Cyber Security and Wireless Technology, a new dimension of emerging technology with some challenges

Saed Fathullah Abuojaylah Saed[1]
M.S (Egypt)
Assistant Lecturer
Head of Department
Dept. of Computer Science
Faculty of Science
University of Derna
AL – Gubba branch
Libya
Email:
Saad_fathallah@yahoo.com

Elmabrook El Saket[2]
M.S (Australia)
Lecturer
Dept. of Computer Science
Faculty of Science
University of Derna
AL – Gubba branch
Libya
Email:
e.elsaket@uod.edu.ly

Mohammed Aijaz Ahmed[3]
M.S (United Kingdom)
Lecturer
Dept. of Computer Science
Faculty of Science
University of Derna
AL – Gubba branch
Libya
Email: m.aijaz@uod.edu.ly

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

KEYWORDS: Wireless Network System, Cybersecurity, Global Community, Cyber-attacks, Fusioncenters, Collaborative.
DOINumber:10.48047/nq.2022.20.22.NQ10324 **NeuroQuantology2022;20(22):3270-3280**

1.0 INTRODUCTION

The internet has enabled virtual control of sensing and control systems in the Crime Investigation sector, allowing for monitoring, operation, prediction, and control of networks. However, many programs and platforms that enable international relationships, business, and collaboration are insecure and vulnerable to terrorist attacks[2]. These systems pose new and increasing hazards and vulnerabilities that have the potential for widespread destruction and communication disruption.

Hence, to provide a national framework for guaranteeing information security and defending cyberspace, the National Cyberspace Security

Response (NCSSR) was established. This organization has three strategic goals in particular:

(i) Prevent cyberattacks on the vital infrastructures of the United States.

(ii) Lower the risk of cyberattacks on the nation as a whole

(iii) Reduce the damage and recovery time from any cyberattacks that do happen.

The organization has developed various strategies to minimize the risks and vulnerabilities of cyber-attacks, establish national cyber security awareness and training programs globally by creating the International Cyberspace Security Cooperation. The need to protect this domain from terrorism has resulted in the formation of the National Cyber Security Division within the Office of Cyber Security and Communication[37]. This division aims to develop and maintain a reliable national cyberspace response system and implement a program to manage cyber risks and protect vital infrastructure.

A terrorist strike on one of our communication systems can corrupt and destroy the majority of computer chips used in communication, transportation, electricity, and other daily life-dependent computer systems. While computer viruses and intrusions have effectively neutralized minor attacks and threats, terrorist groups has continued to exploit technology such as the internet, cell phones, satellite telecommunications, electronic banking, and jetliners to plot activities, pass national borders covertly and spread their ideology. Terrorist communities engage in worldwide terrorism, which knows no boundaries and exists everywhere simultaneously [27].

The United States views cyberwar as an international issue that requires the participation of all nations where cyber activities occur due to the lack of effective communication networks. The 9/11 Commission discovered that around two dozen terrorist groups, have attempted to obtain or create chemical, biological, radiological, and nuclear weapons to attack the United States and its allies. Therefore, the Commission recommended that the United States collaborate with the international community to prevent the spread of such weapons or materials required for their development. To prevent terrorists from traveling, accessing critical infrastructure, and having financial resources to support their organizations, the House of Representatives passed laws. These measures led to the creation of the National Strategy to Secure Cyberspace, which included six initiatives aimed at improving U.S. national security and promoting international cooperation.

Strengthencyber-relatedcounterintelligenceefforts

(i) Improvecapabilitiesforattackattributionandresponse

(ii) Improvecoordinationofrespondingtocyber-attackswithintheUS.nationalsecurityandcommunity

(iii) Work with industry and through international organizations to facilitate dialogue and partnershipsamong international public and private sectors focused on protecting information infrastructures and promoting a global – culture of security[7].

(iv) Foster the establishment of national and international watch-and-warning networks to detect andpreventcyber-attacksastheyemerge.

(v) Encourage other nations to accede to the Council of Europe Convention on Cyber Crime or toensurethat their lawsandproceduresare at leastascomprehensive [2]and[5].

This system was initially created to promote communication, safety, and combat global terrorism. However, it can also be exploited by terrorists to harm free states and nations. Therefore, it is crucial for all global parties involved in cybersecurity to collaborate and work together towards common goals. Any efforts to expand cyber networking or nuclear plants must consider the significant human, material, and financial costs involved in creating and safeguarding the network against misuse and terrorist attacks. While these networks can be effective in promoting collaborative survival, they are equally vulnerable to the disclosure of information that could lead to massive destruction and confusion. Ultimately, the success or failure of these networks depends on who uses them and for what purpose.

