Cross Current International Journal of Economics, Management and Media Studies
*Abbreviated Key Title: Cross Current Int J Econ Manag Media Stud*
**ISSN:** 2663-2462 (Print) & Open Access
**DOI:** 10.36344/ccijemms.2021.v03i01.001

Volume-3 | Issue-1|March, 2021 |

Review Article

# Internet of Things and Cyber Terrorism

**Pranab Kumar Goswami[1*], Dr. Sunandan Baurah[2], Dr. Laba Thakuria[3]**
[1]Research Scholar, Assam Downtown University, Assam, India
[2]Dean, Eng. & Tech. Dept, ADTU, Assam, India
[3]Dy. Controller of Examinations, AHSEC, Assam, India

***Corresponding author:** Pranab Kumar Goswami

| **Received:** 26.12.2020 | **Accepted:** 11.01.2021 | **Published:** 23.03.2021 |

**Abstract:** The Internet of Things (IoT) is the next technological leap that will introduce significant improvements to various aspects of the human environment, such as health, commerce, and transport. The IoT represents a technologically optimistic future, where the objects will be able to utilize the Internet and make intelligent collaborations with each other anywhere and anytime. In particular, the IoT combines a wide range of technologies, such as sensors, actuators, Internet, cloud computing as well as many communication infrastructures. As the IoT continues to become more hyperconnected it will be imperative that cyber security experts to develop new security architectures for multiple platforms such as mobile devices, laptops, embedded systems, and even wearable displays. The futures of national and international security rely on complex countermeasures to ensure that a proper security posture is maintained during this state of hyperconnectivity. The heterogeneity of various technologies which the IoT combines increases the complexity of the security processes, since each technology is characterized by different vulnerabilities. Furthermore, the tremendous amounts of data which is generated by the multiple interactions between the users and objects or among the objects make harder their management and the functionality of the access control systems. To protect these systems from exploitation of vulnerabilities it is essential to understand current and future threats to include the laws that drive their need to be secured.

**Keywords:** Internet of Things, Cyber Attack, Cyber Security, Social Networks, Virtual Communication, Network Attacks, Information Assurance, Cyber Terrorism.

## BACKGROUND ON RESEARCH

Information Technology has transformed the global economy and connected people and markets in ways beyond imagination. With the Information Technology gaining the centre stage, nations across the world are experimenting with innovative ideas for economic development and inclusive growth. It has also created new vulnerabilities and opportunities for disruption. Cyber Security has become a matter of national, international, economic, and societal importance that affects multiple nations [1]. Cyber-attacks happen on all types of organizations and individuals. They can start in many different places, including any device that's connected to the Internet. Experts and government officials have warned for years of cyber terrorism as a threat to national security [2]. This becomes highly problematic in our modern society when we have devices such as copy machines that are hooked up to the Internet in order to update themselves report usage, install software, etc. Having all these devices connected to the Internet increases our exposure and vulnerability. These malicious attacks can affect one individual to entire government entities. These attacks can be done with a few lines of code or large complex programs that have the ability to target specific hardware. The authors investigate the attacks on individuals, corporations, and government infrastructures throughout the world. Provided will be specific examples of what a cyber terrorist attack is and why this method of attack is the preferred method of engagement today. The authors will also identify software applications, which track system weaknesses and vulnerabilities. As many national governments have stated, an act of cyber terrorism is an act of war; it is imperative that we explore this new method of terrorism and how it can be mitigated to an acceptable risk.

Information Assurance (IA) is defined as the practice of protecting and defending information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This definition also encompasses disaster recovery, physical security, cryptography, application security, and business continuity of operations. To survive and be successful, an enterprise must have a disaster recovery strategy and response plan in place to mitigate the effects of natural disasters (e.g., floods, fires, tornadoes, earthquake, etc.), inadvertent actions

Quick Response Code

**Journal homepage:**
http://crosscurrentpublisher.com



**Citation:** Pranab Kumar Goswami *et al* (2021). Internet of Things and Cyber Terrorism. *Cross Current Int J Econ Manag Media Stud*, *3*(1), 1-4.

by trusted insiders, terrorist attacks, vandalism, and criminal activity. In order to lay the groundwork for this review properly, it is essential to detail current processes techniques being utilized by officials within the government to accredit and certify systems to include their TA enabled products [3]. Since the 1990s users have exploited vulnerabilities to gain access to networks for malicious purposes. These cyber attacks can be initiated from anywhere in the world from behind a computer with a masked Internet Protocol (IP) address. This type of warfare, cyber warfare, changes the landscape of war itself by removing the need to have a physically capable military and requires the demand for a force that has a strong technical capacity e.g. computer science skills. Many developed countries have come to understand that this is an issue and has developed policies to handle this in an effort to mitigate the threats.

