*i*Journals: International Journal of Software & Hardware Research in Engineering (IJSHRE)
ISSN-2347-4890
Volume 9 Issue 3 March 2021

THE IMPACT OF EMERGING WIRELESS NETWORK SYSTEM AND CYBERSECURITY IN A GLOBAL COMMUNITY

Odey John Adinya[1], Ele, B. I.[1]& Obono,I. O.[1]

johnodey@yahoo.com, mydays2020@gmail.com, obonoio@gmail.com

[1]Department of Computer Science, University of Calabar, Calabar, Cross River State - Nigeria

ABSTRACT

Wireless network systems and cyber security threats are growing faster than their mitigation measures. World Economic Forum has identified wireless network security and cyber security threats as its top global risks for the past eight years. This paper aims to critically examine the impact of emerging wireless network systems and cyber security in a global community and suggest some best countermeasures against wireless and cyber security threats that have been of global concern. To achieve this, the study conducted an in-depth review of wireless network security and cyber security. This study has presented a robust wireless security mechanism and suggests appropriate countermeasure against wireless network and cyber security threats that is more cost-effective in mounting attacks in the service area, and simultaneously providing higher security than basic security mechanisms.

KEYWORDS: Wireless Network System, Cybersecurity, Global Community, Cyber-attacks, Fusion centers, Collaborative.

1. INTRODUCTION

According to research, Internet-based sharing of computational facilities and data resources has created opportunities for collaborative virtual working environments, and virtual control of sensing and control systems of monitoring, operation, prediction, and control within the country's Crime Investigation (CI) sector networks. Unfortunately, these initiatives and systems created to facilitate and speed up communications, work, and collaboration between nations and continents are largely insecure and susceptible to terrorist attacks. These systems have been called "the new and emerging threats and vulnerabilities" [1] with the potential for mass and widespread destruction and disruption of communications.

Consequently, the National Cyberspace Security Response (NCSSR) was created to provide the national framework for ensuring information security and protecting cyberspace. Specifically, this agency had three strategic objectives:

(i) Prevent cyber-attacks against America's critical infrastructures
(ii) Reduce national vulnerability to cyber-attacks
(iii) Minimize damage and recovery time for cyber-attacks that do occur.

The agency came up with a series of measures to reduce the threat and vulnerability programs, to institute national cyberspace security awareness and training, and to go global by creating the International Cyberspace Security Cooperation [1]. The creation of the National Cyber Security Division within the Office of Cyber Security and Communication reflected the importance of the need to keep this domain intact and safe from terrorism. The agency was created to build and maintain an effective national cyberspace response system and to implement a cyber-risk management program for the protection of critical infrastructure. A terrorist attack on any of our communication systems can infect and destroy the workings of most of our computer chips in communication, flights, electricity, and every other element of our daily life that depends on computer systems. So far, we have had threats and limited attacks that have been dealt with quickly and swiftly through computer viruses and infiltrations. But al Qaeda has continued to use tools like the World Wide Web, mobile telephones, satellite telecommunications, electronic banking, and jetliners to coordinate its actions, to enable movement through state borders without detection, and to disseminate its ideology" [2]. And al-Qaeda and the ISIS have engaged in transnational terrorism which is "borderless, present everywhere at once"[3].

The paucity of communication network called on the US to consider this cyberwar an international affair, one to be fought by all nations where cyber activities take place. Indeed, the 9/11 Commission found out that about two dozen terrorist groups including al-Qaeda have attempted to acquire or develop chemical, biological, radiological, and nuclear weapons to attack the USA and its allies. So the recommendation of the Commission to the House was for the United States to work with the international community to prevent the proliferation of such weapons or materials that are necessary for the development of these weapons. As a result, the House enacted acts to prevent terrorist travel, terrorist access to critical infrastructures and key assets, and to prevent the financial strength and flexibility of terrorist organizations. These measures led to the creation of the National Strategy to Secure Cyberspace with the view of engaging in the following six initiatives to strengthen U.S. national security and international cooperation:

(i) Strengthen cyber-related counterintelligence efforts
(ii) Improve capabilities for attack attribution and response
(iii) Improve coordination of responding to cyber-attacks within the US. national security and community
(iv) Work with industry and through international organizations to facilitate dialogue and partnerships among international public and private sectors focused on protecting information infrastructures and promoting a global "culture of security"
(v) Foster the establishment of national and international watch-and-warning networks to detect and prevent cyber-attacks as they emerge
(vi) Encourage other nations to accede to the Council of Europe Convention on Cyber Crime or to ensure that their laws and procedures are at least as comprehensive
[1] and [4].

So this system which was initiated to facilitate communication, safety, and the global attack on terrorism can equally be used by the terrorist against the Free states and nations. The above agenda and objectives set a scenario for collaborative endeavors on the part of all global parties or would-be participants in cybersecurity. Any attempts therefore to expand cyber networking or nuclear plants must take into consideration the enormous cost both in human, material, financial aspects that go, not only into creating the network but safeguarding it from misuse and terrorist attacks. Just as they are effective in building a network of collaborative survival, they are equally susceptible to divulging information for massive destruction and confusion. It all depends on who uses it and for what purpose.

