JENRS

Received: 12 January 2022, Accepted: 31 March 2022, Online: 12 April 2022

DOI: https://dx.doi.org/10.55708/js0104002

An Overview of Cyber Security Considerations and Vulnerabilities in Critical Infrastructure Systems and Potential Automated Mitigation - A Review

Roberto Mazzolin [1,*], Asad Madni [2]

[1] RHEA Group, Ottawa, Canada
[2] Samueli School of Engineering, UCLA, Los Angeles, California, USA

[*]Corresponding Author: Roberto Mazzolin, Email: r.mazzolin@rheagroup.com

ABSTRACT: Executive leadership in government, military and industry are faced with many difficult challenges when trying to understand the complex interaction of public and government security policies, the vulnerabilities in the wide array of key technologies supporting critical infrastructure upon which society is vitally dependent, and the identification of key cyber security trends that will need to be considered in the future. This invited paper discusses public policy issues related to the threat environment and provides a comprehensive description of the various cyber vulnerabilities and risks arising from a broad range of technologies supporting critical infrastructure and highlights key requirements and design principles desired from next generation automated defence capabilities. This document provides a unique review of key aspects related to these separate but interrelated subject areas that will hopefully provide greater context, background and clarity for senior decision makers responsible for shaping development agendas for their organizations.

KEYWORDS: Critical Infrastructure, Mitigation, Leadership

1. Introduction

Senior executive leadership in the government, military and industry communities are faced with an increasing degree of complexity when confronting the contemporary cyber security threat to the critical infrastructure supporting our societies vital systems that support not only essential systems but also government legitimacy and societal stability. The discussion related to potential approaches is made even more complex when considering the current challenging threats against the broad range of technologies that comprise our critical infrastructure and their specific vulnerabilities. The nature of this environment is such that traditional approaches to securing this environment are no longer adequate and potential solutions will need to look toward innovative applications of emerging technologies.

This paper is divided into three sections. The first section highlights public policy issues related to the threat environment and the need for critical infrastructure cyber defense in systems supporting societal resiliency under the following headings: The impact of Cyber, The Threat Environment, Policy, Societal Stability, Critical Infrastructure and Defence and Security. The second section provides an overview of the cyber risk across a broad range of critical infrastructure technologies supporting automated systems under the following headings; Cloud Computing, SCADA, Vehicular Environment. Mobile Computing, Unmanned Aerial Vehicles, Aviation, Space and Artificial Intelligence. Finally, it highlights some key principles desired from next generation automated defensive capabilities. These are treated under the following areas; Mitigation and Automated Defence, Automated Cyber Defence, Automated Defence in Software Defined Radio and Cognitive Radio Networks.

This invited journal paper expands upon an initial paper "A Survey of Contemporary Cyber Security Vulnerabilities and Potential Approaches to Automated Defence" presented at the IEEE Syscon 2020 Conference in Montreal, Quebec, Canada [1]. This paper updates and expands upon the original paper in a number of areas. It

provides greater detail in the treatment of public policy considerations that apply to critical infrastructures in addition to identifying and explaining the potential impact of vulnerabilities inherent in key technologies that underpin these systems. This document adds new contributions in the area of Artificial Intelligence and further develops discussion related to Cloud Computing. It further expands the treatment of cyber security issues relating to SCADA and vehicular and mobile computing technologies. Finally, it further expands upon the initial treatment of techniques related to automated defence supporting mitigation approaches and the application of security in the areas of software defined and cognitive radio technologies that increasingly form the basis for next generation wireless networks. As such, the document serves to provide a unique treatment of a broad range of policy, technology, and future developmental considerations to support executive leadership synthesis of this wide-ranging subject matter.

2. Policy considerations

The impact of Cyber; a double-edged sword in an automated environment – The West's decisive technology superiority holds the potential for its demise. As technology increasingly permeates the functionality provided by critical infrastructure that supports society, our personal lives, economy, defence and security is critically dependent upon the security of internet and connected technologies.

Since the early days of the internet in the 90s, manual approaches to operating critical infrastructure have been rapidly superseded by the adoption of advanced technology in the interest of speed, efficiency and low cost. This focus on flexibility and openness have been at the expense of security.

Our society has arrived at an inflection point where the dependence on technology is ubiquitous, the average millenial has grown up in an online culture and technically expert senior leaders are rare. This paper is an invited paper that expands upon the original paper "A Survey of Contemporary Cyber Security Vulnerabilities and Potential Approaches to Automated Defence" presented at the IEEE Syscon 2020 Conference in Montreal, Quebec, Canada [1]. This paper will examine the nature and import of the cyber threat to the automated systems that power our societies and suggest a way forward in the interest of ensuring the integrity of these systems.

The Threat Environment – The threat presents itself daily in a variety of forms at the geopolitical and economic levels. The collective aggregation of the variety of the many diverse from thousands of cyber attacks across the broad range of systems supporting critical infrastructure could serve to cause grave impact to western innovation and commerce without reaching the threshold of spurring meaningful government engagement and response [2]. The increasing international investment in cyber security and the creation of military Cyber Commands highlights the awakening of many nations to this threat and notable announcements by international leaders have identified the cyber threat among the most serious economic and global security challenges.

Policy – National and institutional ability to address the difficult challenges that encompass the broad domain of cyberspace technology, operations and security are further complicated by the legal and policy development environment that lags rapid technology advancement. Governments are developing an increasing appreciation of the fragility of the national infrastructure and the potential destructive effects of a cyber attack whose effect would be analogous to that of a conventional military attack, but difficult to attribute and more subdued and difficult to identify over an extended period of time. A former Chairman of the House Intelligence Committee, Mike Rogers, indicated that 95% of private networks are vulnerable and had already been penetrated, and introduced the Cyber Intelligence Sharing and Protection Act (CISPA) in November 2011. Further, cyber security expertise is in critically short supply, with the cited global shortage forecasted in 2020 according to the 2019 $(ISC)^2$ Cybersecurity Workforce Study, being 4.07 million cyber security professionals to adequately defend organizations. While efforts to recruit and develop qualified personnel continue, federal policy focused on ensuring privacy, the corporate culture of focusing on the bottom line and the defence and security communities' kinetic warfighting culture may resist supporting these programs.

