The growing menace of Cyber Crimes: An approach to tackle it

Aniket Kumar Gupta
akgupta98@gmail.com
Singapore International School, Mumbai, Maharashtra

Dr A. Prabaharan
nmc.dean@gmail.com
Nehru Memorial College, Puthanampatti, Tamil Nadu

ABSTRACT

The world witnesses disruption of normal computer functions very often. These disruptions range from personal to business companies to government networks. In this research paper, an attempt has been made to discuss the problems arising out of various forms of cybercrimes, their definition, present laws about cybercrimes and the methodology adopted by cyber criminals. This paper shall also analyze growing use of technology in identity theft, hacking and its use by terrorist organizations. Statistical data is presented to explain how cybercrimes have increased over time and their cost implications. The purpose of this study is also to make the reader aware as to where we stand today in our fight against cyber criminals, what are the future trends and the commitment of various countries of the world for cyber security. Since it is being widely accepted that physical devices and human intervention have not proved to be sufficient for protecting cyber infrastructure, there is a need for more sophisticated cyber defense system which is also robust and flexible. Computing methods using Artificial Intelligence tools have begun to play an important role in cyber crime detection and prevention and their application can be further extended to assist human intelligence in the fight against cybercrimes. This study shall evaluate the progress made till now in the fight against cybercrimes and discuss which Artificial Intelligence tools can be made use of in the fight against this menace.

Keywords: Cybercrime, IT laws, Artificial intelligence, Cost of cybercrimes, Cybercrimes in countries, Cyberlaw, Artificial intelligence.

1. INTRODUCTION

In this interconnected world, keeping one’s personal information private has become a challenge. Due to the ease provided by technology in doing business and transactions, government policies regarding identification of each citizen and social interactions through mobiles and computers, people are sharing personal data which can be sifted by those for whom it is not intended. The data thus stolen has become a commodity with a price tag. This provides a negative connotation to the use of technology and makes people fearful of cybercrimes.

Internet being the strongest and widespread medium of cyber crime, common user is unaware of the magnitude of the problem. In fact, till someone is directly affected by an attack from a cyber criminal, the realization of the danger inherent in the use of computer technology is generally not appreciated. Cybercrimes bring to the surface the issues surrounding privacy and confidentiality. When there is a dent in privacy and confidentiality, different forms of cybercrimes like hacking, financial theft, identity theft, spamming and copyright infringement take place.

The methodology adopted by cyber criminals has also changed over time. Earlier, one used to hear about worms, viruses unleashed to grow inside the computers and networks, but these days one hears about ‘phishing’ which is a similar fake website in appearance which is hosted and managed by high-class cyber criminals. To a layman, the website shall appear to be from an authentic source. An email purporting to be genuine shall be sent by a criminal mastermind who shall guide the reader towards furnishing personal information or through ‘links’ it shall open another website requiring confidential data of the reader.

The law enforcement machinery of the state is not adequately equipped to handle the high technological nature of the cybercrimes. There is a dearth of high trained and skilled professionals in police and other law enforcement agencies of the state. There are cyber cells in countries like India also but the skills and competence of cyber criminal are beyond their reach. The cyber criminal can be located in any part of the world and taking advantage of the interconnectedness of computer data through internet cause havoc.
Hence not only the countries have to modernize their legislation but also at the world level a concerted action is more required than ever.

This paper shall make an analytical attempt to educate people about various cybercrimes, how they happen, and how they are important as technology progresses. Since technology has almost taken over the normal lives of people, understanding the implication of cybercrimes is of paramount importance. This study not only aims at increasing the awareness of the people about the methods adopted by cyber criminals, the laws providing protection to citizens and the commitment of various countries to cyber security. Not only this study attempts to make readers aware of the problem, it also suggests a future course of action to combat the threat of cyber crime in the world.

2. DEFINITION OF THE PROBLEM OF CYBER CRIME

The term cybercrime does not give a clear picture to everyone about the specific nature of the crime. Few people think it simply relates to the crime committed on the internet. Can hacking be done by a mastermind in the intra-net without the use of internet stealing the data of the company? The methodology adopted by the cyber criminal defines the medium used for committing fraud. There are various definitions of cybercrimes,

Techopedia<sup>1</sup> defines “Cybercrime as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.”