Another area that has been impacted by these re-organizations has been the shipping ports where security has been beefed up. The SAFE Port Act of October 2006 was passed to enhance port authorities and as an extension of the USA Patriot Act that empowered the Department of Homeland Security to use any of its law enforcement agencies to detect and intercept terrorists and terrorist acts. More money and manpower were deplored to the various ports of entry and exit which are susceptible to terrorists who may use them to export Weapons of Mass Destruction or guns. Terrorist attacks of any ports will not only lead to the loss of life but also to the loss of national and international business in a society where the economy is a life wire of each country. These anti-terrorist moves were made in conjunction with the international communities because commerce involves local citizens and governments and foreign citizens and their governments as well. So, the DHS has successfully planted intervention steps at key ports and areas in the shipment process using the Container Security Initiative Plans to prevent the shipment of terrorist materials. Operation Safe Commerce has been implemented in collaboration with international agencies and foreign governments that have allowed US workers to inspect and handle the materials exported to America and from those foreign ports and countries. These collaborations have yielded success since the US Coast Guards, the Immigration and Customs Enforcement Agency (ICE), and other agencies have not reported incidents resulting from the penetration of US ports [1]. The immigration service was immediately co-opted into the Department of Homeland Security to ensure that those who entered and left the US were legal and had no criminal intent. The Office of Detention and Removal Operations was empowered to detain and deport those who were illegal in the US, and the US borders were given more sweeping powers to mount checkpoints and increase surveillance activities at the borders to protect the US borders from invasion or being used as a way into the heart of the USA for further attacks. Indeed, physical barriers, unmanned vehicles, and sophisticated imaging devices were created to monitor borders to keep terrorists away [5]. They have virtually succeeded in doing so as terrorist suspects have been apprehended on the Canadian-USA borders struggling to smuggle bomb-making devices to attack Los Angeles airport.

However, the USA has succeeded immensely in stopping and interrupting terrorists from effecting any blow again in the USA since 9-11. A minor lapse in airport screening and imaging indeed let the Nigerian-born Christmas Day Bomber slip through from the checks at the airport; however, he was apprehended when the bomb failed to be detonated. This oversight again shows how the system cannot be completely watertight and is still in need of improvement. Good is not good enough, but we have to go for better and closer surveillance. Hence, the creation of Fusion Centers.

2. FUSION CENTERS

The creation of Fusion Centers was an excellent move by the Bush Administration to bring together professionals within the law enforcement community with diverse backgrounds in intelligence gathering to work together to detect, deter, and prevent terrorist elements from engaging in homeland attacks. Indeed, a “fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources” [6]. Fusion Centers emerged out of necessity: the need to fight crime and terror with all the information available across the globe. According to the Authors in [6], "the ultimate goal of Fusion Centers is to provide a mechanism through which government, law enforcement, public safety, and the public sector get together with a common purpose and improve the ability to safeguard our homeland and prevent criminal activity" (p. 4). They were created out of a crisis and given the freedom to penetrate the core of the society to dig out the roots of terrorist and criminal activities by engaging every level of society. They have sprung up across the nation since the last decade.

Fusion Centers have become a much more manageable way of solving terrorism and crime in a collaborative and all-inclusive way. They involve law enforcement Offices, the office of public safety such as the Fire Department and Medical Emergencies, and the public sectors, all united in a single effort to fight crime and to prevent a 9-11-like attack from taking place in the USA again. The Center also has the advantage of sampling the best from all walks of life and technical fields that bring to the table a diverse assortment of skills needed to fight crime. In this way, the Fusion Center becomes a microcosm of the community because it is composed of representatives from all the sectors of that community. The Center engages in training on intelligence gathering, analysis, calibration, and dissemination with the goal of keep-enabling the members to make informed decisions about activities and actions deemed un-American to keep the society safe.

Indeed, the Fusion Center concept is a new or innovative way of eliminating crimes in society. The idea is that if these homegrown terrorists do exist and engage in activities within the society, somebody somewhere should be able to discern these changes in attitudes and report back to the authorities. The innovation here is that everybody is deemed capable of acting in the role of an informant and therefore a contributor to the safety of society. Formerly, security and public safety were considered the prevue of the police and law enforcement agents. The police, CIA, and FBI had almost total control of these situations but Fusion Centers have debunked this idea and demystified intelligence activities making it a privilege also for those who have the character traits of honesty and who are determined to assist in protecting the nation.

Fusion Centers have also shifted the center of allegiance from the Unit of Origin to the Center of Activities. This calls for a shift in *organizational behavior and protoco*l as the shift is now towards the Center and away from the local precincts or former areas of employment. This shift brings in a true test of loyalty as conflicts will always arise in the dissemination of information across jurisdictions where each officer or person will feel called to pay particular attention to the home precinct or jurisdiction. The underlying concept behind these centers is that a united effort yields better results. It will be more useful to empower the member to be independent of their various feeder groups through the provision of salaries concomitant with the training and level of each member being initiated to give them each a reason to be fully committed to the Centers. This change in management paradigm does not undercut the loyalties to the intelligence offices, but rather ensures continuity of operations through shared experience and information. Each intelligence agency (NIA, FBI, CIA, DoJ, DOD, DNS, etc.,) fully collaborate and even trains those lay individuals who have dedicated time and effort to the solving of crime in society. Many of those from the neighborhood can have greater leverage among their local friends and colleagues who can trust them with information than they would a strange FBI and CIA agent whom they do not know. These traditional agencies should not consider these Centers as upstarts or presumptive individuals who pretend to be intelligent agents. Rather, they are genuine individuals who want to help the intelligence community in their little ways to solve a crime.

The world is evolving quickly and terrorists are coming up with innovative methods and cyber intelligence to circumvent what is put in place against crime. These Centers seem to be the most effective and least expensive way of counteracting these homegrown terrorists, many of whom are very much indistinguishable, except through daily interactions. According to the [8], and reiterated throughout the [7], collaboration seems to be the defining glue or principle that holds these Centers together: “Fostering a collaborative environment is not only important to sharing, collecting, developing, and disseminating intelligence but also sharing decisions and ownership” (p.29). Indeed, the purpose of the collaboration is to increase capacity, communication, and continuity of service while decreasing duplication [9]. So, there will have to be a concerted effort to avoid service duplication and waste through intensive education of the public to buy into it. These Fusion Centers continue to remind the nation of the dire need to have full control of security and safety. The events of 9-11 took the nation by surprise and Presidents Bush and Obama did not want to take any chances with security by encouraging these Fusion Cells. There may be overlaps and duplications, but this may be a way of making sure that the information does not escape the attention of one of the layers of security.

