaceX and Blue Origin would fare better learning from other companies based on the surface of the Earth. The vulnerability of satellites continues to be an afterthought and one that has not been properly tied to similar cyberthreats tied to our critical national infrastructure.[51] "This is a significant failing, given society's substantial and ever increasing reliance on satellite technologies for navigation, communications, remote sensing, monitoring and the myriad associated applications."[52] Indeed, the reality to be found in the future use of cyberspace in outer space is complex and urgent. It would be appropriate to consider that given the time and expense needed to launch a satellite, the consequences of SCADA systems' use and due diligence expectations by organizations' executives are paramount. A commercial outer space cybersecurity strategy needs to be carefully considered, especially now, and this strategy depends on the lessons learned from other domains. The communications' data that this industry manages involves practical applications that have a direct repercussion on daily human activity. These applications of valuable communications have become susceptible to cyberattacks.

The very solemn and insightful message contained in the 1958 *General Assembly Resolution on the Question of the Peaceful Use of Outer Space* opened up a process that continues to this day.[53] The General Assembly established the United Nations Ad Hoc Committee on the Peaceful Uses of Outer Space, and is

---

[48] *Id*. at 401.

[49] *See id*.

[50] Peter W. Singer & Allan Friedman, *Five Lessons from the Sony Hack*, CNN (Dec. 17, 2014, 6:00 PM), https://www.cnn.com/2014/12/17/opinion/singer-friedman-sony-hacking-lessons/index.html.

[51] DAVID LIVINGSTONE & PATRICIA LEWIS, CHATHAM HOUSE, SPACE, THE FINAL FRONTIER FOR CYBERSECURITY? 3 (2016), https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

[52] *Id*.

[53] *Question of the Peaceful Use of Outer Space*, GA Res 1348(XIII), UNGAOR, 13th Session, U.N. Doc A/RES/13/1348(XIII) (1958), at Preamble.

so doing, observed that it would be necessary to be mindful of "legal problems which might arise in the exploration of outer space."[54] Later, the members of the United Nations Ad Hoc Committee, Legal Committee observed that "it would be impossible to identify and define, exhaustively, all the juridical problems which might arise in the exploration of outer space."[55] In that light, our present understanding of SCADA systems seems to be challenged by the available understanding of the technology and the activities that reflect cyber operations.

II. SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEMS

The present-day space venture executive may obtain big rewards because it has confidence in new projects that push the boundaries of technological developments. The modern executive observes as NASA's Commercial Crew Program partners for the second time—next October—with astronauts traveling to the International Space Station aided by a Crew Dragon spacecraft propelled by a Falcon 9 rocket.[56] Yet, threats found on the land domain, and for that matter, in the cyber domain, have not been constrained to these theaters of operation. The domain of clandestine online maneuvers continues to threaten industry stakeholders. In August 2007, cosmonauts traveling to the International Space Station carried laptops that unknowingly were infected with a virus known as *Gammima.AG*.[57] The virus was designed to lay dormant on the infected laptops in preparation to steal login names for popular online games.[58] "NASA said it was not the first-time computer viruses had travelled into space and it was investigating how the machines were infected."[59] While in outer space borders are imperceptible, closer to the ground, our legal challenges stress the threats to well-established legal notions that raise doubts within present realities. The need to protect systems has increased along with the deserved awareness of cyberthreats and the needed countermeasures.[60] The system components of the SCADA systems are designed to manage critical infrastructure components; for example, those controlling the generation of power.[61] These systems are now

---

[54] *Id.* at para. 1(d).

[55] *See* Ad Hoc Committee on the Peaceful Uses of Outer Space, *Report of the Legal Committee*, U.N. Doc A/AC.98/2 (1959), at para. A.1.

[56] Anna Heiney, *NASA, SpaceX Targeting October for Next Astronaut Launch*, NASA: COMMERCIAL CREW PROGRAM (Aug. 14, 2020), https://blogs.nasa.gov/commercialcrew/2020/08/14/nasa-spacex-targeting-october-for-next-astronaut-launch/.

[57] Pierluigi Paganini, *Improving SCADA System Security*, INFOSEC RES. (Dec. 6, 2013), https://resources.infosecinstitute.com/improving-scada-system-security/.

[58] *Id.*

[59] *Id*.

[60] *Id*.