The re-organizations have had a significant impact on shipping ports, where security measures have been strengthened. In October 2006, the SAFE Port Act was passed to enhance the authorities responsible

for port security. This Act was an extension of the USA Patriot Act and empowered the Department of Homeland Security to use any of its law enforcement agencies to detect and intercept terrorists and terrorist acts.

As a result, more money and manpower were deployed to the various ports of entry and exit. These ports are susceptible to terrorists who may use them to export Weapons of Mass Destruction or guns. Any terrorist attacks on ports could result in the loss of life and a negative impact on national and international business. The economy is crucial to every country, and commerce involves local citizens and governments, as well as foreign citizens and their governments. Therefore, the DHS has successfully implemented intervention steps at key ports and areas in the shipment process using the Container Security Initiative Plans to prevent the shipment of terrorist materials [2]. The international community collaborated with the United States to implement anti-terrorist measures, such as Operation Safe Commerce. This allowed American workers to inspect and handle materials exported to the US from foreign ports and countries, resulting in no reported incidents of US ports being penetrated. The immigration service was integrated into the Department of Homeland Security to ensure legal and non-criminal entry and exit from the US. The Office of Detention and Removal Operations was given authority to detain and deport illegal immigrants. The US borders were equipped with physical barriers, unmanned vehicles, and imaging devices to monitor and prevent terrorist attacks[29]. As a result, terrorist suspects have been apprehended on the Canadian-USA borders attempting to smuggle bomb-making devices to attack Los Angeles airport.

The USA has been successful in preventing terrorist attacks on its soil since 9/11. However, there have been some incidents where terrorists have managed to slip through airport security, such as the Nigerian-born Christmas Day Bomber who was caught when his bomb failed to detonate in the year 2009. This shows that the security system is not foolproof and needs to be improved. One way to do this is by creating Fusion Centers that can provide better surveillance with higher quality and more detailed information [22].

1. FUSIONCENTERS

The creation of Fusion Centers by the Bush Administration was a strategic move to enhance collaboration among law enforcement professionals with diverse backgrounds in intelligence gathering. The aim was to detect, deter, and prevent terrorist attacks within the country. Fusion Centers provide an efficient mechanism for exchanging information and intelligence, maximizing resources, streamlining operations, and improving the ability to fight crime and terrorism by analyzing data from various sources [6].

The ultimate goal of Fusion Centers is to bring together government, law enforcement, public safety, and the public sector to work towards a common purpose of safeguarding the homeland and preventing criminal activities. These centers have been established across the nation over the past decade and have become a more manageable way of addressing terrorism and crime collaboratively and inclusively. They involve law enforcement offices, the office of public safety, such as fire departments and medical emergency responders, and the public sectors, all united in a single effort to fight crime and prevent another 9-11-like attack.

One of the advantages of Fusion Centers is that they are able to tap into the best from all walks of life and technical fields, bringing to the table a diverse assortment of skills needed to fight crime. As a result, the Center becomes a microcosm of the community, composed of representatives from all sectors of that community. The Center engages in training on intelligence gathering, analysis, calibration, and dissemination to enable its members to make informed decisions about activities and actions that may pose a threat to the safety of the society.

Yes, the concept of Fusion Centers is an innovative approach to addressing and preventing crimes in society. The idea is that if there are any homegrown terrorists who engage in activities within the society, someone should be able to notice changes in their behavior and report it to the authorities. The innovation lies in the fact that everyone is considered capable of acting as an informant and contributing to the safety of society.

Previously, security and public safety were considered to be the responsibility of the police and law enforcement agencies. The police, CIA, and FBI had almost complete control over these situations. However, the introduction of Fusion Centers has demystified intelligence activities and made it possible for anyone with the character traits of honesty and a determination to protect the nation to contribute.