Societal Stability – Modern democratic societies are confronted with significant challenges in efforts to confront systematic cyber conflict whose intent is institutional destabilization of a targetted state. To that end, information security activities such as assessments are required to develop coordinated, pre-event frameworks that ensure institutional stability, public trust, and limit challenges to the state. Such assessments can take the form of Model Based Simulation and Emulation and supporting exercises that replicate bespoke environments and enable the development of detailed tactics, techniques and procedures or "playbooks" to counter threats. Theories based on Dwight Waldo's theoretical work on nation state stability dependencies depending on factors of legitimacy, Authority, Institutional Knowledge, Bureaucratic Control, and Confidence establish the criteria upon which societies may be destabilized and crippled by a coordinated cyber campaign to reduce institutional entropy [3]. Emerging societal cyberwarfare theories advocate the development of defence strategies in anticipation of massive state actor initiated automated attacks to mitigate risk for societal

system compromise. An important aspect relates to the informational aspect of cyber security, which if manipulated effectively, impacts the confidence and trust that a population has in its government and societal systems. Recent news coverage of impacts on electoral integrity serve as important examples of the scope of potential impact.

Critical Infrastructure - When considering national security, one must recognize the intrinsic relationship between traditional concepts of physical security and economic security. To that end, given societal dependence on the Internet of Things (IOT), and activities related to Health and Insurance, Banking, Financial and Personal Privacy interests, attacks against infrastructure supporting such areas would result in the potential for devastating cyber security events that could threaten our way of life. Critical infrastructure includes technology-based systems and services that provide critical functionality to ensure the security, economic prosperity, and social well-being of the public. Examples of such systems include transportation, communications, water, energy, finance, health, agriculture and government services among others. This potential threat to these areas is further accentuated by the many complex logical, physical and geographic interdependencies and collections of interacting components. As computer systems become more integrated, the distinction between security and safety decreases.

Defence and Security – Militaries serve as extensions of national power and cyber now represents a central element of the contemporary military art. Armed forces have evolved the nature of their operations as we see the establishment of Cyber and Space Commands in most countries. Cyber security is a central consideration in modern military operations given the dependency of command and control, weapon systems, precision timing, intelligence, surveillance and reconnaissance and supporting space systems on networking and automated processing technology. To this end, as the commercial environment has led the development of technology over the past 30 years, this has driven the impetus for enhanced military/industry cooperation. This aligns to the significantly increased emphasis placed on cyber and data protection in the military environment, and cybersecurity research has increased dramatically since 2011. Significant effort has been devoted to the investigation of offensive capabilities that are convergent with the evolving threat to address military mission specific requirements. One example of such an incident is the example of possible Asian military hackers that had attacked two US satellites at least 4 times between 2007 and 2008. Russian cyber attacks, such as those launched against Georgia and the Ukrainian power grid in conjunction with physical proxy operations illustrate the new nature of hybrid operations that are conducted just below the threshold that would normally trigger political or military response on the part of the international community. This potential threat applies to broader national critical infrastructure upon which many military installations and associated communities depend.

When considering the national industry base as a critical element supporting national economic security, such threats, particularly associated with the theft of data from defence contractors and associated subcontractors warn that the West's technical leadership and strategic military advantage are at risk with the ensuing compromise of related national security interests. In this instance, advanced persistent threats (APTs) involving sophisticated infiltration techniques that are beyond the ability of most government agencies and businesses to counter are particularly relevant. Such techniques can be countered through a combination of defence in depth and detection capabilities along with the development of response and recovery plans and security and awareness training.

3. Critical infrastructure technologies

Cloud Computing – Security has been a critical consideration in decisions surrounding the movement of critical institutional data to off site premises. To that end, cloud technology and associated security measures have evolved and new approaches are being used to ensure that data is secured. Recent reports from market research predict that the cloud security market will expand at an annual growth rate of approximately 49% around the globe, thereby highlighting the importance of this area. This growth is driven by increased collaboration between cloud service providers and security solution vendors, along with the perceived reduced ownership costs. Here cloud-based security solutions effectively reduce operational costs to an organization as the maintenance, operation and infrastructure costs and associated risk are handled by a third party. Challenges to this model exist as many new vendors are entering the open source security software market. The clear emphasis within this community is placed on web-based safeguards.

Key emerging trends include greater reliance on a hybrid cloud where data is kept local but applications are provided by multi-provider public cloud infrastructures. There is greater emphasis on protection of data at rest, notwithstanding the traditional focus of securing data in transit. This is achieved through the use of encryption and data centric security in light of the increasingly malicious environment and advanced persistent threats that target this environment. Additional restrictions arise from the imposition of data residency and sovereignty laws as a result of nation state surveillance and related privacy considerations and regulations. To address this, tokenization techniques which substitute critical information with fewer sensitive substitutes are used to counter unauthorized access and data surveillance.

Malware threats and hactivism, given their capability to launch large scale denial of service attacks and wipe out data are driving greater emphasis on server security. The increasing use of an increasing variety of devices such as smartphones, internet connected printers, smart televisions, DVD players, and peripheral devices, mandates the employment of increasingly comprehensive security strategies to protect their services. Multi-Factor authentication is driven by the weakness of traditional username and password approaches. Such techniques involve the increasing use of single use codes that are transmitted to separate users' devices and accounts to protect very sensitive information, and is increasingly being used in financial and healthcare industries. Finally, breach insurance has become an increasing trend. As the reality of "not a matter of if, but when" compromises will occur, enterprises are taking a more pragmatic approach to cloud security. This is forcing enterprises to consider adoption of cloud insurance along with the application of security measures to combat risks.

Supervisory Control and Data Acquisition (SCADA) – Smart city initiatives which depend on highly interconnected traffic control, building automation, electrical grids, communications, water, HVAC, video/security, systems are subject to security threats to architectures in light of the many vulnerabilities. The significant security concerns relate to principal vulnerabilities related to control system environments that are present in a number of areas. As communication systems increasingly link smart grids and associated systems, the corresponding increase in access points translates into greater surface exposure and complexity. Further, given that smart grid systems increasingly use similar commercial service providers and computing technologies, a greater proportion of the infrastructure will be exposed to similar vulnerabilities. Additional risk is incurred as increased automation further generates, gathers and processes data in new ways as smart grid technologies embrace and automate new functions.

There is a requirement to reconsider SCADA threat models to represent a broader security context and develop more unified frameworks that coalesce security and safety risk. Intelligent automated tools and techniques specific to SCADA systems are being developed to enable more progressive methods of risk management so as to require minimal human intervention to control processes and provide defence in depth.