[61] Aleksander Gorkowienko, *Five Steps to Reduce Risk for Critical Infrastructure and Industrial Control*

connected to the Internet and vulnerable everywhere and at any time. The convenience of real-time connections has come at a cost.[62]

There is a much darker threat that forces the modern executive to understand the shortcoming and necessities of today's SCADA systems. Historically, SCADA systems were designed with dedicated networks. Once the remote management process was connected to the IP networks, this opened the systems to the challenges associated with cyberspace.[63] The control for the generation of power—by design—was intended to be a distributed system. In other words, this system has been managed with advanced software that offers "independence on distance, flexible operation, easy upgrade, and reasonable cost to monitor and control" all devices in widespread areas.[64] The key or purpose of a SCADA system is efficient communication. The critically interrelated components of the system manage to function as one unit, yet each is a system on itself. SCADA systems operate with five main components, including a human machine interface (HMI), a supervisory system, remote Terminal Units (RTUs), programmable logic controllers (PLCs), and other communication infrastructures.[65] The function of the HMI is to present the information graphically to the human operator.[66] The information could be related to scheduled maintenance, schematics, logistic information, and diagnostic data.[67] The supervisory system can be a single PC or multiple servers used to link the communication between the SCADA equipment and the HMI software.[68] The RTUs are microprocessors that transmit telemetry data to the supervisory system, while the PLCs are designed to collect the sensor output signals or digital data.[69] The communication infrastructures work with a combination of radio and direct wired connections to connect the systems.[70] Once the five SCADA components are connected with the appropriate software, the end result

Systems, AM. CITY & CNTY. (Apr. 24, 2019), https://www.americancityandcounty.com/2019/04/24/5-steps-to-reduce-risk-for-critical-infrastructure-and-industrial-control-systems/.

[62] *See* Randy Dennison, *A Pre-SCADA System Assessment*, 36 POLLUTION ENG'G 22, 22 (2004).

[63] Marcio Andrey Teixeira et al., *SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach*, 10 FUTURE INT. 1 (2018), https://arxiv.org/ftp/arxiv/papers/1904/1904.00753.pdf.

[64] Phan Duy Anh & Truong Dinh Chau, *Component-Based Design for SCADA Architecture*, 8 INT'L J. CONTROL, AUTOMATION & SYS. 1141, 1141 (2010).

[65] Donald Krambeck, *An Introduction to SCADA Systems*, ALL ABOUT CIRCUITS (Aug. 31, 2015), https://www.allaboutcircuits.com/technical-articles/an-introduction-to-scada-systems/.

[66] *See id.*

[67] *Know All About SCADA Systems Architecture and Types with Applications*, WATELECTRONICS (July 26, 2019), https://www.watelectronics.com/scada-system-architecture-types-applications/.

[68] *Id*.

[69] *Id*.

[70] *Id*.

is the SCADA system.[71] The SCADA software functions in the traditional manner of processing, distributing, and displaying the data for the human operators.

The human machine interface is the component within the SCADA system that can easily demonstrate the future challenges for the industry. In order to assess the technological aspects of cybersecurity, it is also important to understand the landscape of threats. Indeed, within the SCADA arena, the problem is exacerbated by professional hackers conducting attacks for the benefit of foreign governments. This is the most dangerous threat for SCADA systems. Ironically, the case that illustrates the most significant damage to the cyber-landscape had nothing to do with SCADA. The case is interesting for several reasons. First, the attack was made by sophisticated hackers believed to be operating from Russia, where a significant portion of their operations may continue to this day.[72] These hackers seemed to have been motivated to adjust their cybercrime landscape of operations and developed a new and politically motivated attack vector to infiltrate another nation.[73] Moreover, this type of attack had never been attempted before.

III. CONFLICT IN ESTONIA

The Estonian DDoS attack forced cybersecurity experts to acknowledge that cyberspace was evolving rapidly along with old techniques being applied to new situations.[74] A new political threat was rising within cyberspace, where governments were fomenting cyber operations, yet would not take credit for them.[75] While the real reason for the attack is not relevant to this Article, the attack illustrated how structurally vulnerable systems could be disabled to the detriment of the nation and the general public. "Online services of Estonian banks, media outlets and government bodies were taken down by unprecedented levels of internet traffic."[76] The attack was particularly pervasive and effective given the use of botnets used to send huge amounts of automated online requests.[77] A sort of paralysis slowed down or completely stopped the banking

---

[71] *Id*.

[72] Gadi Evron, *Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War*, 9 GEO. J. INT'L AFF. 121, 122 (2008).

[73] *Id*.

[74] *Id.* at 125.

[75] Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace*, 6 STRATEGIC STUD. Q. 126, 129 (2012).

[76] Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC NEWS (Apr. 27, 2017), https://www.bbc.com/news/39655415.