Fusion Centers have also shifted the focus of allegiance from the Unit of Origin to the Center of Activities. This requires a shift in organizational behavior and protocol as the focus is now on the Center rather than on local precincts or former areas of employment. This shift poses a true test of loyalty as conflicts may arise in the dissemination of information across jurisdictions where each officer or person may feel a particular allegiance to their home precinct or jurisdiction. The concept behind these centers is that by working together, better results can be achieved. To achieve this, it would be useful to provide salaries that are commensurate with the level of training and experience of each member, empowering them to be independent of their feeder groups. This approach does not diminish the loyalties of members to their intelligence offices, but rather ensures continuity of operations through shared experience and information. Each intelligence agency, such as the NIA, FBI, CIA, DoJ, DOD, and DNS, should collaborate fully and even train lay individuals who have dedicated time and effort to solving crime in society. Many members from the local neighborhood can have greater leverage among their friends and colleagues who may trust them with information, compared to unfamiliar FBI and CIA agents. Traditional agencies should not consider these centers as upstarts or presumptive individuals who pretend to be intelligence agents. Rather, they are genuine individuals who want to help the intelligence community in their own ways to solve crimes.

As the world evolves, terrorists are becoming more innovative and using advanced technology to carry out their activities. In response to this, Fusion Centers have been established as a cost-effective way to counter these threats [21]. Collaboration is the key principle that holds these Centers together, as it allows for increased capacity, communication, and continuity of service while reducing duplication. However, education of the public is necessary to avoid service duplication and waste.

Fusion Centers discard theoretical restrictions in favor of best practices and experimentation to determine what works best. The focus is on motivating citizens and agents to work collaboratively to prevent criminal activities. It is important to create a unique link and relationship between the Fusion Centers and professional intelligence agencies [25], as well as to provide education and training to lay citizens on intelligence and protocol, technology, and collaborative co-existence.

To facilitate the success of the Centers, a reasonable budget should be allocated to cover training, materials, equipment, logistics, and other necessary resources. Each Center should be a fully independent unit with its own organizational chart, division of labor, and specialization. Members should be selected from top-performing feeder units and stakeholders to facilitate training and ensure that the best knowledge is shared.

While enhancing Fusion Centers may not be easy, it is a welcome innovation. The success of these Centers in the US should inspire other nations to implement similar techniques to ensure security. Security is a collective venture, and it is essential to find new ways to guarantee security without making it too expensive.

2. An Overview of Wireless Technology

The evolution of wireless technology has led to the widespread acceptance and adoption of wireless services [35, 34]. This technology has extended coverage and connections to a variety of devices and application programs. It has contributed to the changeover from analog connections to digital connections, creating productivity enhancements and effective communication for the global community [28]. However, the vulnerability of wireless networks presents significant challenges and risks that continue to threaten wireless security. There is an urgent call to decrease the vulnerability of wireless network systems to uphold confidentiality, ensure integrity, and provide constant protection of wireless network operation

[8].

The advantages of wireless services include allowing important information to be accessible to a large segment of the global community, empowering individuals, organizations, local, state, and federal government agencies, and nations by transforming analog (wired-cable) to digital (wireless) services [17, 9]. It has been instrumental in organizing, transmitting, and preserving important documentation and learning endeavors around the world [19]. However, wireless service users in various countries are subjected to unlawful tracking, monitoring, and data interception that tend to undermine and overturn the fundamental rights of privacy and freedom of expression.

The future of wireless technology is limitless, with 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 [23, 32]. The prominence of the wireless service system is validated primarily based on usage convenience, cost efficiency, and almost effortlessness of integration, connection, and universal compatibility with major wireless network providers [26]. However, challenges such as unauthorized access points, dissemination of information, and spoofed medium access control addresses and wireless local area network vulnerabilities still exist [24]. It is important to continue to establish a well-conceived alliance with regulatory agencies to minimize emerging wireless services challenges.

3. An Overview of Cyber security and Cyberspace

The article discusses the importance of cyber security for safeguarding sensitive data, sustaining operations, and protecting national infrastructure. Cyber security involves technologies, processes, and practices aimed at protecting networks, computers, programs, and data from unauthorized access, damage, or attack. It requires an understanding of potential threats and the implementation of various strategies such as identity management, risk management, and incident management. Cyber security also involves both physical and virtual security. Elements of cyber security include application security, information security, network security, disaster recovery, operational security, and end-user education.

The traditional approach to cyber security has been insufficient due to the rapidly evolving nature of security risks. A more proactive and adaptive approach is needed, which involves continuous monitoring and real-time assessments [36]. The global cyber security market is expected to reach $170 billion in 2020. The article presents a notional cyber security landscape of the Reference Diagram, which introduces the concepts and terminology of cyber security but does not accurately represent real cyber security defense and can apply to physical and virtualized environments.

