International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 09 | Sep 2018 www.irjet.net p-ISSN: 2395-0072

Cyber Security – Current Issues and Challenges among Global Countries

K. Vinod Kumar[1], Suram Madhusudhan[2]

[1,2] *Assistant Professor, Department of CSE, RGUKT, Idupulapaya, Andhra Pradesh*

Abstract: – *Data was considered as an important aspect of any political problem like power or any issue related to supreme diplomacy for a very long time. Since the 1990s, its role into global market, it was categorized and its importance for many other issues has increased, because of information and communication technology (ICT) into all aspects of everyone's daily life. Parallel, issues of cyber-(in)-security have become a major security issue. In this paper, the cyber-(in)-security protocol is unwrapped in four sections, with the first providing the necessary technical background information and second the information infrastructure is inherently insecure, thirdly on how computer vulnerabilities are conceptualized and lastly on ways of exploiting.*

Key Words: Cyber Security, Security, ICT, Vulnerabilities, Attacks, Solutions

1. INTRODUCTION

In the recent years, experts and other policymakers have expressed increasing showing interest about protecting ICT based systems from vulnerable cyberattacks [4]—which deliberate attempts made by unauthorized persons to access various ICT [2] systems, usually with the goal of theft, disruption, damage, or other unlawful actions. Many researchers expect the number and severity of cyberattacks to increase in the future coming years. This act of protecting ICT based systems and their major contents have known as cybersecurity. It is a broad logical idea that cybersecurity can be a useful term but tends to be a precise definition. It generally refers to the three things below:

•Some set of activities and other measures intended to protect—from attack, disruption, or other threats related to hardware and devices software, the information they contain and communicate, including software [1] and data, as well as other elements of cyberspace.

• Quality [2] of being protected from such threats.

• Implementing and improving those activities which enhance quality.

Cybersecurity is sometimes visualized inappropriately with other concepts such as privacy, information sharing, and surveillance. Privacy is a combined by an ability with individual person to control access by other users. Thus, cybersecurity will protect privacy in an electronic environment, but information which is shared to assist in cybersecurity efforts might sometimes contain personal information that at least some observers would regard as private. It is a means of protection against undesired surveillance and gathering of intelligent information from any system. However, when aimed at potential sources of cyberattacks, such activities can also be useful to help effect cybersecurity.

The risks associated with any attack depend on three major factors: threats - which is attacking, vulnerabilities - the weaknesses they are attacking, and impacts - what the attack does.

1.1 Threats

Those people who perform cyberattacks are widely falling into the following categories: people who intent on monetary gain; people who intent on stealing are classified on proprietary information; regional warriors who develop capabilities to overcome cyberattacks in support of an organizational strategic objectives; people who perform cyberattacks for nonmonetary reasons; people who engage in cyberattacks.

1.2 Vulnerabilities

Cybersecurity is an arms race between attackers and defenders. ICT based systems are very complex in nature, and attackers are constantly probing for weaknesses, which can occur at many points. Others can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by insiders with access to a system; supply chain vulnerabilities, which can permit the insertion of malicious software during the acquisition process. Many vulnerabilities remedies are known, they may not be implemented in many cases because of many constraints.

1.3 Impacts

Many attacks can compromise with the confidentiality, integrity, and availability of an ICT system. Cyber theft can result in exfiltration of financial, proprietary, or personal information from which the attacker can benefit, often without the knowledge of the victim. Denial-of-service attacks can slow or prevent legitimate users from accessing a system. Botnet malware can give an attacker command of a system for use in cyberattacks on other systems. Attacks on industrial control systems can result in the destruction or disruption of the equipment they control, such as generators, pumps, and centrifuges.

Figure-1: Schematic diagram of Federal Agency Cybersurity Roles

2. CYBER CROOKS AND DIGITAL SPIES

The cyber-security [4] and the discourse [5] are very closely related. The development of IT policies in different countries plays a crucial role because it allows the definition and prosecution of its crime. The development of legal tools to prosecute unauthorized entry into computer systems coincided with the first serious network incidents [2]. Cyber-crime has come to refer to any crime that involves computers and networks and many other things.