[77] *Id*.

industry, along with government agencies.[78] By now there were no doubts that Estonia was experiencing a Distributed Denial of Service(DDoS) attack, and one powerful enough to swamp, jam, and disable sites by overcrowding the bandwidths of the servers running them.[79] It has been noted that "massive flooding attacks in the 50 Gbps range are powerful enough to exceed the bandwidth capacity of almost any intended target."[80] The attack's origins were Russian, including Russian government institutions.[81] The age of cross-border government cyber operations was just beginning.

The challenges for SCADA are many, yet there is a commonality across the industries. In essence, modern systems of control automation need to interface with old and obsolete equipment.[82] The obsolete equipment functions with proprietary technology to handle data and applicable solutions tend to be complicated and very expensive.[83] Modern SCADA systems are impressive and offer rapid application development.[84] These systems offer "real-time data from the plant floor to be accessed from anywhere in the world. This access to real-time information allows governments, businesses, and individuals to make data-driven decisions about how to improve their processes."[85] For example, organizations with seemingly workable SCADA devices have had little incentive to upgrade the hardware.[86] As noted earlier, "utilities and other industries rely on SCADA devices that were developed before the internet age and cannot be updated. And even if a vendor can provide a security patch," the immensity of the system makes it impractical to shut it down simply to apply the patch.[87]

For managers discovering the new landscape, this is the typical story that CISOs have learned to expect. The existing legal standards for cyber operations—in outer space—are inadequate, and this may become more troublesome in times of rising tension. Future cybersecurity plans must include potential cyberattacks and new developments in SCADA technologies. Indeed, just as on land, space activities are bound to be "understood in relation to a

---

78 *Id.*

79 *See id*.

80 WILLIAM STALLINGS & LAWRIE BROWN, COMPUTER SECURITY, PRINCIPLES AND PRACTICE 243 (2014).

81 *See* McGuinness, *supra* note 77.

82 *See* Dennison, *supra* note 63.

83 *What is SCADA?*, INDUCTIVE AUTOMATION (Sept. 12, 2018), https://inductiveautomation.com/resources/article/what-is-scada.

84 *Id*.

85 *Id*.

86 *See* Gorkowienko, *supra* note 62.

87 *Id*.

broader concept of 'information warfare'—as its offensive aspect, i.e. 'activities aimed at destruction, take-over, harmful modification or use of informational resources of attacked entity or the means of their storage, transfer and processing.'"[88] This was the case in Estonia. While the shutdown of an entire power plant (to patch the system), for example, could cost millions of dollars a day, managers may not have considered carefully the more significant losses associated with a massive breach.[89]

IV. SECURITY DESIGN AND LEGAL PERCEPTIONS

The commercialization of the space industry has opened up opportunities to conduct activities that create security challenges for organizations utilizing satellite systems. These practices include communications with organizations' space assets via "the landlines that link ground stations to terrestrial networks, user terminals that link satellites, and antennas on satellites and ground stations."[90] The communications originating from ground stations may involve public web servers and web pages that are accessible on the Internet.[91] These public web servers' accessibilities are also, in turn, a security risk that requires an understanding of necessary measures.[92] The threats associated with data transfers through ground stations are of particular relevance because of the dependence on outer space activities related to cyber-enabled communications between satellites and ground users.[93] This means that a SCADA attack could result in the death of dozens or even hundreds by "shutting down power to a hospital or an Air Traffic Control tower."[94] It has been suggested that a SCADA attack that would cause bodily harm to a larger population, for example, by "interfering with control elements of the power grid, air traffic control networks, or nuclear power plant safety systems" would be unlikely used as a cyberwarfare tool.[95] This suggestion may have been reasonable over ten years ago. The truth

---

[88] Marcin Terlikowski, *Cyberattacks on Estonia: Implications for International and Polish Security*, 16 POLISH Q. INT'L AFF. 68, 69 (2007).

[89] *See* Gorkowienko, *supra* note 62.

[90] RAJESWARI PILLAI RAJAGOPALAN, U.N. INST. FOR DISARMAMENT RSCH., ELECTRONIC AND CYBER WARFARE IN OUTER SPACE 9 (2019).

[91] DEBRA LITTLEJOHN SHINDER & MICHAEL CROSS, SCENE OF THE CYBERCRIME 495 (2d ed. 2008).

[92] *Id*.

[93] *See* NATO COOPERATIVE CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 270 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

[94] *See* Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 147 (2009).

[95] *See id.* at 148.

is that cybersecurity professionals and organization executives must precisely expect the opposite.