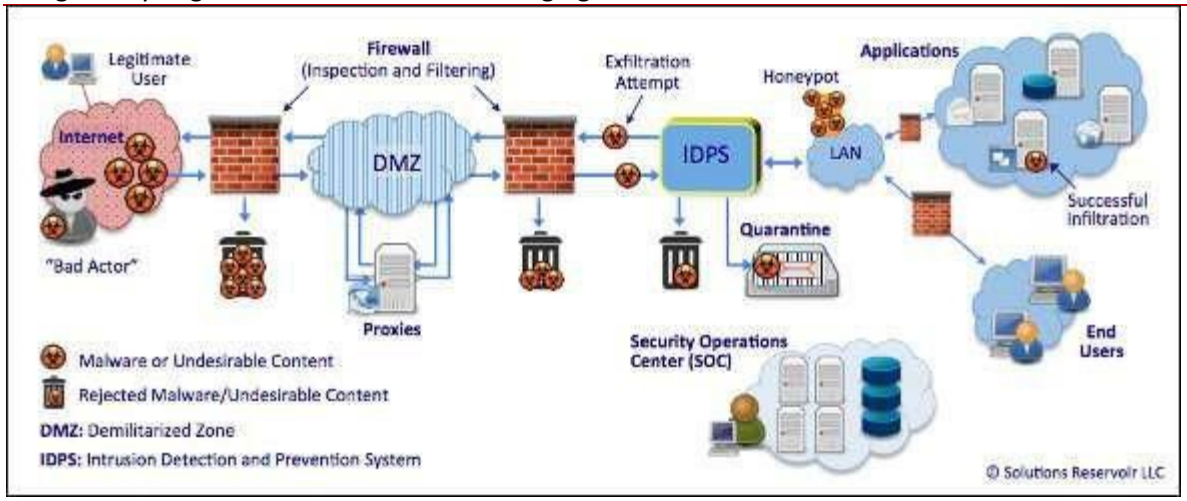

Fig. 1:Reference Diagram of Notional view of the cybersecurity landscape (Adoptedfrom[31])

In the world of cyber security, bad actors attempt to achieve their goals by taking advantage of

vulnerabilities in computer systems. These vulnerabilities are flaws in the software or code that allow malicious software (malware) to be installed and executed without the user knowing. The battle between cyber security and bad actors is about fixing vulnerabilities before they can be exploited, and discovering and fixing new ones as quickly as possible.

A "zero-day attack" is when vulnerability is exploited before a security patch or update is available, making it especially dangerous. One example of this is the Heartbleed vulnerability in OpenSSL, which went undetected for two years before being discovered and patched.

Cyberspace is vulnerable to a wide range of risks, including physical and cyber threats. Cyber criminals and nation-states exploit vulnerabilities to steal information and money, and can even disrupt or threaten essential services. Traditional crimes like financial fraud and intellectual property violations are also committed through cyberspace, with significant consequences for individuals and the economy.

Securing cyberspace is difficult because malicious actors can operate from anywhere in the world and cyber networks are complex. The linkages between cyberspace and physical systems also create new risks, especially as technology becomes more integrated with critical infrastructure. Strengthening the security and resilience of cyberspace is an important mission for homeland security to protect individuals and our economy from potential harm or disruption caused by cyber events.

AnOverviewofCybercrime

Cybercrime, or computer crime, is a type of crime that involves the use of a computer or network. The computer can be used to commit a crime or can be the target of a crime. Cybercrimes are defined as offenses that are committed with a criminal motive to harm an individual or group of individuals, intentionally causing physical or mental harm, reputation damage, or loss using modern telecommunication networks such as the internet and mobile phones.

Cybercrime can threaten a nation's security and financial well-being, and issues surrounding these crimes have become high-profile, particularly those involving hacking, copyright infringement, child pornography, and child grooming [30, 11]. Privacy issues also arise when confidential information is intercepted or disclosed, lawfully or otherwise.

Cybercrime is a broad category of offenses that involve 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, the 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, are intended only to disrupt or destroy computer networks. Internet security experts estimate that the global annual cost of cybercrime approaches $1 trillion.

A significant amount of cybercrime involves 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 can 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 [23, 15]. 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.

TheRiseofthe Cyber Threats

The Internet of Things (IoT) is becoming more integrated into our daily lives, but with this integration comes growing security risks that are constantly evolving. Due to the always-on nature of technology and a lack of security awareness on the part of users, cyber-attacks are no longer a question of if, but when they will happen.