Wikipedia<sup>2</sup> says, “Cybercrime is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes can be defined as ‘offences that are committed against individuals or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as internet and mobile phones (Bluetooth/SMS/MMS).’”

Encyclopedia Britannica<sup>3</sup> refers it to “the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.”

The definitions of cybercrimes may vary but use or abuse of computer power and criminal intent is common to all.

3. LAWS RELATING TO CYBER CRIMES

This section has been further subdivided into existing major laws against cyber crimes in US, UK, and India. As the purpose is to make people aware of the existing laws for their protection, only the salient points of different acts in the US, UK and India have been mentioned due to the limit of the scope of this paper.

US- The first federal computer crime statute was the **Computer Fraud and Abuse Act of 1986 (CFAA)**. This act has been modified on many occasions to address the difficulties in its implementation. CFAA is also known as Title 18 U.S.C Section 1030. ‘In its current incarnation CFAA criminalizes seven types of computer activities: (1) the unauthorized access of a computer to obtain national security information with an intent to harm the United States or for the benefit of a foreign nation; (2) the unauthorized access of a computer to obtain protected financial or credit information; (3) the unauthorized access of a computer used by the federal government; (4) unauthorized access to a protected computer with the intent to defraud; (5) intentionally damaging a protected computer; (6) the fraudulent trafficking in computer passwords and any other information which can be used to gain access to a protected computer; and (7) threatening a protected computer with the intent of extorting money or something else of value. The term “protected computer” is defined in the CFAA as either a computer in use by a financial institution or the United States Government or a computer used in interstate or foreign commerce or communication.’

The second important act, “the **WireTap Act**, also known as the **‘Title III’**, involves the use of wiretaps while investigating the crime. This act prohibits ‘any person’ including a law enforcement officer, from making an illegal interception or disclosing or using the illegally intercepted material.

The third is a catchall of all what is known as other **Network Crime Statutes**. These statutes all have their own penalties and fines depending upon the circumstances under which the offense is committed.

- Unlawful Access to Stored Communications: 18 U.S.C. Sec. 2701
- Identity Theft: 18 U.S.C. Sec. 1028
- Aggravated Identity Theft: 18 U.S.C. Sec. 1028A
- Access Device Fraud: 18 U.S.C. Sec. 1029
- CAN-SPAM Act: 18 U.S.C. Sec. 1037
- Wire Fraud: 18 U.S.C. Sec. 1343”

There are state laws also aimed to increase cyber security.
UK- Computer Misuse Act, 1990. It is aimed at unauthorized access to computer material, unauthorized access with intent to commit or facilitate the commission of further offenses, unauthorized modification of computer material. This act was amended to include Police and Justice Act 2006 and Serious Crime Act 2015. This amendment aimed at unauthorized acts causing, or creating a risk of, serious damage and making, supplying or obtaining articles for use in the offense under section 1, 3 or 3ZA of the Act.

In the UK there happen to be a significant number of acts, directives, and regulations to consider when it comes to malicious computer hacking and offensive security. The EU Directive 2013/40/EU and Terrorism Act 2000 are also related acts.

INDIA- The primary law dealing with cyber crime in India is the Information Technology Act 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate the filing of electronic records with the Government. The offenses covered are-

- Tampering with computer source documents
- Hacking with Computer systems
- Receiving stolen computer or communication device
- Using a password of another person
- Cheating using the computer resource
- Publishing private images of others
- Acts of cyber terrorism
- Publishing information which is obscene in electronic form
- Publishing images containing sexual acts
- Publishing child porn or predating children online
- Failure to maintain records
- Failure/refusal to decrypt data
- Securing access or attempting to secure access to a protected system
- Misrepresentation

Another section 66 A was added in 2008 to make publishing offensive, false or threatening information punishable.

4. COMMON CLASSIFICATION OF CYBERCRIMES, AND HOW THEY ARE COMMITTED BY CYBER CRIMINALS

Cyber crimes can be classified into different categories.