The perception that SCADA systems are difficult to attack is contrary to reality as many tools openly exist on the Internet, such as the Shodan computer internet search engine that provides a search engine for network devices such as routers, servers and load balancers and provides detailed information on potential targets including authentication techniques that in many instances are not updated. SCADA architectures typically support a variety of components that sense process variables and operate equipment connected to programmable logic and process automation controllers, remote terminal units, intelligent electronic devices. These local processors often communicate over various ranges to host computers using a variety of legacy wireline connections such as leased dial up lines, ADSL, cable and fibre in addition to wireless communications such as private radio, cellular, spread spectrum, WLAN or satellite networks. These connect to host computers that serve as a central point for monitoring and control of overall system processes and databases and display statistical control information and reports.

SCADA architectures primarily TCP/IP, UDP and other IP based protocols as well as proprietary industry protocols like Modbus TCP and Modbus over TCP or UDP. Architectural decisions are often driven by practical considerations related to existing and available communications infrastructure, particularly at remote sites, signalling protocols, installation budgets and the ability to meet future needs. Such systems typically comprise hundreds of thousands of input/output channels at speeds of up to 1Mb/s. Hardware and software used in SCADA systems has evolved over the decades with a greater dependence on personal computers and TCP/IP which in turn have become of increased concern due to terrorist threats. Internet and mobile connectivity architectures have evolved, and as such, security concerns have led to the introduction of new features such as encryption and dedicated access controls. Although systems historically were isolated from the Internet, notwithstanding the limited connectivity, these systems are still vulnerable to both external and internal threats through the exploitation of vulnerabilities within operating systems, data storage software as well as custom and vendor software, databases and applications. Commercial standardization is creating pressure to use open market COTS technologies that rely upon complex software applications involving time criticality, embedded systems, distributed, intelligent, fault tolerant, distributed and heterogeneous systems. Notwithstanding the greater awareness of terrorist related risks and hostile state based attacks, such threats are often misunderstood or underestimated. Further architectural challenges relate to an increased reliance on web technologies such as ActiveX, Java and OPC to support internal communications between client and server modules.

Web based applications are increasingly targetted by automated cyber attacks as web development has emerged as a key software development platform and secure web-based software development remains immature. Consequently, Web application vulnerabilities are still exploited by highly sophisticated Web worms. Further, the common software environment upon which all SCADA systems are developed present similar vulnerabilities which may be more easily and widely

exploited. Although UNIX based systems have served as the historical standard, they have now been displaced by Linux and Windows based operating systems which contain a greater range of vulnerabilities that may be more readily exploited over time. A further cultural challenge compounding such vulnerabilities relates to the expectation on the part of plant operators that software should run for extended periods of time without oversight, monitoring, modification or patching even though SCADA vendors annually release enhanced versions based on new technologies and to compete for market opportunities. The vulnerabilities associated with Linux and Windows based operating systems centre around the larger number of lines of code. Typically cited studies of software reliability estimates that Linux kernels have more than 15000 bugs for 2.5 million lines of code, whereas Windows has a proportionally larger number of bugs commensurate with its increased size. As operating system bugs pose higher risk than those in application programs, a serious concern arises given the high concentration of Windows in computers supporting SCADA environments. In this case, the principal vectors for exploitation are software design, operations and human interfaces.

A cultural element exists related to challenges in software intensive control system design given that development requires both Control Engineers and Software Programmers, who have different perspectives and working practices, and frequently lack the overarching picture for the overall responsibility associated with ensuring enterprise level security. The unique nature of the vulnerabilities that exist in the SCADA environment that may not be modeled or understood by these practitioners creates further challenges. As there are comparatively few global SCADA system providers, the commonality of technology between the various SCADA systems, the often inter-related corporate systems that they support, and the Internet, represent a principal cause of further significant risk.

Risk management and vulnerability of SCADA systems is a relatively new area of development as the practice as the CERT and NIST began publishing SCADA vulnerabilities in 2005. Companies have been reticent to divulge vulnerabilities and compromises of their systems and few standards exist to provide guidance. Key issues that require attention include critical path protection, safety policies and procedures, knowledge management, system development skills in both control system engineering and software development for distributed control systems. Further effort is required in the areas of enhanced security feature development for sensor networks, micro-kernal architecture operating systems and increased software security features.

Additional system design concerns relate to adherence to accepted standards during the requirements and development phases of the system lifecycle and integration of new technologies. Further security architecture and associated policy recommendations include the implementation of more rigorous security for corporate and enterprise network connections to the internet, a complementary security zone architecture to isolate critical networks, and the addition of multiple screened subnets or demilitarized zones with no transit traffic. Further, architectural solutions should permit no connections between security zones that are not firewall protected and that inventories of remote access paths entering the architecture be taken to ensure that no connections bypass a firewall infrastructure. Finally, any remote access should be through a VPN connection with strong access controls. Additional policy measures include greater innovative risk management approaches using adaptive, proactive discovery solutions that focus on identifying and mitigating both natural and man-made disruptions through various vectors such as human error, sabotage and terrorism.

Vehicular Environment – Many cyber defence concerns in the vehicular environment across the spectrum of manually operated to fully automated controlled vehicles. The complexity arises from the many electronic control units (ECUs), typically numbering from 30-100, more than 100 actuators, 4000 signals, and typically between 70-100 sensors that are interfaced to both wired and wireless external interfaces for sensors receiving input from accelerometers, cameras, radars, sonars, temperature and rain sensors to control the vital vehicle functions such as navigation, steering and braking. When combined, over 25 Gbytes of data is produced per hour. Consequently, key safety features are vitally reliant upon the ability of these ECUs to communicate with one another. Attacks against such systems may be launched via wireless means by accessing the vehicle telematics system that is responsible for managing an impressive amount of information and typically contain more than 100 million lines of code. Uconnect, an entertainment system, is one example of such a protocol that interfaces to the internet for both GPS navigation and entertainment.