There has been an increase in many allegations among global countries which are responsible for high-level problem creations among government and other business computer systems across globe. Because many authorities have argued that they consider cybersecurity as a strategic domain by targeted attacks or intelligence gathering operations [5]. However, these allegations rely on circumstantial evidences. It mainly refers to the difficulty in determining initially responsible for a cyber-attack plus identifying their motivating factors in the cyber domain. Due to the architecture of cyberspace, online identities can be optimally hidden.

3. CYBER CROOKS AND DIGITAL SPIES

There are three different discourses which produced specific types of concepts and countermeasures in accordance with their focus and main referent objects, some of which are discussed later. It is most common practice that the entities that own a computer network are also responsible for protecting its policies. However, there are some aspects in cyber security considered very important for the functioning of society to ensure an adequate level of protection. These efforts are usually subsumed under the label of critical information protection.

Table -1: Three discourses of Cyber Security

	Technical	Crime–Espionage	Military/civil defence
Main actors	▪ Computer experts ▪ Anti-virus industry	▪ Law enforcement ▪ Intelligence community	▪ National security experts ▪ Military ▪ Civil defence establishment
Main referent object	▪ Computers ▪ Computer networks	▪ Business networks ▪ Classified information (government networks)	▪ Military networks, networked armed forces ▪ Critical (information) infrastructures

In the earlier period, information became the main problem in the cyber-security. Whereas critical infrastructure protection (CIP) [6] encompasses more than cyber-security. Public–Private Partnerships (PPP) [1] is a form of cooperation between the state and the private sector. The PPP idea is part of all existing initiatives in the field of CIP today, though with varying success. Very large number of them is towards facilitating information exchange between companies and best practices. Mutual win–win situations are to be created by interchanging. The government offers variety of information acquired by its intelligence services.

4. THE LEVEL OF CYBER-RISK

Many political, economic, and military conflicts clearly had cyber policies for many years of time. Furthermore, criminal activities with the help of computers are happening every day. Many cyber incidents are causing minor and major inconveniences [2]. These may be in the form of lost intellectual property, maintenance and repair, lost revenue, and increased security costs. Beyond from direct impact, other cyber-attacks have also damaged corporate reputations, the potential to reduce public confidence in the security of Internet transactions. There are some examples of cyber-attacks which resulted in violence related activities against persons or organizations. The huge majority of cyber-incidents have caused inconveniences or minor losses rather than serious or long term disruptions. There are risks that can be dealt with by individual entities using standard information security measures in comparison to other risk categories like financial risks.

This danger of overly dramatizing the threat supports itself in reactions that call for retaliation or other exceptional measures. There are many different types of countermeasures where most of them are in fact not exceptional. Some computer attacks whose effects are sufficiently destructive need the attention of the traditional national security updates. Attacks that disrupt nonessential services or that are mainly a costly nuisance.

5. CONCLUSION

Cyber-security issues are challenging for students and in academics perspective. Researchers widely disagree about the future cyber scenarios are. While there are some proof and experiences of cyber-crime, or other lesser forms of cyber-incidents on a daily basis, cyber-incidents of bigger proportions exist solely in the form of stories or news. It influences our judgement and there are an infinite number of ways in how we could percept them. Therefore, there are some ways to study the 'actual' level of cyber-risk in some way because it only exists in and through the representations of various actors in global domain.

REFERENCES

[1] Richard Stiennon, Chief Research Analyst, IT-Harvest, National Fintech Cybersecurity Summit 2016

[2] Internet Users by Country 2016, Internet Life Stats, July 2016 www.internetlivestats.com/internet-users-by-country M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[3] Biggest cybersecurity threats in 2016', CNBC, Dec 2015

[4] 'Hackers remotely kill a jeep on the highway', Wired, July 2015

[5] 'Hackers can send fatal dose to hospital drug pumps', Wired, June 2015

[6] 'Hackers can hijack Wi-Fi Hello Barbie to spy on your children', The Guardian, November 2015

[7] Simi Bajaj, 'Cyber Fraud: A Digital Crime', www.academia.edu/8353884/cyber_fraud_a_digital_crime

[8] 10 Akamai's State of the Internet Security Report Q2 2015

[9] 11 Contracting for the Internet of Things: Looking into the Nest, Social Science Research Network, February 2016

[10] 12 'Cisco CEO Pegs Internet of Things as $19 Trillion Market', Bloomberg Technology, January 2014.