A. Cyber Crimes against Persons.

There are offenses which affect the personality of an individual and can be defined as

- Harassment through emails and social networking sites: This is a very common type of harassment through sending letters, attachment of files and folders. Using abusive language on Face book and Twitter etc.
- Cyber stalking: It means a threat-expressed or implied-to create fear through the use of computers, internet, text messages, websites or videos
- Dissemination of obscene material: It includes Indecent exposure/Pornography (basically child pornography), hosting of the web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
- Defamation: It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to the unknown person mail account.
- Hacking: It means unauthorized control/access over computer system and the act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hack telecommunication and mobile network.
- Cracking: It is amongst the gravest cyber crimes known to date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it’s origin to be different from which actually it originates.
- SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here an offender steals the identity of another in the form of the mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is a very serious cyber crime against any individual.
- Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim’s bank account fraudulently. There is always unauthorized use of ATM cards in this type of cyber crimes.
- Cheating & Fraud: It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having a guilty mind which leads to fraud and cheating.
k. **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

l. **Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

### B. Crimes Against Persons Property:

There are certain offenses which affect person’s properties which are as follows:

- **Intellectual Property Crimes:** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offense. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
  
  a. **Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first or by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.
  
  b. **Cyber Vandalism:** Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
  
  c. **Hacking Computer System:** Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity, there will be a loss of data as well as a computer. Also, research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.
  
  d. **Transmitting Virus:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks play a major role in affecting the computerized system of the individuals.
  
  e. **Cyber Tresspass:** It means to access someone’s computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.
  
  f. **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else’s ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person’s knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

### C. Cybercrimes against Government

There are certain offenses done by a group of persons intending to threaten the international governments by using internet facilities. It includes:

- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by a distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
  
  a. **Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
  
  b. **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
  
  c. **Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of the internet and to possess that information for political, religious, social, ideological objectives.

### D. Cybercrimes Against Society at large

An unlawful act done with the intention of causing harm to the cyberspace will affect a large number of persons. These offenses include:

- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
  
- **Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects a large number of persons. Trafficking in the cyberspace is also the gravest crime.
  
- **Online Gambling:** Online fraud and cheating are one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.
  
- **Financial Crimes:** This type of offense is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through the internet. Ex: Using credit cards by obtaining password illegally.
  
- **Forgery:** It means to deceive a large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today’s life style.
Few methods used by cyber criminals and which are on the rise are:

**Phishing:** bogus emails that may look like they come from a trusted source asking for security information and personal details.

**File hijacker:** where criminals hijack files and hold them to ransom also known as ‘Ransomware’.

**Key logging:** where criminals record what you type on your keyboard and steal passwords and **Screenshot manager:** allows criminals to take screenshots of your computer screen.

**Ad clicker:** criminals will create online adverts that direct a victim’s computer to click a specific link.

According to Indian Computer Emergency Response Team (CERT-In), as reported in the Times of India, a prestigious newspaper of India on 22 Jul 2017 the cybercrimes registered increased from 44679 in the year 2014 to 49455 in 2015 and in 2016 it went up to 50362. The newspaper further reported that ‘one cyber crime was committed every ten minutes in the first six months of 2017, higher than 2016 when there was one in every twelve minutes.’ Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion annually by 2021.

According to an assessment, the top five cyber security concerns for 2018 are

I. “The crypto jacking “gold rush” will be the top priority for cybercriminals

**Cryptojacking** activity began exploding toward the end of 2017 and we suspect that we will see far more activity in 2018, particularly as the value of crypto currencies. What makes this kind of activity interesting is how it has created a blurry line between the everyday Internet user and the cybercriminal. An individual mining crypto currency could very well be mining for their own wallet, based on visitors to their own web properties. There is also a very likely chance within those circumstances that disclosed crypto jacking activity could replace advertising on sites to become an entirely new revenue stream. However, the largest portion of crypto jacking is likely to occur from legitimate websites compromised to mine currency for the criminal wallet. Regardless, crypto jacking will be one of the cybercrime activities to watch in 2018.