Cybercriminals are constantly developing new techniques to breach the security of established organizations, gaining access to everything from intellectual property to individual customer information. They do this in order to cause damage, disrupt sensitive data, and steal information. Every day, their attacks become more sophisticated and harder to detect [28, 32]. This ongoing development means that we cannot predict exactly what kinds of threats will emerge in the future, but we can be certain that they will be even more dangerous than those of today. Additionally, as old sources of these threats fade, new sources will emerge to take their place.

Despite this uncertainty, it is important to be clear about the type of security controls that are needed. Effective cybersecurity is becoming increasingly complex to deliver. The traditional organizational perimeter is eroding, and existing security defenses are coming under increasing pressure. While point solutions, such as antivirus software, intrusion detection systems (IDS), intrusion prevention systems (IPS), patching, and encryption, remain key controls for combating known attacks, they become less effective over time as hackers find new ways to circumvent them [11]. Therefore, it is necessary to have a comprehensive and dynamic cybersecurity strategy that includes continuous monitoring, threat intelligence, and incident response capabilities.

3.1 ChallengesinWirelessSecurity

Wireless LANs (WLANs) have become increasingly popular in recent years due to their lower installation costs and improved efficiency for mobile users [18, 7, 30]. However, a major challenge in deploying WLANs is the unpredictable nature of signal propagation, which depends on factors such as building materials, layout, and obstacles.

In addition, WLANs pose security risks as they extend beyond physical boundaries and require additional mechanisms for access control [10]. Current access control solutions either provide little protection or incur high management costs. As a result, many WLANs operate with insecure configurations and are vulnerable to attacks [1, 33, 12].

Studies have shown that a large percentage of WLANs lack basic security measures, making them susceptible to abuse. As the number of deployed access points continues to rise, it becomes easier for malicious users to find vulnerable networks [16, 15].

In conclusion, while WLAN technology has many benefits, it also introduces new security challenges that require cheaper yet effective solutions to ensure the protection of networks and their users [14, 4, 13].

3.2 RisksandVulnerabilitiesofWirelessNetworks

Along with the many conveniences and cost-saving advantages to wireless networks, there are also someinherentrisksandvulnerabilities.

3.2.1 TheNatureoftheWirelessMedium

Wireless networks are more vulnerable to attacks compared to traditional wired networks. As mentioned, wireless signals can travel through walls and other physical barriers, making it easier for hackers to intercept and sniff the traffic.

In addition, the nature of the wireless medium is shared, which means that multiple users can access the same network simultaneously [38]. This makes it easier for an attacker to gain access to the network and carry out malicious activities. Moreover, wireless networks are often less secured because they rely on encryption and authentication protocols that are susceptible to hacking.

To mitigate these risks, it is important to implement strong security measures such as using robust

encryption and authentication protocols, deploying firewalls and intrusion detection systems, and limiting the number of devices that can connect to the network. Regular security audits and updates are also crucial to ensure that the network remains secure against the latest threats.

InsecureWirelessNetworkDevices

Wireless LAN devices like access points and user stations that lack security can be a significant threat to both the wireless and wired networks, which makes them a prime target for hackers.

InsecureAccessPoints

Access points can have security vulnerabilities due to improper configurations and design flaws. Some access points are shipped with insecure default configurations, such as pre-configured default passwords, broadcasted SSIDs, and no encryption or authentication requirements [31]. If deployed with these default settings, they can become gateways for hackers to access both the wireless and wired networks.

Hackers can also convert laptops into "soft" access points by using various software programs like HostAP, Hotspotter, or Airsnark or by using a USB wireless adapter. By using soft APs, a hacker can cause a legitimate user to connect to the hacker's laptop, which compromises the user's machine.

InsecureUserStations

One common attack is called "Man-in-the-Middle" (MitM) attack. In this attack, the hacker intercepts the communication between two wireless devices and can eavesdrop or alter the communication. The hacker can use this technique to steal sensitive information or spread malware.

Another attack is called "Rogue Access Point" attack. In this attack, the hacker sets up a fake wireless access point that mimics a legitimate one[20]. When users connect to this fake access point, the hacker can capture their credentials or redirect them to malicious websites.

A third attack is called "Evil Twin" attack. In this attack, the hacker sets up a fake wireless access point with a similar name to a legitimate one. When users unknowingly connect to the fake access point, the hacker can launch further attacks.