## LAWS AND POLICIES TO COMBAT TERRORISM

International law circumscribes nations' authority to exercise jurisdiction in matters that implicate foreign interests or activities. Each nation must avoid undue encroachment on other countries' jurisdictions or territories. The events of 9/ll not only changed policies with the United States of America (U.S.A.) but also policies with other countries in how they treat and combat terrorism. The United Nations (U.N.) altered Article 51 of the U.N. charter. This article allows members of the U.N. to take necessary measures to protect themselves against an armed attack to ensure international peace and security. Israel is a country with some of the most stringent policies towards national and international security. The United Kingdom (U.K.) has the Prevention of Terrorism Act 2005 and the Counter-Terrorism Act 2008 which was issued by Parliament. The USA PATRIOT was signed into law by President George W. Bush in 2001 after September 11, 2001 [4]. This act was created in response to the event of 9/11 which provided government agencies increased abilities. These increased abilities provided the government rights to search various communications such as email, telephone records, medical records, and more of those who were thoughts of terrorist acts[4]. Whereas, after the 26/11 attack, the Indian Government had brought into effect a set of proposed amendments to the Information Technology Act 2000, which has specific provisions for combating cyber terrorism.

## CORE CHARACTERISTICS OF CYBER TERRORISM

Cyber terrorism has some universal characteristics, which are as follows:

1. It is done to convey a particular destructive or disruptive message to the government(s).
2. There are various methods to convey this message, viz., through denial of services, sending threatening emails, defacing of government websites, hacking and cracking of crucial governmental systems or 'protected systems' [5], disrupting the civil amenities through destroying the proper working of the digital information systems, etc.
3. It could affect the computers and the networks as a whole, it could also affect the governing system, and it could affect the population of target area to create threat.
4. Computer and digital communication technology are used as a main tool to achieve extremist purposes.
5. The whole act could be motivated by religious, social or political ideologies.
6. It is mostly done by hi-tech offenders.

## INTERACTION BETWEEN HUMAN & COMPUTER

The number of devices on the Internet is growing exponentially. There are currently 26 billion devices connected to the Internet; experts suggest that this figure is supposed to grow to 41.6 billion by 2025. Future national and international threats that will be directly correlated to the Internet will be many as more devices are added to the Internet the problem of security also multiplies. Our dependence and interdependence with the Internet creates new challenges as the more devices that are put online, the more exposure or vectors we are creating. As more applications for technology and wireless technologies are adopted, we are going to see this grow even further. We already have some self-driving cars, but they are not widely adopted yet or available to the public. When this does happen, we are going to see another exponential growth rate and the number of connected devices as each automobile will constitute at least a single IP address if not probably more. Communication is the on-going and never ending process through which we create our social reality. Never in history has this been truer, as the computing and communication platforms that we have today far exceed anything that has ever been planned or projected. Information technology has radically altered the process in the way people learn and communicate. As these technologies are weaved into our lives, so are the dangers.

## MODUS OPERANDI FOR NETWORK ATTACKERS

A network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity. Network attacks pose a significant challenge to information systems due to the dramatic impact such attacks have on computer networks. Such attacks could paralyze entire networked systems, disrupt services, and bring down entire networks. In the recent years, network attacks have increased exponentially and have evolved rapidly in complexity to evade traditional network defences (e.g. intrusion detection systems, firewalls, etc.). As computer networks grow and evolve

to include more applications and services; malicious hackers continue to exploit inevitable vulnerabilities in network based applications. This, in turn, creates a fertile ground for hackers to develop and implement complex attacks and break into critical information assets. Hackers use a portscan attack, one of the most popular reconnaissance techniques, to break into vulnerable network services and applications. Most of the network services need to use TCP or UPD ports for their connections. Further, a port scan allows hackers to listen via open and available ports by sending a message to each port one at a time and waiting to receive a response. Once the port replies to a message, a hacker would then dig further and attempt to find potential vulnerabilities, flaws, or weaknesses in that port and ultimately launch a port scan attack which can compromise a remote host. The consequences of port scans are numerous and diverse ranging from draining network resources, to congesting network traffic, to actual exploitation of network devices. Another attack, which is known as IP address spoofing or IP spoofing, refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of hiding the true identity of the packet (sender) or impersonating another host on the network. IP address spoofing is a form of denial of service attacks where attackers attempt to flood the network with overwhelming amounts of traffic without being concerned about receiving responses to attack packets. Implementing packet filters at the router using ingress and egress (blocking illegitimate packets from inside and outside the network) is the best defense against the IP spoofing attack.

## HAZARDS OF SOCIAL NETWORKS

The significance of the virtual communication, its privacy and security problems comes into prominence by the rapid development of online social networks. Virtual communication has become a distinct area of interest for many as it has become second nature and also weaved into our everyday life. People tend to create a social reality that is based on the connection to the Internet and using tools that assist communication. These tools have danger sides that a vast majority does not see or think about on a daily basis. Currently, there has never been a higher danger in the social networks for the public than there is now. This danger is easily spread to everyone who use this mode of communication based that people unintentionally make themselves vulnerable. With a connection to a vast number of social networks, people are easily consumed by submitting personal information via the Internet. The time is now for the public to understand where they stand in the future of the Internet connectivity and what they can do to assist or lessen this danger.