As time has passed, attacks on SCADA systems have become more dangerous. In 2008, a pipeline explosion in Turkey was caused by a cyberattack.[96] At the time, this was not known and it would not be until 2014 that experts managed to reach that conclusion.[97] The hack occurred via the pipeline's surveillance cameras, which in turn, were connected to the control system network.[98] Eventually, the hackers manage to "cut off communications between the pipeline and the control room, jammed the backup satellite communications, erased all surveillance footage," then continued by super-pressurizing the crude oil in the pipeline which caused an explosion.[99] The damage was financially catastrophic. Unfortunately, these types of attacks will continue simply because the nation-states that sponsor them can do it and will continue to pursue them as long as these prove valuable.[100] These "cyber attacks do not require the wealth and resources of traditional military attacks, they can be utilized by poorer nations or rogue organizations, and victims are provided little to no forewarning."[101]

At present, SCADA cybersecurity threats could be analyzed in levels of alarming damage, yet all continue to grow in frightening consistency.[102] For example, these cyber threats may include:[103]

- Service Disruption - disruption of essential services such as power, water, and emergency services;
- Safety Degradation - it can result in loss of human life and other severe effects;
- Military Targeting - serious military consequences via targeted attacks at government services supporting the warfighter.[104]

---

96 Hillary Hellmann, *Acknowledging the Threat: Securing United States Pipeline Scada Systems*, 36 ENERGY L.J. 157, 165 (2015).

97 *See id*.

98 *Id*.

99 *Id*.

100 *Id.*

101 *Id.*

102 Ryan Gallagher et al., *A Case Study on Improving ICS Cyber Security Legislation*, 8 J.L. & CYBER WARFARE, Spring 2020, at 108.

103 *Id.*

104 *Id.* at 108-109.

Just as with terrestrial communications, space activities also suffer from vulnerabilities that adversely affect space-enabled communications.[105] One of these vulnerabilities involves the uplinks that connects the ground station to the satellite, which could be intercepted in the way to the satellite.[106] For this reason, cyber activities that support space activities should not simultaneously include offensive operations that may be designed for the destruction of satellites, their subcomponents, or supporting infrastructure.[107] In other words, a nation-state that sponsors a hacker group to perpetrate an attack masqueraded as a legitimate satellite communication is truly problematic. This is the real source of the cyber threat. A greater threat is always associated with higher vulnerability. One vulnerable space segment involves the very small aperture terminals (VSATs), "which are small satellite dish-based computer systems, that provide broadband Internet access to remote locations, or transmit point of sale credit card transactions, SCADA and other narrowband data."[108] The landscape of vulnerabilities is vast with "over 2.9 million active VSAT terminals in the world, with two-thirds of those devices [in] the U.S., being used in the defense sector," along with banks and the industrial sector.[109] Unfortunately, many of these unprotected terminals operated with very poor password strength and had become good targets for attacks.[110]

The problem has gone beyond expected vulnerabilities. For SCADA executives, the problem now extends to the consumer they serve. For example, a group of Russian-speaking hackers also hacked "commercial satellites to siphon sensitive data from diplomatic and military agencies in the United States and in Europe," while concealing their location.[111] The group, known as Turla, "after the name of the malicious software it uses . . . [focuses on] diplomatic and military targets in the United States, Europe, Middle East and Central Asia to gain political and strategic intelligence."[112] Turla's crimes required concealment, which meant that the hackers needed to hijack "the satellite IP

---

[105] *See* TALLINN MANUAL 2.0, *supra* note 94, at 270.

[106] BRUCE R. ELBERT, THE SATELLITE COMMUNICATION GROUND SEGMENT AND EARTH STATION HANDBOOK 175 (2d ed. 2014).

[107] *See* TALLINN MANUAL 2.0, *supra* note 94, at 274–75.

[108] Darlene Storm, *Hackers Exploit SCADA Holes to Take Full Control of Critical Infrastructure*, COMPUTERWORLD (Jan. 15, 2014, 12:51 PM), https://www.computerworld.com/article/2475789/hackers-exploit-scada-holes-to-take-full-control-of-critical-infrastructure.html.

[109] *Id*.

[110] *See id*.

[111] Ellen Nakashima, *Russian Hacker Group Exploits Satellites to Steal Data, Hide Tracks*, WASH. POST (Sept. 9, 2015), https://www.washingtonpost.com/world/national-security/russian-hacker-group-exploits-satellites-to-steal-data-hide-tracks/2015/09/08/c59fa7cc-5657-11e5-b8c9-944725fcd3b9_story.html.