Generally, vehicle based cyberattacks occur in three phases; first by gaining access to the vehicles' ECU, followed by injection of malware into the ECU, and finally activation of the code. Generally, such an attack is complex and expensive as the nature of egress must be gained via direct and indirect physical connections as well as short and long range wireless connections in order to gain full control over a vehicles automated functions. Potential avenues to mitigation involves the analysis of the Controller Area Network (CAN) packet traffic over extended time periods to detect anomalous traffic and disconnect the associated automated functionality. The CAN is the preferred bus for in-vehicle communications

to exchange data as it is reliable in noisy electromagnetic environments. This is accomplished by collecting data streams to detect offending code and associated IP addresses. Additionally, WiFi and Bluetooth signal blockers may be used to protect against untrusted wireless connections near the vehicle. Commercial 3G/4G telematics and IEEE 802.11p protocols are used to provide general connectivity and inter vehicle communications as major software developers seek to gain a strong hold on the vehicle market space. This exposes vehicles to the wide array of Internet of Everything (IoT) threats most commonly experienced on more traditional networks. Vehicles currently rely on multiple of ECUs with processing power in the order of 100MB to manage a variety of processes and peripherals connected via Bluetooth and proprietary manufacturer systems like the GM OnStar system. The simple, low level CAN bus supports data transfer at speeds ranging from 125kbp/s - 1MB/s. The CANbus standard is also used in the aerospace and industrial automation sectors.

The inherent weakness with this protocol is that it does not implement any security features such as sender identification and authentication, thereby facilitating spoofing. Therefore all security functionality must be provided by higher level applications. CAN bus hacking can be achieved by simple chipsets to bypass encryption within the vehicle prior to reading and writing data from a vehicles ECU memory. It can then be wirelessly triggered to launch a programmed attack. Given that all vehicular systems are connected to the CAN Bus, automated wireless access typically involves targeting power door locks, MP3 via iPod, infecting USBs and discs either directly or remotely through interconnected devices and OBD-II diagnostic ports. The dedicated OBD-II port is the most common avenue of access and dedicated Windows diagnostic scan tools are readily available that are designed to both gather information and program ECUs, which can serve as a ready access for malevolent actors. Short range devices include WiFi, Bluetooth, WiFi, wireless key fobs, keyless entry, tire pressure monitoring and RFID systems. Depending on the frequency band used, these may be effectively targeted by placing a wireless transmitter within 5-300 metres from the vehicle. For example, as vehicles increasingly employ Bluetooth to enable hands free calling, a compromised smartphone can be used as an access point into the vehicles telematics environment and enable access to critical vehicle ECUs.

A significant development is the increasing adoption of the SAR J2534 Passthru standard. This is a Windows based Data Definition Language application programming interface that can communicate over both wireless and ethernet with the CAN bus and facilitate injection of malicious binary code via a shell injection interface to control a vehicles' programming. Consequently, a PassThru device compromise via WiFi or Ethernet connectivity may be used to affect multiple vehicles via subsequent connections to activate viruses on specific dates or when a specific event or vehicle condition is met. Of further note, electric cars may also be subject to compromise through connectivity via charging infrastructure.

The abundance of programs developed by third parties for the mobile device market has created a demand for vehicle manufacturers to rapidly offer infotainment capabilities which can download software. Longer range broadcast receivers that provide access to GPS, Digital Radio, Satellite Radio, Radio Data Systems and Traffic Message Channel signals are now integrated into increasingly complex vehicle telematic systems. GM OnStar, Ford Sync, Lexus Enform, Toyota Safety Connect, Mercedes Mbrace, and BMW Assist all connect via data and 3/4/5G cellular voice and SMS data networks to internet based location and navigation, crash reporting, diagnostics, mechanical fault alerts, anti theft remote tracking and disablement, hands free data access convenience and safety. Again, connectivity to vehicle telematics enables CAN bus access and the opportunity to exploit the vulnerabilities of these well understood commercial protocols. Although vehicle hacking presents significant challenges, the interactive nature of traditional computer exploits would be more difficult to effect given the nature of vehicular infrastructure. Therefore, the most likely scenarios for such attacks would be related to serious crimes such as erasing information from vehicular event data recorders and theft, and targeted attacks against very high value targets, kidnapping and assassination.

Mobile Computing – The Google's Android, Apple's iOS and RIM Blackberry have accounted for the vast majority of the mobile device market within the US. This has driven access to portals, productivity tools and back end transactional and reporting systems to provide convenience, functionality and efficiency for the commercial workforce. This presents significant data security issues as users, when choosing a smartphone, generally do not consider the mobile platform that their company supports. Although Blackberry had afforded greater security, iPhone and Android devices have been targeted by increasing malware as criminals saw greater egress to these environments. Relatively few users appear sensitive to the threats as the installation of security applications onto smartphones is comparatively low, thereby placing the onus on companies to protect their networks.

Two major areas that impact mobile security involve application markets and file synching and transfer services. Given the demand for easily downloadable applications and the current immature state of security development in this market, industry will need to more closely examine the application review process or create increasingly proprietary application stores to counter

irresponsible downloading of applications. Here the significant volume of data breaches result from data that is constantly moving between host storage sites which is either lost or intercepted in transit. Mitigation approaches include the use of encrypted virtual private networks through centrally managed platforms to ensure that the mobile device environment maintains a security posture commensurate with that of enterprise desktops and servers. This environment however, can still be infected through the importation of infected applications. Key enterprise policy governance regarding all connected devices should focus on greater centralized mobile device management, strong access governance through password and two factor` authentication. An additional step should involve implementation of mobile application software to support the protection of endpoints and enable network administrators to handle increasingly sophisticated threats.

Unmanned Aerial Vehicles (UAVs) – The rapid increase in use of UAVs and drones supporting first responder, military and commercial civilian environments has generated an increased emhphasis on security. A notable event demonstrating both the vulnerability of previously believed sophisticated and secure systems as well as national capacity and intent involved the 2011 Iranian cyber attack that led to the capture of a US military UAV in northeastern Iran. Key vulnerabilities impacting UAVs arise from the use of autopilot components taken from larger aviation applications. These include GPS, magnetometers, inertial measurement units (IMUs), actuators, manual controls and associated payload technologies such as video, radio relay and telemetry links. Magnetometers and IMUs which receive onboard platform sensor input, can cause crashes if given wrong information. Actuators are managed by information from main processing boards that also derive data from sensors and pre-programmed hardware and firmware commands are subject to denial of service from malicious data injection attacks. Wireless spoofing attacks have been well demonstrated and traditional approaches to ensure signal integrity against sophisticated attacks are inadequate. Spoofing of GPS, video feeds and Automatic Dependent Surveillance-Broadcast (ADS-B) devices can also lead to complete loss of platform control. The pervasive IEEE 802.xx and WIFI protocols in the 925 MHz, 2.4 and 5 GHz frequency bands provide a ready environment for hacking.