Indeed, Fusion Centers tend to discard all forms of theoretical restrictions in favour of Best Practices, experimenting with what works best. Like with system theories and empowerment, the underlying principle here is what will motivate the citizens and agents to work faithfully and collaboratively to solve a crime and prevent criminal activities. It would be advisable to reconsider the internal organization of each Fusion Center and to create a very unique link and relationship with the professional intelligence agencies such as the National Intelligence Agency, the FBI, CIA, the Department of Homeland Security, the Department of Defense, and the Department of Justice who will act as resource agencies to the Centers. It will also be important to initiate a rigorous program of education to train the lay citizens in the issues of intelligence and protocol, the effective and judicial use of new and innovative technology to track and analyze information, and the need for collaborative co-existence with other groups. There will also need to inform the interested parties that intelligence gathering, analysis, dissemination, and action thereupon is a serious issue of life and death and should not be taken lightly.

Finally, there will be a need for the President to come up with a reasonable budget for each Center to take care of the training, materials, equipment, logistics, and all that will facilitate the job and encourage members to be excited about working for each Center. Each Center should be raised to a fully independent unit with its organizational chart, division of labor, and specialization so that members will realize that they are being recognized and compensated for work done. Furthermore, there should be a system of remuneration where good and outstanding work is being recognized and rewarded. Moreover, the appointments of members of the Fusion Centers should be selective and should constitute the top cream of any of the feeder units and stakeholders who will bring in the best from their areas to share with the rest. This will make the Center training much easier and manageable since those undergoing training already has a base of knowledge on which the training is built.

It will not be an easy task, but the enhancement of the Fusion Centers is a welcome innovation. Many cities have engaged in the creation of these Centers and the Department of Homeland Security should be encouraged and given full support to see this initiative spread and succeed. The President should personally share a vision with these Centers and own them. The success of these Centers in the USA should inspire foreign nations to implore the same techniques and create similar bodies to overlook security. This concept is built on the biblical paradigm of being your brother’s keeper. Security is a collective venture and any talk about expanding nuclear power and use and cyber facilities must take into consideration new ways of guaranteeing security without making such a venture too expensive.

3. An Overview of Wireless Technology

The evolution of wireless services has led to an unrestricted accelerated pace of adoption and widespread acceptance of wireless technology. This evolution in communication is recognized as a promising breakthrough for the next decade and beyond. The wireless technology invention is strengthening and integrating wireless communication, network protocols, and next-generation internet protocols into a more unified wireless technology architecture. Unlike analog, wireless technology has added considerable value to wireless communications by extending wide range coverage and connections to a multiplicity of devices and application programs[10]. Wireless technology has created productivity enhancement and an effective medium of communication on a just-in-time service to the global community. The advancement of wireless technology and its unhindered utilization for communications has stretched the conversion and contributed to the changeover from dial-up, cable-wired analog connections to digital connections. The wireless service code-named "direct connections" transmission is easier, faster, and less expensive than its predecessor[11].

However, the vulnerability of wireless networks still presents enormous challenges and risks that continue to threaten wireless security. The author in [12] argued that wireless communication takes place through the air using radio frequency signals that minimize the threats of interception. Conventional wisdom maintains that encrypted information and data with a weak algorithm will continue to be vulnerable to hackers and cyber terrorists. The authors in [13] and [14] asserted that the majority of converted data and information is powerless and at the risk of being intercepted, read, and compromised by unauthorized officials. Consequently, there is an urgent call to decrease the vulnerability of wireless network systems to uphold confidentiality, ensure integrity, and to provide constant protection of wireless network operations. The evolution of wireless technology is entrenched with the potential for dramatic improvement of individual, organization, and social communication services. We are amid a historic proliferation of wireless transmission and communication services across the globe. The growth and universal approach to wireless technology has increased demands for data and information transmission and communications. It has collectively improved the efficiency of wireless technology.

Wireless technology is deployed in almost every corner of the world community for on-going operative transmission and communication. The authors in [15] noted that organizations and individuals residing in remote regions of the world now have access to wireless services for data and information transmission, communication including instant and emergency contacts. Certainly, the wireless services industry is currently entrenched with widespread support from private and general public agencies. Wireless communication is beginning to receive important regulatory supervision from the government by restricting the use of wireless devices in school zones and texting while driving for safety reasons. Amid existing challenges, wireless services remain sustainable, inevitable, and convenient solutions to innovative daily life. Statistics revealed that large segments of the world community and approximately one million people in the United State have wireless service accounts with various carriers [16]. The evolution of wireless services and associated technology is working intelligently by empowering the lives of individuals, organizations, local, states, and federal government agencies, nations by transforming analog (wired-cable) to digital (wireless) services.

The advantages of wireless services involve allowing important information to be accessible to a large segment of the global community. Today's universal society consists of the first time beneficiary of wireless service and efficient communication around the world in ways that were never thought possible. The authors in [12]noted that the global community collaboration and active participation in both progressions of wireless services and associated technology is a credible avenue to reinforce a universal alliance around the world. Wireless services have been instrumental in organizing, transmitting, and preserving important documentation and learning endeavours around the world.

Universal wireless has benefits, shortcomings, and challenges. Wireless service users in various countries, precisely in Africa and Asia are subjected to unlawful tracking, monitoring, and data interception that tend to undermine and overturn the fundamental rights of privacy and freedom of expression. Despite these potential vulnerabilities, the reward of wireless services in the education institutions, government agencies, and corporate enterprises cannot afford to shy away from wireless service challenges. Stakeholders must continue to establish a well-conceived alliance with regulatory agencies such as the Global Network Initiative (GNI) and the Electronic Industry Code of Conduct (EICC) to minimize emerging wireless services challenges [12].