[112] *Id.*

addresses of legitimate users to use them to steal data from other infected machines in a way that hides their command server."[113] On the other hand, ground stations are known to handle command and control of space communications. Since SCADA systems are located in the ground stations, the hacking of these facilities would expose nation-states in the crossing of the proverbial line into the space activities arena.[114] As noted earlier, the Outer Space Treaty is specific about this type of interference. Article I (2) of the Outer Space Treaty highlights how outer space shall be free for exploration and use.[115] In the same manner, the ITU Constitution Article 45(1), establishes that the operation of all stations should be in "a manner as not to cause harmful interference to the radio services or communications."[116] Regrettably, at the moment, perfectly defined legal structures seem to simply symbolize guideposts rather than function as legal sentries with the power to exert real consequences on perpetrators. This leaves the industry organizations with one option: strong cybersecurity measures.

These practices include communications with organizations' space assets via "the landlines that link ground stations to terrestrial networks, user terminals that link satellites, and antennas on satellites and ground stations."[117] The communications originating from ground stations may involve public web servers and web pages that are accessible on the Internet.[118] These public web servers' accessibilities are also, in turn, a security risk that requires an understanding of necessary measures.[119] The real challenge arises with the satellite industry's practice of operating with remote users. Satellites contain hardware and software truly distant and isolated from the user.[120] The satellite-spacecraft, only connected to a ground station, would be lost, "with no possibility of recovery" without the control of the user.[121] The ground stations function as the facilities that "directly support space activities terrestrially" to accomplish a mission in or through space.[122] These facilities operate by

---

113 Kim Zetter, *Russian Spy Gang Hijacks Satellite Links to Steal Data*, WIRED (Sept. 9, 2015, 8:30 AM), https://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/.

114 *See* TALLINN MANUAL 2.0, *supra* note 94, at 278.

115 Outer Space Treaty, *supra* note 17, at art. I.

116 Constitution of the International Telecommunication Union, Dec. 22, 1992, 1825 U.N.T.S. 330 (entered into force on July 1, 1994) (as amended by the 2018 Plenipotentiary Conference).

117 RAJAGOPALAN, *supra* note 91, at 9.

118 SHINDER & CROSS, *supra* note 92, at 495.

119 *Id.*

120 *See, e.g.*, Consultative Comm. for Space Data Sys., *Rep. Concerning Space Missions Key Mgmt. Concept*, CCSDS Doc. 350.6-G-1 (Nov. 2011), https://public.ccsds.org/Pubs/350x6g1.pdf.

121 *Id.* at 4-1.

122 U.S. DEP'T OF DEF., DICTIONARY OF MILITARY AND ASSOCIATED TERMS 198 (2019).

transferring data between segments.[123] Thus, a means of data transmission is maintained between a satellite and its operator-users. The ground segment equipment supports command and control of space segment resources, as well as the user terminal equipment, "and the interconnectivity between the facilities in which this equipment is housed."[124]

Another example of the commercial satellite industry is the Amazon Web Services (AWS) Ground Station. Amazon offers the ability for executives to obtain, direct, and create satellite data without having to invest in building a ground station.[125] In essence, organization executives can now borrow one of several stations owned by Amazon, and in turn, access the control interface via a secure multifactor authentication, known as the customer onboarding.[126] Authentication includes encryption via two keys, one private key and one public key, working as security credentials for identity.[127]

V. A CYBERWAR IN UKRAINE?

The satellite and space venture industry is, at the moment, an industry in rapid evolution, but is one constantly threatened by cyberthreats. The inopportune and ongoing threats have continued with BlackEnergy—regrettably—a tool utilized by the group known as Sandworm. This band is in essence a unit of the General Staff of the Armed Forces of the Russian Federation, also known as GRU.[128] The GRU has been associated with Russia's military intelligence agency, election meddling, attempted assassination, and the downing of MH17 over Ukraine.[129] A group so ruthless and vicious should give pause, not just to any IT department, but to any organization with assets connected to the Internet. Around 2007, BlackEnergy attacks were common. The group's weapon of choice was a bot designed for distributed denial of service (DDoS) attacks.[130] BlackEnergy offered to its user a two-way malicious

---

123 U.S. DEP'T OF DEF., JOINT PUBLICATION 3-14, SPACE OPERATIONS, at I-2 to I-3 (Apr. 10, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14ch1.pdf (incorporating Change 1 made on Oct. 26, 2020).

124 *Id.* at I-3.

125 AMAZON WEB SERVICES, AWS GROUND STATION USER GUIDE 1 (2020), https://docs.aws.amazon.com/ground-station/latest/ug/groundstation-ug.pdf.

126 *Id.* at 10.

127 *Id.* at 53.