There are a number of readily available applications such as SkyGrabber, which can receive commercial satellite feeds, SkyJack, which enables the control of multiple drone, and Snoopy, which is a capability that enables distributed WIFI, RFID. 802.11 tracking and profiling. All these can be employed to monitor and perform unauthorized control over UAV functions in the absence of radio frequency link encryption. Given the obvious challenges associated with the employment of encryption, particularly in sensitive government and military environments, potential approaches to mitigation could involve the use of software to identify abnormalities and counter data injection attacks against UAV system components and correlate with other on-board sensors to recognize and rationalize incongruities.

Ground stations are subject to vulnerabilities associated with smart device applications that are used to operate and control UAVs. The wide range of malware that impact traditional networks can also be used to penetrate and exploit UAV systems. For example, key logger software has been detected onboard UAVs as well as in associated ground station infrastructures despite efforts to segregate such mission specific networks from the internet. In this instance, effective mitigation measures should include the strong management of smart devices and associated software applications to ensure the secure download and use of applications. Additional threats to ground station capabilities involve hardware based attacks against USBs that facilitate surveillance, traffic flooding and cause battery exhaustion. The reliance on Android based mobile device operating systems that provide a familiar PC based environment facilitates common software based attacks such as botnets, trojans, key loggers, rootkits and worms. Such embedded malware can be used to gather sensitive information and gain control of the infrastructure and disrupt operations. The implementation of encryption, authentication, firewalls and development measures such as fuzz testing to identify and counter security vulnerabilities, particularly malware in foreign sourced hardware and software is effective, however, there is no guarantee that testing can detect all malware, particularly bespoke code targeting specific capabilities.

Aviation – Commercial airline incidents in recent years have generated awareness regarding the potential for penetration of aircraft and the compromise of pilot control over vital on-board systems. Aircraft infrastructure is comprised of a complex array of separate systems supporting specific functions that are mediated by an over-arching software component that can be compromised through corrupted traffic in the various sub-components. Topical theories highlight potential vulnerabilities to wireless radio signals transmitted by small devices or platform based attacks against in-flight entertainment systems. There is a challenge in dealing with radio frequency based vulnerabilities given the requirement for various transponders, cockpit radios and Aircraft Communications Addressing and Reporting System (ACARS) to exchange status information with air traffic control.

As it regards the aircraft data bus, access to critical platform and data networks supporting aircraft control can be achieved gained via connections between passenger service computer network using USB ports and Ethernet. Android based hacks against the Flight Management System (FMS) have been demonstrated by

monitoring the systems communications and injecting bespoke code to modify navigations parameters and ADS-B and ACARS systems. A further vulnerability relates to the emergency intervention system that enables a ground based remote operator to land an aircraft using the autopilot.

NextGen navigation systems employ GPS data instead of traditional radar to track aircraft movement. Currently, the positioning information exchanged between aircraft and ground control systems are unencrypted and communication is established without mutual authentication. One potential attack scenario against the navigation system involves the injection multiple spoofed aircraft position inputs to overwhelm air traffic control and corrupt the position, location, direction and velocity data of other aircraft provided to pilots. Further navigation based attacks can be launched through the use of radio frequency jamming against radar by injecting false returns or noise and repeater based techniques to disrupt radar receivers that are designed to receive highly concentrated energy transmissions. Such jamming and flooding "denial of service" techniques against ground based radars can result in the loss of critical messages which could drive the emergency adoption of less accurate and inefficient surveillance and control mechanisms. This would cause compromise of surveillance and collision avoidance systems with disastrous consequences in dense traffic environments near major urban centres. In light of such vulnerabilities, the development of aircraft and navigation system software and hardware integrity standards for the aviation industry represent imperative elements of air worthiness standards to counter an increasing cyber threat.

Space – Virtually all earth-based critical infrastructure have some dependency on space based capabilities. The 2014 hacking of a US NOAA weather satellite forced the associated Satellite Data Information System offline, preventing the dissemination of forecasting data to international weather agencies for 48 hours. Cyber threats against space assets involve tracking and monitoring satellite transmissions along with electronic attacks against satellites and related services at ground segments, associated communication links. Ground segments that provide telemetry, communications, tracking and command of space nodes and launch mission functions can easily attacked, either electronically or physically, and result in disruption, degradation and destruction of the space capability.

Electronic attack involves jamming uplink and downlink signals to jam or spoof information through the satellite. Uplink jamming can disrupt command and payload links and imparts a broad based effect as all recipients of the satellite's transmission are affected. Downlink jamming, is primarily oriented at preventing selected users from receiving a satellites broadcasts and navigation signals and is achieved by transmitting radio frequency transmissions with enough power to overcome the satellites downlink signal. Smart jamming differs from traditional broadband or traditional techniques as it simulates or spoofs the targeted satellite signal to furnish targeted users with erroneous data. This technique has a more local effect, typically limited to tens or hundreds of kilometers depending on downlink signal strength, as it requires the jammer to operate from line of sight, however, it is potentially more effective as lower power jamming transmitters may be employed. As satellite telemetry contains information related to system mission, health and status, a successful downlink attack will disrupt essential information flow and potentially have more immediate effect. Spoofing involves a variety of techniques to capture, alter and retransmit transmissions to mislead intended recipients. Other threats against satellite systems include kinetic, directed energy (laser, particle beam and radio frequency weapons) and nuclear effects.

Artificial Intelligence – As an enabling technology, Artificial intelligence (AI) technology is of particular relevance as it will comprise a foundational element of any automated cyber defence system. It has evolved from its origins in the 1950s to modern machine learning, expert systems and neural networks that seek to replicate the functioning of the human brain. AI now exceeds the performance of the human brain in many activities once considered too complex for any automated system to master. The application of AI is currently making its greatest impact in the areas of threat detection and the shaping and execution of cyber defence work flows. Traditional approaches to threat detection were based on software code that involved pattern matching programs that would search for signatures or specific patterns that would provide potential indicators of compromise. The application of AI now goes beyond the detection of individual signatures to detection of malicious behaviour such as phishing, ransomeware and compromising applications on mobile devices and networks. This is complementary to the earlier signature based detection approaches, however, in order to "teach" AI systems, there is a reliance on the development of large databases of threat artifacts that have been accumulated over time. Although focused signatures may be developed and deployed quickly, AI "learning" requires considerably more time.