The projection or aspiration of wireless service is a continued expansion of wireless transmission of data, information, and communication services to individuals, villages, government agencies, and other nations in all regions of the world. Today, the purchase of wireless technology has increased tremendously and is escorted by a drastic decrease in the prices of wired cable technology, connections, and communication. Individuals, organizations, institutions of higher education, government agencies, and entire segments of the world communities have acquired millions of wireless technology for immediate daily use. Without any doubt, well-defined high volume purchase of wireless devices has inspired individuals, schools, and university students, and society to use wireless technology for effective connection and communication. The continued purchase and use of wireless services and associated technology will certainly lead to the acquisition of approximately three billion wireless devices every-where and every-year for the next decades. The future for the wireless transaction is limitless.

Boeing and other commercial airliners such as Lufthansa, British Airways, Japan, France, and Scandinavian Airlines have equipped their long-range jetliners with wireless technology to allow passengers direct access to a control center of approximately 12 kilometers or 7.5miles above ground [17] and [18]. The prominence of the wireless service system is validated primarily based on usage convenience, cost efficiency, and almost effortlessness of integration, connection, and universal compatibly with major wireless network providers. The author in [19] noted that most wireless technologies sold to consumers are pre-equipped with factory built-in compatible capabilities and user-friendly-wireless connections and communication tools. The major line of challenges, according to the authors in [20], consists of unauthorized access points; dissemination of information, service set identifier (SSIDs), and spoofed medium access control (SMAC) addresses and wireless local area network (WLAN), scheduled maintenance, systematic troubleshooting policy, and procedures. Indeed, the advent of wireless technology has unbolted enormous latitude of any-where, any-place, and any-time connection across the globe.

However, the dawning of wireless service involves interrelated consequences. Current researchers on wireless technology, such as [21], [22] and [23], highlighted a credible solution to a vulnerability which includes ongoing professional training of wireless equipment manufacturers, providers, and consumers on factory settings, well-synthesized equipment manuals, web sites link and online product technical support. In contrast with cabled-wired connection service, wireless service is very susceptible to the accidental Association (AA) involving unauthorized access to individuals and the organization's wireless services. The authors in [24] point out that accidental association start from several different techniques, and usually occurs as soon as users turn on and start operating a computer system that latches into wireless access points overlapping a neighboring organization wireless service without the organization's or user's permission.

This is not an attempt to downplay the importance of emerging wireless services; rather, it is an indication that failure to prevent perpetrators from an organization's sensitive information and data is recognized as a wireless service security breach. To sidestep individuals, organization, and institutions of the higher education access point (AP) at all times, each director of information technology (IT) must be adequately trained and equipped with the expertise to protect against planned and the unplanned threat of malicious association (MA) of perpetrators' vicious activities on already a vulnerable wireless technology network. Cyber terrorists, hackers, and crackers code-named as "perpetrators," are repeatedly inclined to adopt various techniques to gain illegal and unauthorized access to organizations' and institutions' wireless service networks[25].

Perpetrators often use laptops as a soft access point (SAP) to create well-suited software to produce illegal wireless network cards (WNC) to gain unauthorized access to individuals, institutions' and organizations' wireless service systems. The authors in [17] and [26], noted that most network systems are defenseless, vulnerable, and generally easy to pass through without an authorized username and password. Notably, the wireless network operates at Layer 2 (Data-Link) and Layer 3 (Network) of the "Open Systems Interconnection" (OSI) models. The OSI consists of seven layers, each playing a specific role when applications are communicating over the network. In the process, each layer, from top to down adds a specific header to the transmission of raw data. Sustained maximum security directly related to wireless services and signals consists of network system authentication (NSA) and virtual private network (VPN). To save wireless service from damage, the author in [26] suggested that NAS and VPN must be adequately integrated and configured to block well-informed and out of control perpetrators from penetrating an organization's and institution's wireless service through Layer 2 network also known as the Data-link layer, which is a software program designed to bridge the gap between two homogeneous network systems. The wireless network is a defenseless system and is inclined to be lacerated by unauthorized users and perpetrators.

Without any doubt, wireless technology has created productivity enhancement and an effective medium of communication on a just-in-time service to the global community. The emergence of wireless technology has histrionically increased and strengthened the integration of wireless data, information transmission, and communications. The projected gridlock of wireless technology (WT) was the rapid and universal adoption of WT to replace the analog network system. In contrast with localized analog technology, wireless technology is a historic technology for a global society. The WT has added considerable value by extending a broad range of value, data, information transmission, communications, and connectivity to a multiplicity of devices and application programs used by consumers all over the world. The advancement of wireless technology and its unhindered utilization for communications has stretched the conversion and contributed to changeover from dial-up, cable-wired analog connections to digital connections.

However, due to the vulnerability of wireless technology, perpetrators can use identifiers broadcasting to attack wireless network systems. Today, most wireless devices are shipped out of the factory to consumers with a built-in identifier broadcasting (BIIB) with the ability to send out signals to wireless networks within the vicinity announcing the BIIB presence. Consequently, wireless technology equipment manufacturers must be prevailed upon to develop and deliver wireless devices such as routers and switches with the encryption feature entirely turned-off and concealed instruction turned-on by IT directors before installation and configuration on organization wireless network system. This way, the privacy and security apparatus will be guaranteed and used only by those authorized to do so.

3.1 Challenges in Wireless Security

Enterprises see many advantages in deploying wireless LANs (WLANs), a technology that in the past few years has witnessed considerable market penetration. Compared to wired networks, WLANs incur lower installation costs per user given the reduced cabling and manual labour required. Moreover, connectivity is provided to mobile users at no extra cost, improving efficiency and productivity.