128 *See* Andrew Marino, *Sandworm Details the Group Behind the Worst Cyberattacks in History*, THE VERGE (July 28, 2020, 1:31 PM), https://www.theverge.com/21344961/andy-greenberg-interview-book-sandworm-cyber-war-wired-vergecast.

129 *Id*.

130 JOSE NAZARIO, ARBOR NETWORKS, BLACKENERGY DDOS BOT ANALYSIS 2 (Oct. 2007), http://pds15.egloos.com/pds/201001/01/66/BlackEnergy_DDoS_Bot_Analysis.pdf.

advantage: the bot could target more than one IP address per hostname and used a runtime encryption to thwart antivirus detection.[131]

When Sandworm began its malicious operations, the risk panorama for the energy industry was not yet clear. Sandworm took a cyberweapon to be utilized for DDoS attacks, known as *BlackEnergy1*, and in the process, created a new version that would target SCADA systems—*BlackEnergy3*.[132] While BlackEnergy 3 evokes the attacks on Estonia, one particular similarity to be accepted would be the potential damage to confidentiality, integrity, and availability of the systems across borders. Executives with any doubts about their need for security should be interested in the history of the BlackEnergy attacks. In 2014, a specific user group of BlackEnergy attackers deployed SCADA-related attacks across industries around the world, demonstrating "a unique skillset, well above the average DDoS botnet master."[133] Trojans used by BlackEnergy have been identified as *Backdoor.Win32.Blakken*, *Backdoor.Win64.Blakken*, *Backdoor.Win32.Fonten*, and *Heur:Trojan.Win32.Generic*.[134] BlackEnergy malware appeared in 2007 as a DDoS tool and was traded among cybercriminals until 2010, when Sandworm began "utilizing BlackEnergy2 to conduct espionage against industrial control system networks."[135] Most recently, BlackEnergy3 was involved in the 2015 cyberattacks in Ukraine that resulted in power outages.[136] These 2015 power grid events served as a reminder that consumers would also become victims in these type of attacks. In Ukraine, the hackers seemed to have spent months conducting extensive reconnaissance while mapping the SCADA network to gain access to user accounts.[137] Once equipped with access to log-in credentials to the SCADA network, the hackers had what they needed to attack.[138]

It is disturbing to consider that a SCADA system, designed to collect real-time data from remote locations, could be used aggressively for malicious purposes.[139] Unlike previous incidents involving other versions of BlackEnergy,

---

131 *Id*.

132 OTW, *SCADA Hacking: Anatomy of a SCADA Malware, BlackEnergy 3*, HACKERS-ARISE (Nov. 19, 2019), https://www.hackers-arise.com/post/2018/10/10/scada-hacking-anatomy-of-a-scada-malware-blackenergy-3.

133 *BlackEnergy APT Attacks in Ukraine*, KASPERSKY LAB (Sept. 19, 2017), https://usa.kaspersky.com/resource-center/threats/blackenergy (last visited Jan. 14, 2021).

134 *Id*.

135 *NJCCIC Threat Profile Black Energy,* STATE OF N.J. (Aug. 10, 2017), https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/blackenergy.

136 *See id.*

137 Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

138 *Id*.

139 STEVEN M. KAPLAN, WILEY ELECTRICAL AND ELECTRONICS ENGINEERING DICTIONARY 680 (2004).

with BlackEnergy3, the hackers utilized spear-phishing emails later delivered to Ukrainian energy companies along with "weaponized Microsoft Word documents."[140] The exact target of the attacks was a Ukrainian power facility, Prykarpattya Oblenergo, and other electricity distribution companies in the same country.[141] The hackers showed remarkable skill by manipulating the Microsoft Office documents with malware that allowed them a foothold in the networks, while also harvesting credentials and accessing the Human Machine Interface.[142] During the attack, the intruders also managed to conduct a telephonic denial of service on the company's call center, controlling thousands of calls that prevented customers from seeking assistance.[143] Finally, to wrap up the wave of destruction, the hackers utilized the KillDisk component, which is designed to delete essential files on the disk drive and empties Windows event logs, rendering the system unbootable.[144] For the SCADA industry executive, the challenge lies in the way these cyberattacks are permeated by foreign government activities that maliciously endangers human life.

VI. RECOMMENDATIONS FOR THE INDUSTRY

One potential solution to ensure the security of the command subsystems is to apply the zero-trust model. This model offers an additional level of security simply because it is "centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access."[145] This method is particularly useful in an industry that relies on roles and user identities. In other words, utilizing the technologies and security methods noted above, the zero-trust model applies "granular perimeter enforcement based on users, their locations and other data" to identify, authenticate, and authorize.[146] A recent report from the Defense Innovation Board (DIB) of the Department of Defense noted that it is best not to see a

---

[140] *NJCCIC Threat Profile*, *supra* note 136.