Consequently, in the near term, AI is largely being deployed in more narrowly defined cyber defence applications supporting signature detection. However, future AI development will need to focus to a greater extent toward complementing the human operator in synthesizing the wider range of actions occurring on a network. This analytical and decision support functionality will enable more sophisticated situational awareness and the ability to posture more sophisticated approaches to defence, for example the detection and understanding of heuristic behaviour on a network as opposed to responding to individual instantiations of threats. Further, given the increasing complexity of

malicious code, there is a role for AI to assist defence analysts and operators to not only detect such code, but also understand its capabilities so as to enable more adequate response.

Although predictions of the pace of AI development have been mixed, current trends suggest the potential for human-level cognition or even artificial superintelligence could be a realisable in the nearer term, with some predictions of an AI explosion by 2045 [4], greatly enhancing the capacity of the human brain. When considering the potential offensive and defensive actions that may be realized on networks supporting critical infrastructure, it is clear that such technology could afford decisive strategic advantage in political, economic and military environments. As such, this creates the impetus behind focused efforts on the part of leading nations in the development of AI supporting cyber security.

A corollary to this when considering the application of AI to sensitive critical infrastructure based applications given their ley impacts on society, is the challenge of ensuring the processes supporting complex AI systems is understandable to humans. This involves ensuring that input data, algorithms and associated results are clear and readily interpretable. The acceptance of AI systems will be fundamentally dependent on enhanced transparency, most notably in mission-critical applications impacting life and death.

4. Future automated defence capabilities

Mitigation and Automated Defence – There are a variety of approaches to resolving the myriad of challenges cited above arising from rapid technology advancements, however the nature of various systems operating in disparate environments prevents a single uniform approach to addressing the plethora of potential attack vectors. Current antivirus systems represent only a partial solution and fail to maintain pace with the rapidly evolving malicious software environment. A wide range of malicious software variants are readily available on the dark web for less than tens of thousands of dollars, and in many instances they easily bypass commercially produced antivirus protection products. The isolation of networks also do not ensure security as the level of sophistication associated with weaponized software by state based entities to penetrate networks can readily exploit the inevitable security lapses that exist in organizations. One classic example is the Stuxnet virus that exploited USB devices to gain access to critical SCADA infrastructure that had been thought to be on a physically isolated network and impervious to penetration.

Automated Cyber Defence – Traditional approaches to institutional cyber security have involved providing perimeter security at border entry points and static policy enforcement. The increasing openness of enterprise network environments in light of Covid driven remote work requirements has introduced greater risk given the broadened aperture and more fragile network posture. Once having penetrated the established network perimeter, an intruder will have greater freedom to move about within the network. To maintain pace with this threat, concepts surrounding the protection of networks must evolve to one where adaptive responses play a principal role and multiple defensive layers must be established that permeate the entire network environment so as to avoid reliance on a single defensive boundary.

Current research and development efforts are aggressively pursuing adaptive security methods by developing new measures that are broader and deeper in scope, and employ increasingly intelligent and effective artificial intelligence driven defence techniques in addition to pressing security perimeters inward. One example of such an approach is the shift from firewalls on network perimeters to managed firewalls that are distributed on individual hosts within the network and embedding application specific filtering throughout the application stack.

Potential methodologies in this vein involve the implementation of managed execution environments that provide automated responses to incidents to prevent the protected applications and environments from future attacks of the same or analogous incursions. As incursions and associated effects are detected, the intended response is provided through the application of the specific networks' input/output mediation policy so that the network may then restored to pre incursion state. Such a response in turn supports the development of further policy adaptation via the application of decision tree classifiers, which may be reinforced by fuzzy experiments to develop a more precise model of the specific incursion. The associated responses can then be implemented as secondary policy patches. Such a protocol enables the blocking of future events that are similar in content, signature or character. Such approaches can provide quasi real-time responses to incursions that contain detectable system conditions. These depend upon software engineering of self improving software systems that integrate a number of complementary technologies such as decision tree classifier generation, deep execution introspection and targeted fuzz testing under the auspices of a managed execution environment. Further development is needed to optimize the balance between speed and precision in protocol adaptation and associated generalized signature combinations that are tailored to specific applications and timing dependencies.

The implementation of successful automated adaptive cyber defence strategies must be effective in mitigating threats and be enforceable under specific network states and capabilities. Successful active cyber defence requires synchronized, real time capabilities to discover, analyze and defend against threats and vulnerabilities. The scope of these measures must be capable of spanning a highly diverse range of network monitoring and management activities to detect attacks and safely mitigate them. To do so, multiple network configurations are required. For

example the migration of key services from one server to another which involves a high degree of complexity. Consequently, the key properties of any successful active cyber defence strategy are consistency, enforceability and effectiveness. Consistency ensures that the sequence of configurations avoid mutual contradiction. Enforceability relates to the ability of the network to reconfigure active cyber defence strategies without incurring violations arising from misconfigurations or resource limitations, and effectiveness means that the desired effect is delivered, either through target disruption or neutralization [5].

As cyber attacks against enterprise and critical infrastructure increase in frequency and impact, there is a heightened appreciation for the merit of a persistent presence on networks. Consequently, active cyber defence to provide automated, adaptive, steerable responses is developing in importance. There are a number of approaches such as network layer solutions that use multiple behavioural models to invoke different routing of traffic through a core network. To achieve this, several conditions must be in place. First, the detection of behaviour that is inconsistent with a users past serves as a proxy for compromised systems or credentials, but renders high false positive rates. Secondly, the automatic redirection of future traffic from a potentially compromised system must provide a graded response that balances the cost of false positives against the risk of allowing the potentially malicious behaviour to continue. These conditions enable the development of a framework to link real-time situational awareness technologies to automated steerable responses that can provide decision support to human operators.

Traditional network defence in depth techniques afford attackers an asymmetric advantage as they permit free movement and propogation about the network once access is gained through the exploitation of credentials and access permissions of valid users. These techniques also fail to identify indirectly observable behaviours such as purpose, time on target and sequences of specific actions such as access attempts. Consequently, many current defences prove inadequate as they typically employ signature-based attributes as opposed to distinguishing between normal and abnormal behaviour such as goals, capability and sequence of action. Further, enterprise organizations often fail to apply appropriate isolation given the technical difficulty, related inefficiencies and impact on productivity. One approach involves adaptive partial quarantines to impede or isolate attackers that may appear to be behaving normally, without impacting the activities of valid users and defenders. Such strategies involve automatic, behaviour triggered, adaptive quarantines to quickly and selectively change access to defender resources without interfering with the normal work of valid users and hosts. This addresses the problem of isolating malicious users and systems without negatively impacting the mission critical work of valid users. Such a capability leverages two well developed areas of research, namely behaviour analysis and containment [6].