## INTELLIGENCE GATHERING FROM OTHER COUNTRIES VIA INTERNET CONNECTIVITY

With the high trend of social networking scattering the Internet's surface, social media are available in every country, thus increasing the use of Internet connectivity. This availability of information helps create a mix between businesses and customers in terms of how information is related. Intelligence gathering is one way of using the available information and putting it to good use depending on the source of the receiver. Businesses can use this type of work by targeting special performance enhancing customers who are local and idealistic to the values that the company brings to the table. It is also valuable in terms of online social marketing because it is feasible for businesses to assist with advertising online as compared to physical. An international point of view that collaborates intelligence gathering can be noted based that Internet connectivity is what brings users from various locations together in one normal new setting. This virtual environment setting becomes a normal atmosphere for many users based that most users are not currently satisfied with physical aspects of businesses. Using intelligence gathering from other countries helps institutions and businesses gather a list of potential customers from varying backgrounds that can help modify the existing performance of the business. A modification for a business is looked at by an increased way information is displayed and given to customers. This method should increase sales within the business, such that there is an absolute return on investment for the business. Institutions can use intelligence gathering to help create new avenues for students to prosper. With this, distance learning and online collaborative learning can be assisted such that these are the main areas that are affected by the online networking. These changes also increase the power and connectivity of the specific institution to the student learner in the sense that they feel connected and secure. These are the most important items in any aspect of online networking in a business or educational field.

## CYBER SECURITY MEASURES TAKEN BY THE INDIAN GOVERNMENT

India is gearing up to bring in new encryption and privacy policies to take on growing cyber security challenges. It may also amend the existing laws to make cyberspace more secure. India has taken steps in establishing institutions and released the National Cyber Policy back in the year 2013 to deal with cyber security issues. In recent times, India has launched a series of cyber security initiatives to digitally empower its citizens and safeguard cyberspace. In the wake of increasing cyber threats, India appointed its first Chief Information Security Officer (CISO). The appointment underlines India's commitment to combating cyber attacks. It will help India develop the vision and policy to fight cybercrime and manage cyber security more effectively. Indian Government has taken a number of legal, technical and administrative policy measures for addressing cyber security. This includes National Cyber Security policy (2013), Framework for enhancing Cyber Security (2013), enactment of Information Technology (IT) Act, 2000 and setting up of Indian

Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC) under the IT Act, 2000.

The then Minister of Defence of India, Late Manohar Parrikar in a reply to a starred Question in Lok Sabha stated that Cyber-crime has emerged as one of the foremost security threats at global level including at the national level. Since armed forces function on exclusive private networks, these establishments have not witnessed institutional attacks. Cyber attacks are largely faced by internet connected Personal Computers (PCs) and these relates to unauthorized data access, malware infestation, denial of service, etc [6].

## CONCLUSION

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation-states and non-state actors. It can be concluded that cyber terrorism in all its forms affect the civilians psychologically and financially. Also it was observed that public confidence does not drop significantly in these situations. It was found that apart from the major advantages provided by IOT, it complicates the situation in the advent of cyber attacks by giving out a huge attack space to malicious attackers. In the future, we need to focus on securing the IOT so that we can reduce the anxiety and threat perceptions of people in these circumstances and think of having common laws to deal with perpetrators because today the laws for cybercrime are national in their implementation while as the internet is borderless and international by definition. The unique characteristics of most important cyber breaches, examines the associated costs to be paid by the industries for these cyber events and finally looks at its effect on psychological well-being of the population as well as the public confidence in government.

## REFERENCES

1. Walker, J. J. (2012). *Cyber Security Concerns for Emergency Management, Emergency Management*. Retrieved from http://www.intechopen.com/books/emergency-management/cyber-security-concernsfor-Emergeneymanagement
2. Cavelty, M. D. (2008). Cyber-terror—looming threat or phantom menace? The framing of the US cyber threat debate. *Journal of Information Technology & Politics*, *4*(1), 19–36. doi:10.1300/J516v04n01_03
3. Dawson, M. E. Jr, Crespo, M., & Brewster, S. (2013). DoD cyber technology policies to secure automated information systems. *International Journal of Business Continuity and Risk Management*, *4*(1), 1–22. doi:10.1504/IJBCRM.2013.053089
4. Bullock, J., Haddow, G., Coppola, D., & Yeletaysi, S. (2009). *Introduction to homeland security: Principles of all-hazards response* (3rd ed.). Burlington, MA: Elsevier Inc.
5. Section 70 of the Information Technology Act, 2000 (amended in 2008) describes protected system and regulations related to it.
6. Lok Sabha, Starred Question No. 400, 12 August 2016.