[141] *Frequently Asked Questions: BlackEnergy*, TREND MICRO (Feb. 11, 2016), https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy.

[142] ROBERT M. LEE ET AL., ELEC. INFO. SHARING & ANALYSIS CTR., ANALYSIS OF THE CYBER ATTACK ON THE UKRAINIAN POWER GRID: DEFENSE USE CASE 1 (Mar. 18, 2016), https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[143] *Id.* at 9.

[144] Anton Cherepanov & Robert Lipovsky, *BlackEnergy – What We Really Know About the Notorious Cyber Attacks*, 2016 VIRUS BULL. CONF. 6, https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cherepanov-Lipovsky.pdf.

[145] Mary K. Pratt, *What is Zero Trust? A Model for More Effective Security*, CSO (Jan. 16, 2018, 3:08 AM), https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html.

[146] *Id.*

network as a trusted and secured house, but instead as an unreliable apartment building, where no trust is offered to the perimeter security and for that reason apartments are locked until proper trust is established (in this case, with the network user).[147]

An example to follow is provided by the best practices of Palo Alto Networks and their clients to ensure identification, authentication, and authorization. The user that enters the ground station building must face the same security protocols as in many other industries.[148] For purposes of this analysis, the immediate concern is the vulnerability associated with satellite Internet connections and authorized subscribers' IP addresses.[149] The systems associated with ground stations "use state-of-the-art terrestrial security technology to establish secure communications suitable for the missions," including Secure Sockets Layer.[150] The SSL application layer encryption is a standard security technology used to establish an end-to-end encryption link between the ground station web server and the user.[151] Once the user is ready, a publicly accessible SSL-enabled Web server serves as a portal to authenticate satellites once the user accesses the system.[152] Additionally, the SCADA system's staff of any organization, from operator to senior management, has the opportunity to participate within a new security awareness environment that is developing across the industry. The US Cybersecurity & Infrastructure Security Agency (CISA) has been appraised of the status of the industry in order to formulate the Industrial Control Systems (ICS) strategy. The strategy concentrates mainly on awareness and aims at a multi-year, focused approach to improve CISA's ability to manage ICS risk.[153] This strategy also serves as the best approach to consider the recommendations in this Article. CISA strategy is only the beginning, yet it helps to summarize the cyberthreat landscape by concentrating on three main facts:

---

147 KURT DELBENE ET AL., DEF. INNOVATION BD., THE ROAD TO ZERO TRUST (SECURITY), at 3 (July 9, 2019), https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF.

148 M. Manulis et al., *Cyber Security in New Space*, INT'L J. OF INFO. SEC. (May 12, 2020), https://doi.org/10.1007/s10207-020-00503-w.

149 *Id*.

150 Consultative Comm. for Space Data Sys., *Sec. Architecture for Space Data Sys. Recommended Prac.*, CCSDS Doc. 351.0-M-1, at 7-2 (Nov. 2012), https://public.ccsds.org/Pubs/351x0m1.pdf.

151 ELBERT, *supra* note 107, at 176.

152 *Configure the Portal to Authenticate Satellites*, PALO ALTO NETWORKS, https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/large-scale-vpn-lsvpn/configure-the-portal-to-authenticate-satellites (last visited Dec. 14, 2020, 3:34 PM).

153 *See* CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, SECURING INDUSTRIAL CONTROL SYSTEMS: A UNIFIED INITIATIVE 1–2 (2020), https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf.

1) Operational technologies are migrating into domains connected to the Internet.

2) The risk topography with the deployment of 5G networks.

3) A diverse ICS community in partnerships with federal, state, and local governments.[154]

At the commercial level, cybersecurity experts can identify efforts such as those from General Electric Digital. The approach of GE Digital is to reduce human error (a serious cause of vulnerabilities).[155] The solution presented by GE is called iFIX and is part of the next generation human machine interface for SCADA. If not upgraded, security systems would suffer from weak efficiency, increased operator errors, and higher risks, given the lack of needed digital certificates and Web tokens.[156] In other words, the next generation human machine interface should be installed on all local and remote workstations.[157] The process of software enhancement should be understood as an organizational security priority. Unfortunately, this may not be enough. As the preceding sections made clear, threats and vulnerabilities have increased, including human error. This could include an error as simple as being tricked by a phishing attack or an unexpected ransomware intrusion. Thus, the main recommendation of this Article is to proceed with a multi-prong cybersecurity approach that includes acknowledging that cyberthreats are changing rapidly, monitoring industry trends and risks, and having a continuous security risk management process, along with periodic reviews, audits, patch management, and antivirus updates.[158] The alternative would be disastrous, as companies slow to upgrade their systems suffer immediate and costly consequences.