One major challenge regarding the deployment of wireless networks is dealing with the unpredictable nature of signal propagation [27]. While signal strength decreases with distance, the rate of decay inside a building depends on the construction materials used, floor layouts, the placement of furniture and other obstacles, as well as the number of people and their moving patterns. The resulting reflection, diffraction, and scattering of waves create environment-dependent oscillations in received signal strength, which challenge not only services such as network planning but also all others that rely on signal strength statistics.

Regarding security, one major disadvantage of wireless networks is that they violate the physical security model that is so effective in wired LANs, therefore requiring additional mechanisms to implement proper access control. Unlike the wired scenario, there is no inherent access control: wireless links extend connectivity beyond physical boundaries, making networks available in parking lots, across the street, and in nearby buildings, adjacent locations where coverage was not intended. When left unprotected, these wireless links make networks vulnerable to misuse and attacks. It is also more difficult to make clients accountable for their acts, as misbehaving devices can move freely and be 50 meters from the access points they use. Moreover, malicious users can use directional antennas and amplifiers to produce higher signal strength levels and create many different signal strength patterns to further obfuscate their physical locations.

To make matters worse, current access control solutions are not suitable for all wireless installations: they either provide little security improvements or incur high management overhead. On one hand, some mechanisms are easy to deploy but that adds little or no protection. For instance, installations may leave their wireless links open, hide network names (SSIDs in 802.11 jargon), or use MAC address lists. As these solutions can be easily broken by hackers, networks are still at risk of being compromised. On the other hand, several mechanisms provide higher security levels and fine-grained access control capabilities, but at much higher costs to secure wireless LANs [28]. The higher management costs come from adding and removing users, granting and revoking access rights, as well as protecting sensitive information (keys), which is vital for keeping systems uncompromised. These mechanisms also place a lot of responsibility on users, who have to choose proper passwords and keep them safeguarded. As a result of this trade-off between security and management costs, a large percentage of wireless networks still operate with insecure configurations and many of them are commonly victims of network abuse.

A world-wide wardriving effort performed in June 2004 detected over 200,000 access points, with more than 60% of them running without cryptographic protection (then using WEP) and over 30% with the default SSID set by the manufacturer [29]. In enterprise environments, insecure configurations are also common. A studyperformed by RSA and NetSurity in March 2005 revealed that over 30% of enterprise wireless LANs in London, Frankfurt, New York, and San Francisco lacked basic security measures [30]. While these configurations can be complemented by VLANs and firewalls to restrict the services available to wireless clients, networks are still left unprotected and vulnerable to misuse. Of 700 institutions that responded to the 2005 CSI/FBI Computer Crime and Security Survey, over 15% acknowledged that their wireless networks were victims of abuse during the previous year [31]. This number is a lower bound, as these institutions need at least to be aware that such attacks took place and willing to share that information. Unfortunately, this situation is doomed to get worse because the number of deployed access points keeps rising at a considerable rate, allowing malicious users to find vulnerable networks with minimal effort.

According to the study by RSA, the number of access points detected in London and Frankfurt increased respectively by 62% and 66% between 2004 and 2005 [30]. Market research shows that WLAN unit shipments increased by 39% between 2004 and 2005, with access points accounting for 81% of the wireless equipment revenue [32].

In summary, if on one hand wireless LAN technology is compelling for many reasons on the other they introduce a new security paradigm that creates challenges for access control. Security problems will continue to exist unless cheaper yet effective solutions become available.

3.2 Risks and Vulnerabilities of Wireless Networks

Along with the many conveniences and cost-saving advantages to wireless networks, there are also some inherent risks and vulnerabilities.

3.2.1 The Nature of the Wireless Medium

Traditional wired networks use cables to transfer information, which is protected by the buildings that enclose them. To access a wired network, a hacker must bypass the physical security of the building or breach the firewall. On the other hand, wireless networks use the air, which is an uncontrolled medium. Wireless Network signals can travel through the walls, ceilings, and windows of buildings up to thousands of feet outside of the building walls.

Additionally, since the WLAN medium is airwaves, it is a shared medium that allows anyone in proximity to “sniff” the traffic. The risks of using a shared medium are increasing with the advent of readily-available “hacker’s tools.” A variety of specialized tools and tool kits enable hackers to “sniff” data and applications and to break both the encryption and authentication of wireless data.

3.2.2 Insecure Wireless Network Devices

Insecure wireless LAN devices, such as access points and user stations, can seriously compromise both the wireless network and the wired network, making them popular targets for hackers.

3.2.3 Insecure Access Points

Access points can be insecure, due to improper configurations and design flaws. Access points shipped with insecure default configurations. They are pre-configured with a default password; they broadcast service set identifiers (SSIDs), and they often require no encryption or authentication. If deployed with default settings, they become gateways that hackers use to access both the wireless and the wired network.

Intruders (hackers) can convert laptops into “soft” access points (APs) by either using a variety of software programs, such as HostAP, Hotspotter, or Airsnark, or, by simply using a USB wireless adapter. Using soft APs, a hacker can cause a legitimate user to connect to the hacker’s laptop, compromising that user’s machine.

3.2.4 Insecure User Stations

Insecure wireless user stations such as laptops or bar code scanners pose an even greater risk to the security of the enterprise network than insecure access points. The default configuration of these devices offer little security and can be easily misconfigured. Intruders can use any insecure wireless station as a launchpad to breach the network. Below is a diagrammatical representation of some attacks usually done by a network hacker?