A further area of activity involves the use of cognitive informatics to counter distributed denial of service attacks against critical infrastructure and domestic defences. Such attacks are simple to initiate as malware is readily available and easy to implant by multiple malevolent users. One ongoing trend is the use of mobile phone botnets to launch attacks and it is expected that major State based actors have the capacity to perform DDOS attacks against other nations' critical infrastructure. The automated defence of such systems may be facilitated through cognitive learning. This is an emerging area of research related to Cognitive Radio Networks. Potential cognitive based design guidelines and algorithms focus on all OSI network, transport and application layers. Information technology artifacts may then be created, evaluated, improved and redesigned until new knowledge is acquired. In such an approach, Cognitive engines require large amounts of information to drive engine development. The development of such environments rely on focused areas of work such as the separation of authenticated and unauthenticated services, the placement of proxies between clients and servers, and micro segmentation of clients during distributed denial of service attacks.

Automated Defence in Software Defined Radio and Cognitive Radio Networks – Clearly, Software Defined Radio (SDR) and Cognitive Radio Networks introduce entirely new classes of security threats [7]. Such classes comprise sniffing, spoofing, jamming, side channel, replay, reinjection and flooding attacks. Sniffing involves monitoring traffic on a communication channel, either encrypted or unencrypted, to obtain confidential information which could include the identities of the sender and receiver in addition to traffic control parameters that could enable a deeper understanding of the network infrastructure.

Spoofing involves the transmission of signals, whose parameters could be seen as valid and representing an authorized user. The intent is to send erroneous information, inject malicious code or gain control of the communication channel. Jamming is ostensibly a denial of service attack that degrades or disrupts valid communications from occurring on a channel and effectively blocks accurate reception of messages by authorized users. Side channel attacks involve collecting and analyzing information related to physical parameters such as electromagnetic radiation from integrated circuits as they are processing. This non-invasive technique is used to breach confidentiality and is typically used to carry out RFID attacks against credit cards in wallets. Replay involves copying a legitimate message and retransmitting it, thereby causing confusion an corruption of legitimate traffic. It can also be used in support of broader flooding attacks that impact the availability and

integrity of a communications channel. Reinjection is similar to a replay attack; however, the message is modified before retransmission in order to compromise the channel integrity and confidentiality. Finally, flooding involves sending such a large volume of messages such that the receiving terminal is overwhelmed and cannot process all of them, thereby compromising the availability and integrity of the communication channel.

SDR allows devices to adapt quickly and function optimally in changing network environments as various attacks are discovered. Further, the Internet of Things imposes the additional challenge of an explosion of sensors which lack the appropriate protections for confidentiality, integrity and availability. The resolution of such a challenge is dependent upon a multi-layered approach. Potential techniques involve the identification of source IP addresses and the use of big data to increase scalability to enable deeper analysis of counter distributed denial of service correlation metrics and analyze which organizations have been attacked using the same IP addresses. Other approaches involve coordinated concealment and proxy solutions to defend Web services. A weakness with this approach is that workflow is sent to a proxy where the service IP address must still be protected against the malevolent client.

When deploying SDR in mobile network environments, a supporting configuration model supporting users and services must be developed that continuously and dynamically adapts its configuration in order to immediately detect malicious sources. Here, a number of significant challenges exist for open and random access environments. The instance of unlicensed secondary users accessing channels when not being used by licenced primary users may be addressed via a-priori authentication. IP tracking based on packet marking and recognition technology to detect attacking packets are main approaches against distributed denial of service attacks and facilitate tracking. Further methods involve implementation of jamming resistant control channels.

Another counter distributed denial of service approach in cognitive radio networks involves furnishing the cognitive engine with information that can identify specific authenticated clients that are potential threats. These can be repeatedly broken down into much smaller groups until one client remains and enable the cognitive engine to rapidly and precisely identify a specific malicious client and remove them from a trusted list and protect servers supporting authenticated clients [8]. Currently large enterprise networks composed of continuously changing networked devices are routinely subject to targeted cyber attacks. Typically, a high volume of information related to attacks reside in various locations and remain unexamined until after attackers have achieved their objectives. Future cyber information management platforms will need to simplify cyber event data that is stored in the many recesses of distributed networks within hours and minutes as opposed to the months currently taken. Most current approaches to automated and operator assisted cyber defence are inadequate in defending against targeted cyber attacks because they focus on a limited number of aggregated one-dimensional characteristics across a number of devices and they are not able to cover all the network devices and observables resident on those devices. They further lack the ability to express and identify the deeper semantic required to identify targeted attacks among the vast multitude of low-level network activity. Progressive solutions will need to address these issues by being able to automatically detect network devices and develop metadata indices of information related to network activity and decompose and federate semantic queries to devices instead of extracting and aggregating information in central stores [9]. These integrated results will then need to be presented in the form of an established ontology.

Such solutions would facilitate information management and eliminate inefficient manual processes by enabling access to all network related data sources via federated query interfaces that leverage new web ontology, semantic query and cyber defence languages and return query results in an integrated, semantically meaningful and immediately useful manner. The intent is for intricate activity patterns to be identified within the network regardless of the type of device, operating system and location of logs. Cyber defenders would then be able to focus on the forensic analysis of data without being burdened by the encumbrance of managing and executing the activities required to laboriously collect data and process it.

From an overall system security perspective, the system must have the ability to function in a contested network environment. In so doing, there are a number of major features that it must possess. All sources of data in the environment must be accessible through well defined languages and interfaces. Additionally, there is a requirement for minimal network loading through scalable distributed architectures to deal with large, complex networks. Further, data must be retained at the network edge through federated access to observables. Finally, coverage over both legacy and new devices and associated intelligent information extraction needs to be provided.

Current commercial offerings focus on high volume commodity technologies marketed to commercial and government organizations that face attacks from broad set targets. Consequently, these capabilities are inadequate in identifying the necessary cyber observables to successfully counter targeted attacks [10].