Experts in the field compared the cost of legacy SCADA systems versus the investment in efficiency, safety, and operational visibility.[159] Cybersecurity experts are now aware of the additional rising trend of ransomware attacks in the SCADA industry.[160] The most recent SCADA attack in this category

---

[154] *Id.* at 4–5.

[155] iFix 6.1 Brochure, *Speed Operator Response and Increase Efficiency with iFIX*, GE DIGITAL, https://www.ge.com/digital/sites/default/files/download_assets/iFIX-6-dot-1-from-ge-digital.pdf (last visited Jan. 14, 2021).

[156] *Id*.

[157] *Id*.

[158] Sunil Doddi, *Understanding Industrial Control Systems Security Basics*, CONTROL ENGINEERING (Apr. 6, 2018). https://www.controleng.com/articles/understanding-industrial-control-systems-security-basics/.

[159] *The Cost of Legacy SCADA Systems*, AUTOMATION IT, https://www.automationit.com/blog/83-the-cost-of-legacy-scada-systems (last visited Jan. 14, 2021).

[160] Kevin Townsend, *Honda Ransomware Confirms Findings of Industrial Honeypot Research*,

occurred in June of 2020, targeting the Japanese car manufacturer, Honda, and security researchers seemed to believe the SNAKE ransomware was involved.[161] The direct effect was the complete shutdown of several plants.[162] A cost analysis, even at the speculative level, would assess losses in the millions of dollars and this case deserves further investigation. This speculation is based on well-known cases, including those mentioned in this Article. Thus, while an unprepared company would lose millions of dollars due to a serious breach of security, an investment of upgrading its SCADA system would be approximately $50,000. For example, three years ago, the city of Union, South Carolina, awarded a contract for upgrading its water plant SCADA system for $44,700.[163] This cost would not include yearly updates and patches to the system. Nevertheless, this would be a reasonable expense to protect the organization.

An organization's cybersecurity strategy must also be designed to tackle—as early as possible—potential vulnerabilities. This strategy must reflect a defense-in-depth approach for implementation, continued monitoring of ongoing risk management, and for maintenance. There is no doubt that an organization's cybersecurity demands long-term solutions and financial resources allocated towards securing its networks. For these reasons, the solution to secure the modern SCADA organization should stay abreast of evolving standards. This recommendation incorporates the following suggestions:

- First, determine the ecosystem of the SCADA system security.
- Second, identify common threats.
- Third, identify common security vulnerabilities.
- Finally, concentrate in identifying and deploying the best practices delineated by industry standards, such as:
    - ISA99 – Industrial Automation and Control Systems Security /IEC 62443 series of standards;
    - The National Institute for Standards Technology (NIST) SP 800-82 – Guide to Industrial Control Systems Security

SECURITYWEEK (June 11, 2020), https://www.securityweek.com/honda-ransomware-confirms-findings-industrial-honeypot-research.

161 *Id.*

162 *Id*.

163 Charles Warner, *SCADA Upgrade to Cost $44,700*, UNION TIMES (Union, S.C.) (Aug. 21, 2017), https://www.uniondailytimes.com/features/lifestyle/12655/scada-upgrade-to-cost-44700.

standard;

- The North American Electric Reliability Council CIP series of standards;
- NISTIR 7628 (guidelines for smart grid cybersecurity).

CONCLUSION

The new space age is evolving in a world of clandestine online maneuvers which industry stakeholders will encounter within cyberspace conflicts. Executives must acknowledge the security needs and rising threats that plague the industry. Similarly situated organizations were confident that all precautions were taken, yet their lack of a modern strategy for their entire organization opened them up to disaster. Lack of planning cost these companies millions of dollars in losses and, most likely, millions of dollars in legal fees. The real answer to the protection of assets is to guarantee an appropriate modernization plan. Since the cyberthreat landscape continues to change, security risk management should be a continuous process. The desire to resolve the challenges associated with SCADA systems have concentrated in surveying the vulnerabilities, understanding these, and proposing a multi-prong solution. The challenges for SCADA are many, yet there is a commonality across the industries. As previously noted, the spear-phishing attacks on the Ukraine energy distribution companies demonstrated the need to have properly trained operators, which, in turn, would protect the human machine interface. For now, the greatest cyber threat may not be technological in nature, but instead political, and cyber operations exist within the legal gray area in between, where the organizations cybersecurity strategy, must be designed to tackle—as early as possible—potential vulnerabilities.