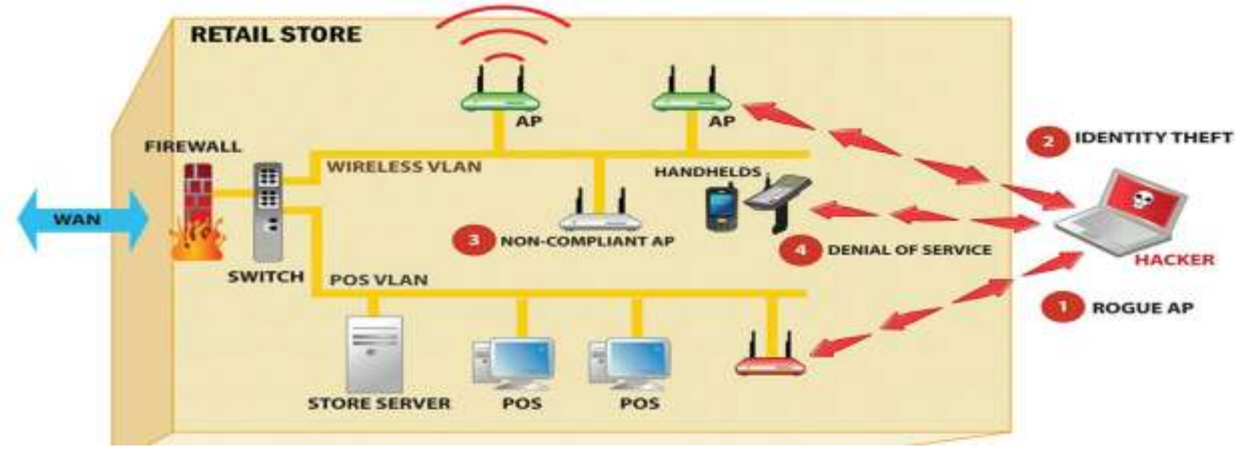

Fig. 1: A common wireless network security risks (Adopted from [19]).

4.0 An Overview of Cyber security and Cyberspace

Cyber security begins with the knowledge of computing assets and how one depends on them. Today's World leaders need meaningful cyber situation awareness to safeguard sensitive data, sustain fundamental operations, and protect national infrastructure.

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access (Wu and Irwin, 2013).Cyber security refers to preventative methods used to protect information from being stolen, compromised, or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cyber security strategies include identity management, risk management, and incident management. In a computing context, security includes both cyber security and physical security (Singer and Friedman, 2014). According to Wu and Irwin (2013), cyber security or IT security is the protection of computer systems from theft or damage to the hardware, software, or the information on them, as well as from disruption or misdirection of the services they provide.

Ensuring cyber security requires coordinated efforts throughout an information system. Elements of cyber security include Application Security, Information security, Network Security, Disaster recovery/business continuity planning, Operational security, and End-user education.

One of the most problematic elements of cyber security is the quickly and constantly evolving nature of security risks. The traditional approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment.

To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach. The National Institute of Standards and Technology (NIST), for example, recently issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments. According to Forbes, the global cyber security market reached $75 billion for 2015 and is expected to hit $170 billion in 2020.

In this paper, we present the notional cyber security landscape of the Reference Diagram, which creates a context for introducing concepts and terminology of cyber security, though, it is not an accurate representation of real cyber security defense and as such it can apply to physical and virtualized environments.

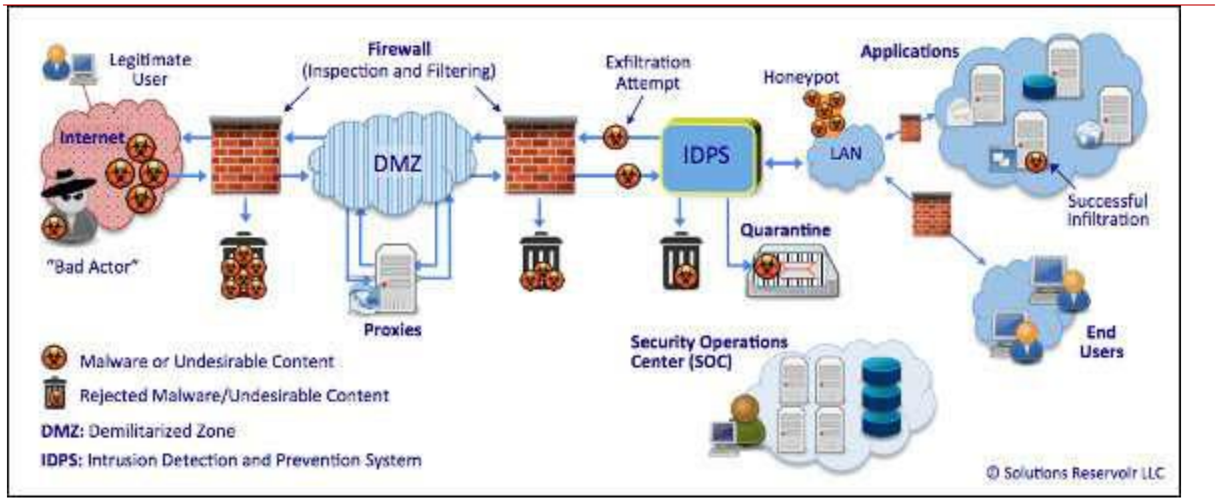
Legitimate User
Firewall (Inspection and Filtering)
Exfiltration Attempt
Applications
Honeypot
Internet
DMZ
IDPS
LAN
Successful Infiltration
"Bad Actor"
Quarantine
Proxies
End Users
Security Operations Center (SOC)
Malware or Undesirable Content
Rejected Malware/Undesirable Content
DMZ: Demilitarized Zone
IDPS: Intrusion Detection and Prevention System
© Solutions Reservoir LLC

Fig.2: Reference Diagram of Notional view of the cybersecurity landscape (Adopted from [34]).

Generally speaking, bad actors seek to achieve their goals through the placement and execution of malicious software (**malware**) that exploits a vulnerability in an information system. Vulnerabilities are flaws in software/code that provide a means for malware to be installed and executed, typically without any overt sign of its presence to system users.