To prevent these attacks, it is important to implement strong security measures for wireless user stations, such as using secure authentication protocols, regularly updating firmware and software, and implementing proper access control policies.

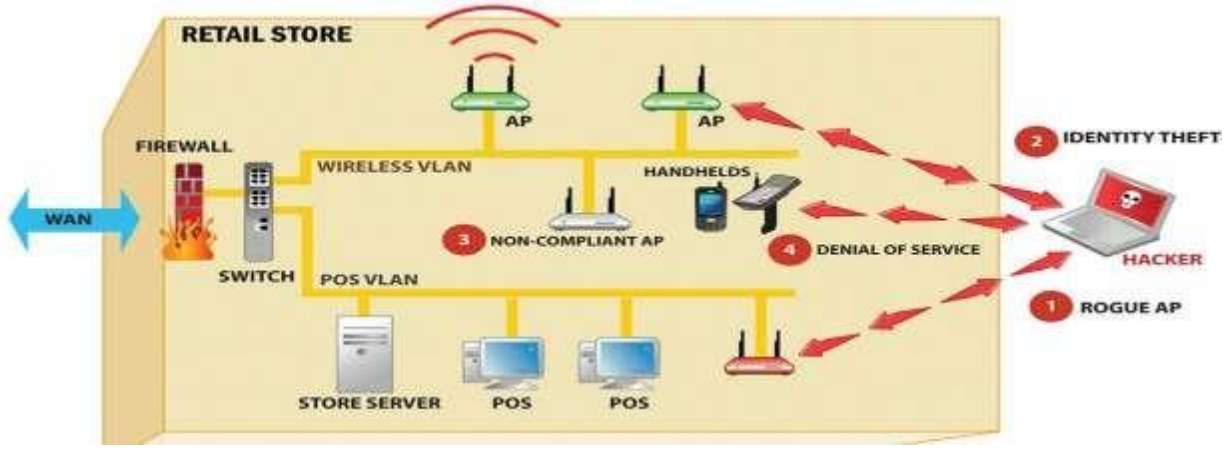

Fig.2:A common wireless network security risks(Adopted from[26])

4. CONCLUSION

The passage above highlights the challenges and complexities associated with the unrestricted application of the Bill of Rights, globalization of the internet and cyber activities, and the proliferation of nuclear energy for peaceful purposes. While globalization has made communication and movement easier and faster, it has also made it difficult to enforce borders between countries. This has come at a great cost to humanity, as conflicts and conflicting interests have become an everyday occurrence.

In order to safeguard the progress that has been made and continue to make progress, we must find

better ways to control and prevent destruction caused by human nature [3]. America's efforts to combat terrorism are less effective when the rest of the global community does not join in identifying and addressing potential threats.

The methods employed by the United States in their fight against terrorism, including travel restrictions and controls, the establishment of the Department of Homeland Security, the creation and operation of Fusion Centers, and the collaboration between various intelligence-gathering and intelligence-sharing organizations, have been highly effective. Other global powers, which have the capability to develop and enjoy unrestricted freedom in areas such as cyber communications, nuclear energy, and travel, should look to emulate or duplicate these methods in order to combat the threat of terrorism.

REFERENCES

[1] Bolton, M.K. (2008). *US National Security and foreign policy after 9/11: Present at the re-Creation.* NewYork:Rowman&LittlefieldPublishers, Inc.

[2] Bullock, J, Haddow, G, Coppola, D. &Yeletaysi, S. (2009). *Introduction to homeland security: Principles ofall-hazardsresponse*.3rd Edition.Burlington, MA:ElsevierInc.

[3] Cucinella,C.(*2016).*BorderCrossings:*ABedfordspotlightreader.* Boston:Bedford/St.Martins.

[4] David,C.,andCliff,P.(2002).*APathLossComparisonBetweenthe5GHzUNIIBand(802.11a)andthe2.4GHzISMBand (802.11b)*.Technicalreport,IntelCorporationEngland.

[5] DepartmentofHomelandSecurity.(200*3).Anationalstrategytosecurecyberspace.* Retrieved on9/25/2015 fromwww.dhs.gov.

