Editorial

Cyber security and cyber forensic

Reeta R Gupta [1]*

[1]*Dept. of Forensic Science, CFSL DFSS MHA, New Delhi, India*

A R T I C L E   I N F O

Tremendous change in the technological development in the digital world and it enforce to all human being to live with it without their own choice as well as also to develop skill with full awareness for understanding and identifying the coming situation of cyber threat in terms of their own safety and protect themselves from financial losses. Today's digital world is gradually growing fast, where data breaches and cybercrime are increasingly frequent and effect people at large. Because of this increases in digital word more cyber security systems and case analysis work of cyber forensics in laboratory also increased.

Cyber forensics and cyber security may in general appear similar, but both are unique in their work scope area. Cyber forensics, or digital forensics, involves collecting, preserving, and analysing digital evidence in cases of cybercrime. The main purpose of cyber forensics is to recover, investigate, and analyse digital traces to reconstruct cyber incidents and aid in legal proceedings. Digital forensic help to retrieve information from computer system and other digital storage devices. This retrieved data can then be used in criminal investigation in cases of various types such as threats include malware, phishing, ransomware, and Distributed Denial of Service (DDoS) attacks of Artificial Intelligence.

Cyber security is more prominent as it plays a critical role in providing proof of evidence before court of law, supporting Law enforcement agencies in analysing criminal exhibits. Cyber security includes various tools and strategies like firewalls, encryption, multi-factor authentication, and employee training. Cyber security can be understood by identifying attack methods, vulnerabilities, and responsible persons. The major objective of cyber security is to provide safeguard confidentiality, integrity, and availability of data. It is used in investigations of fraud, hacking, data theft, and unauthorized access. Process of examination involves, several phases, including identification, collection, examination, analysis, and reporting.Specialized software like EnCase, FTK, and Autopsy help gather and interpret digital evidence accurately.

Wherein in current scenario, AI has significant role to boost economic growth and market productivity, but at the same time it equally piles up the serious risk of already existing unemployment, reducing jobs thus creating economic inequality and emergence of new undesirable development of security issues as well as its unethical use. As new role of artificial intelligence (AI) emerges, the impact AI going to have on each and every citizen and public at large on global. The facial identification as well as voice of any person can easily replicate with artificial intelligence. Henceforth it enforced to all human being to think about their personal safety and security.

Now, it is important for every citizen to ensure themselves by creating an atmosphere to aware and encourage themselves for the use of technology with developing the right analytical talent to understand technological innovation prior to use and maintain the cyber

* *Corresponding author.*
  E-mail address: reetacbi@gmail.com (R. R. Gupta).

security of the own. All these efforts help as a deterrent for safe society, protect economic loss and promoting accountability.

Conflict of Interest

None.

Author's biography

Reeta R Gupta, Assistant Director https://orcid.org/0000-0001-8546-9841