5. Conclusion

The contemporary threat permeates itself across a variety of technology areas supporting societal critical infrastructure; each with their own particular characteristics in light of the nature of technology

implementation in these environments. Given the pervasiveness of contemporary information technology in support of critical societal infrastructure supporting the broader national economic and security interests, a significantly increased role exists for cyber and data protection. Of particular note are advanced persistent threats that take advantage of sophisticated infiltration techniques that most government agencies and businesses cannot counter collectively. However, if addressed individually, these techniques can be countered. This leads to consideration of specific vulnerabilities that require specialized knowledge of such bespoke systems, are difficult to foresee and predict and require near real time detection and response based on the aggregation of complex observables. The sophisticated nature of current state, terrorist and criminal threats require enterprises to better understand their systems and implement more automated processes to ensure resiliency and support the limited human cyber security professionals charged to oversee protection of these systems.

Traditional risk management approaches to assessing and implementing security on large enterprise networks supporting critical infrastructure have been based on passive and reactive techniques given that such environments had historically been based on more clearly defined and understood technologies. The increasing diversity and complexity of modern networks supporting critical infrastructure have rendered such approaches inadequate to provide the sole means of assessing and guiding the development and management of their protection. To that end, automated approaches to threat assessment and defence are increasingly needed. However, in order to posture such automated approaches within an enterprise environment, an appreciation of the nature of various considerations related to the broader strategic context of security along with a detailed understanding of vulnerable technologies.

References

[1] R. Mazzolin, A. Madni, "A Survey of Contemporary Cyber Security Vulnerabilities and Potential Approaches to Automated Defence", *IEEE SYSCON 2020 Conference, 2020*, Montreal, Quebec, Canada

[2] Salvador Llopis Sanchez, Robert Mazzolin, Ioannis Kechaoglou, Douglas Wiemer, Wim Mees, Jean Muylaert. "Chapter 108-1 Cybersecurity Space Operation Center: Countering Cyber Threats in the Space Domain", *Springer Science and Business Media LLC, 2019*.

[3] J. Kallberg, B. Thuraisingham, E. Lakomaa, "Societal CyberwarTheory Applied: The Disruptive Power of State Actor Aggression for Public Sector Information Security", *2013 European Intelligence and Security Informatics Conference, 2013*.

[4] Seth D. Baum, Ben Goertzel, and Ted G. Goertzel, 2011. "How long until human-level AI? Results from an expert assessment." *Technological Forecasting & Social Change, vol. 78, no.1 (January)*, pages 185-195, 2011.

[5] B. Benyo, D. Musliner, "Automated Self-Adaptation for Cyber Defense Pushing Adaptive Perimeter Protection Inward", *2013 IEEE 7th International Conference on Self-Adaptation and Self-Organizing Systems Workshops*, 9-13 Sept. 2013.

[6] M. Alsaleh, E. Al-Shaer, "Towards Automated Verification of Active Cyber Defense Strategies on Software Defined Networks", *SafeConfig'16*, Oct 24, 2016.

[7] Christopher S. Oehmen, Thomas E. Carroll, Patrick C. Paulson, Daniel M. Best et al. "Behavior-dependent Routing", Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense, *SafeConfig '15, 2015*.

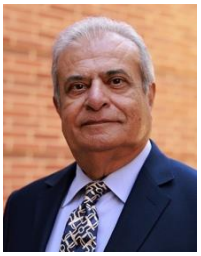
[8] G.. Baldini, et al. "Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and a Way Ahead", *IEEE Communications Surveys and Tutorials*, Vol 14, no 2, pp 355-379, 2012.

[9] T.Booth, K. Andersson, "Critical Infratructure Network DDOS Defense via Cognitive Learning", *14th IEEE Annual Consumer Communications and Networking Conference (CCNC)*, Las Vegas, Nevada, USA, 2017.

[10] M. Atigehetchi, J. Griffith, I. Emmons, D. Mankins, R. Guidorizzi, "Federated Access to Cyber Observables for Detection of Targetted Attacks", *MILCOM 2014*, October 2014.

Copyright: This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

Brigadier General (Retired) ROBERTO MAZZOLIN is the Chief Technology Strategist at the RHEA Group, a multinational company providing bespoke engineering solutions, systems development and security services for space, military, government and other critical infrastructure. During his military career, he served in a variety of key command and staff roles at all ranks. Notable appointments during his military service include responsibility for all Canadian Armed Forces and Department of National Defence strategic network, signals intelligence, electronic warfare and cyber operations, strategic cyber policy development, and responsibility for the engineering and program management of the Canadian Army command, control, communications, computers and intelligence, surveillance and reconnaissance system. He also served at United States Cyber Command as the Vice Director for Strategic Policy, Plans, Force Development and Training. He is a Senior Fellow at the Centre for International Governance Innovation and has written numerous publications and spoken extensively in a wide array of international engineering, commercial and industry fora. General Mazzolin holds a Bachelor of Electrical Engineering from the Royal Military College of Canada, a Master of Science with specialization in electronics and guided weapon systems from Cranfield University, U.K., a Master of Arts in Security and Defence Management and Policy from the Royal Military College of Canada, and a Ph.D. in Engineering Management from California Coast University, USA. He is a licensed Professional Engineer and a Senior Member of the Institute of Electrical and Electronics Engineers. He is an officer of the Canadian Order of Military Merit, and his many awards include the US Legion of Merit, the US Meritorious Service Medal, the Canadian Chief of Defence Staff Commendation and the Italian Army Chief of General Staff's Encomio Solenne ("Solemn Commendation"), in recognition of professionalism and courage for combat actions in Somalia.



DR. ASAD M. MADNI served as President, COO & CTO of BEI Technologies Inc. from 1992 until 2006. Prior to BEI he was with Systron Donner Corporation for 18 years in senior technical & executive positions, eventually as Chairman, President & CEO. He is currently, an Independent Consultant, Distinguished Adjunct Professor and Distinguished Scientist at UCLA ECE Department, Faculty Fellow at the UCLA Institute of Transportation Studies and Connected Autonomous Electrical Vehicle Consortium, and Executive Managing Director & CTO of Crocker Capital.

Dr. Madni received an A.A.S. from RCA Institutes Inc., B.S. & M.S. from University of California Los Angeles (UCLA), Ph.D. from

California Coast University and S.E. (Program for Senior Executives) from MIT Sloan School of Management. He is credited with over 200 refereed publications, 69 issued or pending patents, and is the recipient of numerous national and international honors and awards and has been elected a fellow or an eminent member by some of the world's most prestigious scientific and technical academies and societies. He has been awarded 6 honorary doctorate degrees and 6 honorary professorships. In 2019, IEEE HKN named its top award *"The Asad M Madni Outstanding Technical Achievement and Excellence Award"* to recognize and honor his nearly 50 years of technical and philanthropic accomplishments, and visionary leadership.