[6] DepartmentofHomelandSecurity.(2013).*FusionCentersGuidelines:Developingandsharinginformationand intelligence in a new era...* Retrieved on 5/29/2016 fromhttp://www.it.ojp.gov/fusioncenterguidelines/intro.html

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

[8] Fagin,J.A.(2006).*WhenTerrorismstrikesathome:DefendingtheUnitedStates.*Boston: PearsonEducation,Inc

[9] Frenkiel,R.Badrinath,B.,Borres,JandR.Yates,R.(2000)–*Theinfestations Challenge:Balancingcost and ubiquity in delivering wireless data*. IEEE Pers. Commun., vol. 7, no. 2, (66-71).

[10] Gupta, S., Islam, S., Nurronnabi, K., Hossain, M. S., and Hasan,Z. (2012). Design & Implementation ofCost Effective Wireless Power Transmission Model: Good-Bye Wires. International Journal of Scientificand ResearchPublications, Vol. 2, Issues12.

[11] Halder,D.,&Jaishankar,K.(2011)CybercrimeandtheVictimizationofWomen:Laws, Rights,andRegulations. Hershey, PA, USA:IGIGlobal.

[12] 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.

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

[14] Kamien,D.(2005).TheMcGraw-Hillhomelandsecurityhandbook:Thedefinitiveguideforlawenforcement,EMT,and other securityprofessionals.NewYork:McGrawHillPublishers,Inc.

[15] Kessler,G.C.(2013)35–ParadigmsforCybersecurityEducationinaHomelandSecurity Program.|| JournalofHomelandSecurity Education,Washington, D.C,Vol. 2no35.

[16] 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.

[17] Lun,D.S.,Koetter,M.,Koetter,R.andEffros, M.(2008)–Oncodingforreliablecommunicationover packet networks‖.Phys. Commun., vol. 1,no. 1, (3–20).

[18] Mansfield, Kenneth C, and Antonakos, James L. (2010). Computer Networking from LANs to WANs:Hardware, Software, and Security.Boston:MA,CengageLearningCourseTechnology.

[19] 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).

[20] Moore,R.(2005)"Cybercrime:Investigating High-TechnologyComputerCrime,"Cleveland, Mississippi:AndersonPublishing.

[21] OfficeofJusticeProgram.(2003).*TheNationalCriminalIntelligenceSharingPlan:Solutions andapproaches for a cohesive plan to improve our nation's ability to develop and share criminal intelligence*.Retrieved24/04/2016fromhttp://www.fas.org/irp/agency.

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

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

[24] Paul,S.,Yates,R.,Raychaudhuri,D.andKurose,J.(2008)–Thecache-and-forwardnetworkarchitecturefor efficientmobilecontent delivery services inthefutureinternet.

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

[26] Pierre,T.(2001).*BuildingSecureWirelessLocalAreaNetworks*.WhitePapersatColubris.comhttp://download.colubris.com/library/whitepapers/WP-010712-EN-01-00.pdf,Retrieved 13/11/2015.

[27] Popescu,G.(2016).Bordersintheeraofglobalization.*BorderCrossings:ABedfordSpotlightReader.* NewYork:Bedford/St. Martins, 273-293.

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

[29] Sauter,M.A.&Carafano,J.J.(2005).*HomelandSecurity:Acompleteguidetounderstanding,preventing, andsurviving terrorism*. NewYork: McGraw-Hill CompaniesInc.

[30] Shelly,G.B.,Gunter,G.A.,andGunter,R.E.(2012).TeachersDiscoveringComputersIntegratingTechnologyinaConnected World.Boston:MA, Cengage Learning Course Technology.

[31] Singer,P.W.,andFriedman,A.(2014).CybersecurityandCyberwar:WhatEveryoneNeedstoKnow.Oxford UniversityPress.

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

[33] Stair, Ralph M & Reynolds, George W. (2016). Principles of Information Systems. Boston: MA, CengageLearningCourse Technology.

[34] Theodore S. R. (2002). *Wireless Communications - Principles and Practice*. Prentice-HallPTR,2ndedition.

[35] Tse,D.,andViswanath,P.(2005). *FundamentalsofWirelessCommunication*.NewYork,CambridgeUniversityPress.

[36] WarrenG.Kruse, JayG.Heiser(2002).*Computerforensics:incidentresponseessentials.Addison-*

Wesley.p. 392.

[37] Watts,M.(2007).RevolutionaryIslam-Violent geographies,NewYork:Routledge.175-204.

[38] Wu,C.J.,andIrwin,J.D.(2013). IntroductiontoComputerNetworksandCybersecurity.BocaRaton:CRCPress.