In many regards, the battle in cyber security is between bad actors seeking to exploit vulnerabilities that have yet to be repaired (or **patched** in a security update) or to discover and exploit a new one. The first exploitation of a newly-discovered vulnerability for which no patch is available (or even under consideration) is called a **zero-day** attack, and it is a very dangerous condition in cyber security for its potential to conduct undetected mayhem. The Open SSL vulnerability known as “Heartbleed” **(CVE-2014-0160)** was undetected for approximately two years, so only a bad actor is certain of the zero-day attack on it.

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes is now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences.

Cyberspace is particularly difficult to secure due to several factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks (Singer and Friedman, 2014). As information technology becomes increasingly integrated with physical infrastructure operations, there is an increased risk for wide-scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission.

4.1 An Overview of Cybercrime

Cybercrime or **computer crime** is a crime that involves a computer and a network[35]. The computer can be used in the commission of a crime, or it can be the target [36]. The authors in [37] define cybercrimes as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes can threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. The authors in [37] further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones". Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes.

Cybercrime is a broad category of offenses involving computers and computer networks. While many acts of cybercrime are essentially high-tech forms of theft or fraud, some have goals other than financial gain. These might include copyright infringement, exchange of child pornography, and even espionage. Some jurisdictions have expanded legal protections against harassment and stalking to include the Internet. Some acts of cybercrime, known as “cyber attacks,” seem intended only to disrupt or destroy computer networks. Internet security experts estimate that the global annual cost of cybercrime approaches $1 trillion.

A substantial amount of cybercrime consists of intrusions into business and personal computer networks, including servers, desktop computers, laptops, and mobile devices. This can be achieved through direct hacking, or through malicious code attached to an email or hidden on a website. Information obtained from these devices could be used in identity theft, bank fraud, credit card fraud, and other fraudulent schemes.

One of the largest cyber security breaches in history occurred in late 2013 when hackers stole millions of customers’ personal information from the retail company Target’s computer system. Investigators suspect that the hackers obtained access to Target’s network by hacking the company that operated its heating, ventilation, and air conditioning (HVAC) system, which shows just how determined and creative cybercriminals can be. Cybercrime also includes the use of computers and computer networks to transmit or receive illegal materials, such as child pornography, or to buy and sell illegal items like drugs. The use of the internet for copyright infringement can result in criminal prosecution, such as the case against **Megaupload**, a file-sharing website that once accounted for four percent of global internet traffic.

In some cases of cybercrime, a computer or computer network is a target rather than a tool used to commit an offense. Malicious code, such as a computer virus, may be used in a targeted attack, or it may be released onto the Internet to sow chaos. A common type of cyberattack is called a distributed denial-of-service (DDoS) attack. Its purpose is to interrupt or disable a server, making it unavailable to other users on the Internet. This is often done by overloading a server with access requests, causing it to essentially shut down network access. After the raid on Megaupload mentioned above, the U.S. Department of Justice’s website was disabled by a DDoS attack.

4.2 The Rise of the Cyber Threats

While the IoT is entering daily life more and more, security risks about IoT are growing and are changing rapidly. In today’s world of “always-on” technology and not enough security awareness on the part of users, cyber-attacks are no longer a matter of “if” but “when.”

Cybercriminals are working on new techniques for getting through the security of established organizations, accessing everything from IP to individual customer information — they are doing this so that they can cause damage, disrupt sensitive data and steal intellectual property.

Every day, their attacks become more sophisticated and harder to defeat. Because of this ongoing development, we cannot tell exactly what kind of threats will emerge next year, in five years, or 10 years; we can only say that these threats will be even more dangerous than those of today. We can also be certain that as old sources of this threat fade, new sources will emerge to take their place. Despite this uncertainty — in fact, because of it — we need to be clear about the type of security controls needed.

Effective cybersecurity is increasingly complex to deliver. The traditional organizational perimeter is eroding and existing security defenses are coming under increasing pressure. Point solutions, in particular antivirus software, IDS, IPS, patching, and encryption, remain a key control for combatting today’s known attacks; however, they become less effective over time as hackers find new ways to circumvent controls.

5. CONCLUSION

The above narrative indicates the complexities, costs, and inconveniences entailed in an unrestricted application of the Bill of Rights, globalization of the Internet and Cyber activities, and the proliferation of nuclear energy for peaceful and productive purposes. Globalization has reduced the world countries into nations without real borders [38], thereby making movement and communications relatively faster and easier. However, the relative peace and material advancement we enjoy come at a great price. Since it is the nature of humanity to control and even destroy one another, in a society determined by daily conflicts and conflicting interests, we must look for better and finer ways to safeguard the advances we have achieved or want to achieve. America's initiatives against the terrorists grow pale when the entire global community does not join her in the fight, even if only to identify the would-be enemies.

Each method of combating terrorism initiated by America such as travel restrictions and control, the development of the Department of Homeland Security, the creation and operation of Fusion Centers, and the collaboration of all intelligence-gathering and intelligence-sharing organizations have yielded enormous dividends. They should all be emulated, if not duplicated by world powers that have the potential to create, build and enjoy unrestricted freedom to cyber communications, nuclear energy, and travels.

REFERENCES

[1] Bullock, J, Haddow, G, Coppola, D. & Yeletaysi, S. (2009). *Introduction to homeland security: Principles of all-hazards response*. 3rd Edition. Burlington, MA: Elsevier Inc.

[2]Watts, M. (2007). Revolutionary Islam-Violent geographies, New York: Routledge. 175-204.

[3] Popescu, G. (2016). Borders in the era of globalization. *Border Crossings: A Bedford Spotlight Reader*. New York: Bedford/St. Martins, 273- 293.

[4] Department of Homeland Security. (200*3). A national strategy to secure cyberspace.* Retrieved on 9/25/2015 from www.dhs.gov.

