International Context of Cybercrime and Cyber Law

Tansif Ur Rehman
University of Karachi, Pakistan

INTRODUCTION

It is clearly evident that as people become more dependent on technology, they become easier targets of cybercrime, as it also could evolve to bring about new problems. It is also important to realize to what extent it is understood by common people that either they are really a victim or can be the victim of a cybercrime.

This research includes significance as well as international aspects of cyber laws, initiatives by the EU, USA, China, and the role of international forum for cybercrime. At the very least, it demonstrates the fact that cybercrime attacks are an almost routine form of criminality and most internet users are likely to face an attack on a daily basis.

OBJECTIVES

1. To highlight the significance of cyber laws.
2. To highlight the international aspects of cyber laws.
3. To discuss the initiatives taken by the EU, USA, and China regarding cybercrime.
4. To discuss the role of international forum for cybercrime.

BACKGROUND

Cybercrime has so advanced that it was reported in August 2018 during the Black Hat and Def Con Hacking Conference that, it was possible to even hack patients' vital signs, pacemaker, and insulin pumps in real time (Smith, 2018). Symantec, one of the leading software firms that operates antivirus and firewall packages, stated in their 'Internet Security Threat Report 2011' (published in 2012) that there had been an 81% increase in malicious attacks that they had identified, with an estimate of attacks being placed over 5.5 billion.

A Barkly sponsored survey of 660 IT companies and professionals by Ponemon Institute, USA (2018) 'State of Endpoint Security Risk' has revealed that 64% of organizations experienced successful endpoint attacks. This survey has also revealed zero-day and fileless attacks that cost millions to organizations, i.e. costs doubling for Small and Medium-sized Businesses (SMBs).

Cybercrime's pace globally is on a high rise. It is an offense that is even harder to identify and resolve as compared to traditional crimes in the international context. Cybercrime cells all around the world receives thousands of complaints on a daily basis.

DOI: 10.4018/978-1-5225-9715-5.ch028

Cyber criminals are honing their skills, while consumers remain unconcerned. Cyber criminals are innovative, organized, and far sophisticated (Hutchings, 2013). They employ their tools effectively, working harder, and focused to uncover new vulnerabilities as well as escape detection. The ICTs are opening a whole new world of opportunities for criminals and the risk remains largely unknown.

The protection against cybercrime largely depends upon the security culture adaptation by government authorities of every networked country, business organizations, and most importantly, every internet user. Prevention will always be the first and best line of defense along with radical changes in policing and legislation (Glenny, 2012). Education and awareness across the citizens will go a long way to prevent individuals against many types of cybercrime and will reduce pertinent risks (Lusthaus, 2012).

FOCUS OF THE ARTICLE

This article focuses on the significance, international aspects of cyber laws, initiatives by the EU, USA and China, and the role of the international forum for cybercrime. This research will also help to understand the computer-related crime advancement, and how to use it as defined within the premises of law in an international context.

CHARACTERISTICS OF CYBERCRIME

1. Scale
2. Accessibility
3. Anonymity
4. Portability or Transferability
5. Global reach

VARIETIES AND SKILLS OF CYBERCRIME

1. Hacking of Computers
2. Denial of Service Attacks (DoS)
3. Distributed Denial of Services Attacks (DDoS)
4. Malware
5. Spyware
6. Offense Relating to Data
7. Destroying, Disclosing, and Accessing Data
8. Misconduct in a Public Office
9. Phishing
10. Pharming
11. Hate and Harm