[5] Sauter, M. A. & Carafano, J. J. (2005). *Homeland Security: A complete guide to understanding, preventing, and surviving terrorism*. New York: McGraw-Hill CompaniesInc.

[6]Office of Justice Programs. (2013). *Fusion center guidelines*. Retrieved on 5/28/2013 from http://www.it.ojp.gov/fusioncenterguidelines/intro.html.

[7] Department of Homeland Security. (2013). *Fusion Centers Guidelines: Developing and sharing information and intelligence in a new era..*. Retrieved on 5/29/2016 from http://www.it.ojp.gov/fusioncenterguidelines/intro.html

[8] Office of Justice Program. (2003). *The National Criminal Intelligence Sharing Plan: Solutions and approaches for a cohesive plan to improve our nation's ability to develop and share criminal intelligence.* Retrieved 24/04/2016 from http://www.fas.org/irp/agency.

[9] Petersen, C. R. P. (2003). Community collaboration. Retrieved 12/12/2015 from http://www.communitycollaboration.net.

[10] Tse, D., and Viswanath, P. (2005). *Fundamentals of Wireless Communication*. New York, Cambridge University Press.

[11] Theodore S. R. (2002). *Wireless Communications - Principles and Practice*. Prentice-Hall PTR, 2nd edition.

[12]Raychaudhuri, Dipankar, and Mandayam, Narayan (2011). "Frontiers of Wireless and Mobile Communications." Proceedings of IEE, Vol 100, No 4 (824-840).

[13] Fagin, J.A. (2006). *When Terrorism strikes at home: Defending the United States.* Boston: Pearson Education, Inc.

[14] Lun, D. S., Koetter, M., Koetter,R. and Effros, M. (2008) "On coding for reliablecommunication over packet networks". Phys. Commun., vol. 1, no. 1, (3–20).

[15] Frenkiel, R. Badrinath, B., Borres, J and R. Yates, R. (2000) "The infestations Challenge: Balancing cost and ubiquity in delivering wireless data". IEEE Pers. Commun., vol. 7, no. 2, (66–71)

[16] Meguerdichian, S, Koushanfar, F., M. Potkonjak, and M. Srivastava, M. (2001). "Coverage problems in wireless ad-hoc sensor networks." 20th Annual Joint Conference. IEEE Computer Commun. Soc. vol. 3, (1380–1387).

[17] Oz, E. (2009). Management Information Systems. Boston: Course Technology, Massachusetts.

[18] Stair, R. M.& Reynolds, G. W. (2014). Fundamentals of Information Systems. Boston: MA, Cengage Learning Course Technology.

[19] Pierre, T. (2001). *Building Secure Wireless Local Area Networks*. White Papers atColubris.comhttp://download.colubris.com/library/whitepapers/WP-010712-EN-01-00.pdf, Retrieved 13/11/2015.

[20] Paul, S., Yates, R., Raychaudhuri, D. and Kurose, J. (2008) "The cache-and-forward network architecture for efficient mobile content delivery services in the future internet."

[21] Mansfield, Kenneth C, and Antonakos, James L. (2010). Computer Networking from LANs to WANs: Hardware, Software, and Security. Boston: MA, Cengage Learning Course Technology.

[22] Esin, J. O. (2011). *The Evolution of Instructional Technology.Journal of Educational Media & Library Sciences* (*JEMLS*), Bloomington, Vol. 29 No. 1: 15-21.

[23] Shelly, G. B., Gunter, G. A., and Gunter, R. E. (2012).TeachersDiscovering Computers Integrating Technology in a Connected World. Boston: MA, Cengage Learning Course Technology.

[24] Gupta, S., Islam, S., Nurronnabi, K., Hossain, M. S., and Hasan,Z. (2012). Design & Implementation of Cost Effective Wireless Power Transmission Model: Good-Bye Wires. International Journal of Scientific and Research Publications, Vol. 2, Issues 12.

[25] Bolton, M.K. (2008). *US National Security and foreign policy after 9/11: Present at the re-Creation.* New York: Rowman & Littlefield Publishers, Inc.

[26] Stair, Ralph M & Reynolds, George W. (2016). Principles of Information Systems. Boston: MA, Cengage Learning Course Technology.

[27] Ivan M., Glen Z., Joe S., and Hao G. (2008). *Design, Implementation, and Performance Analysis of DiscoSec – Service Pack for Securing WLANs. The* University of Kaiserslautern, Germany.

[28] LAN MAN Standards Committee of the IEEE Computer Society (2004). *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements*. Technical Report 2004 Edition, IEEE Std 802.11i.

[29] Kessler, G. C. (2013) 35 “Paradigms for Cybersecurity Education in a Homeland Security Program.” Journal of Homeland Security Education, Washington, D.C, Vol. 2 no 35.

[30] Kamien, D. (2005). The McGraw-Hill homeland security handbook: The definitive guide for law enforcement, EMT, and other security professionals. New York: McGraw Hill Publishers, Inc.

[31] David, C., and Cliff, P. (2002). *A Path Loss Comparison Between the 5 GHz UNII Band (802.11a) and the 2.4 GHz ISM Band (802.11b)*. Technical report, Intel Corporation England.

[32] Jorgen, B., Clement D., and Joshua H.(1995). *Propagation Measurements and Models For Wireless Communications Channels*. IEEE Communication Magazine, 33(1):42-49.

[33] Wu, C. J., and Irwin, J. D. (2013). Introduction to Computer Networks and Cybersecurity. Boca Raton: CRC Press.

[34] Singer, P. W., and Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

[35] Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[36] Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials. Addison-Wesley. p. 392.*

[37] Halder, D., & Jaishankar, K. (2011) Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global.

[38] Cucinella, C. (*2016).* Border Crossings: *A Bedford spotlight reader.* Boston: Bedford/St. Martins.