II. We will see an increase in PowerShell-based attacks

Earlier this year, entities of the Saudi Arabian government were compromised using a macro in Microsoft Word to infect the target’s computer with an information-stealing Trojan. Rather than retrieving a binary payload, the attack relied on malicious scripts to maintain persistence on the device and to communicate with compromised websites acting as proxies for the command and control server. These malicious script-based attacks, specifically PowerShell-based attacks, are incredibly difficult to identify. They can easily evade antivirus engines, making it that much more appealing to cybercriminals. Many more **PowerShell** attacks in the year to come are predicted.

III. The cybercriminal underground will continue to evolve and grow

While it may seem like we are already overwhelmed by the number of cyber-attacks occurring daily, this will not slow down in 2018. In fact, with a recent increase in cyber criminal tools and a lower threshold of knowledge required to carry out attacks, the pool of cybercriminals will only increase. This growth is a likely response to news media and pop culture publicizing the profitability and success that cybercrime has become. **Ransomware** alone was a $1 billion industry last year. Joining the world of cybercrime is no longer taboo, as the stigma of these activities diminishes in parts of the world. To many, it’s simply a “good” business decision. At the same time, those already established as “top-players” in cybercrime will increase their aggressive defense of their criminal territories, areas of operations and revenue streams. We may actually begin to see multinational cybercrime businesses undertake merger and acquisition strategies and real-world violence to further secure and grow their revenue pipeline.

IV. Security software will have a target on its back

In 2018, cybercriminals will target and exploit more security software. By targeting trusted programs and the software and hardware supply chain, attackers can control devices and wholeheartedly manipulate users. Hackers will leverage and exploit security products, either directly subverting the agent on the endpoint, or intercepting and redirecting cloud traffic to achieve their means. As these events become more publicly known, the public and business perception of security software, particularly that of antivirus solutions, will further deteriorate.

V. More cyber criminals will use worms to launch malware

In 2017, we saw **WannaCry** and **Trickbot** use worm functionality to spread malware. More malware families will use this technique in 2018 because network compromise from worms spread faster than many other methods. If hackers can figure out how to use worms without being too noisy (a traditional downfall of this approach), this tactic can amass a large number of victims very quickly.

VI. Cybercrime statistics: the big picture

- Cybercrime was the 2nd most reported crime in 2016.
- In proportion to the total number of crimes, cybercrime now accounts for more than 50% of all crimes in the UK.
- An attacker resides within a network for an average 146 days before detection.
- Most network intrusions—63 percent—are the result of compromised user passwords and usernames.
- 18 million new malware samples were captured in Q3 2016.
- In their 2017 Annual Cyber security Report, Cisco found that globally, 8 percent of malicious email attachments were docm files (a type of Microsoft Word XML file that executes macros).
At 91.6 percent, “Theft of Data” continues to be the chief cause of data breaches in 2016 counting total by identities stolen. “Phishing, Spoofing, and Social Engineering” were a distant second at 6.4 percent.15 Mobile platforms are one of the fastest-growing targets for cyber criminals. Symantec identified 18.4 million malware detections in 2016, a 105 percent increase of 2015.16 The number of ransomware families increased from 30 in 2015 to 98 in 2016, revealing the distinct focus by cyber criminals on using ransomware to extort money from businesses and individuals.17 The average ransomware demand also increased significantly, from $294 in 2015 to $1,077 in 2016.18 In 2016, adware affected around 75 percent of organizations in 13 countries.19 43 percent of cyber attacks against businesses worldwide target small companies.20

VII. Cybercrime statistics directly affecting consumers

• During a 6-month period, more than 1.8 million cyber attacks were conducted through home network routers in several countries, including the U.S., Canada, the U.K. and China, often for the purpose of Bitcoin mining.21 76 percent of consumers in 21 countries acknowledge the importance of keeping their account information secure, yet many still share their passwords, among other risky behaviors with their data. A further 35 percent allow at least one device to go unprotected and vulnerable to all forms of viruses and malware.22 Most smart home attacks occur in the U.S., China, and the U.K.23 2015-2016 saw identity takeover become the fastest-growing type of fraud in Australia and New Zealand, with up to 80% of reported cases of fraud falling into this category.24 41 percent of people globally cannot properly identify a phishing email and often guess as to an email’s legitimacy.25 30 percent of phishing emails in the U.S. are opened, with 12 percent of those targeted by these emails clicking on the infected links or attachments.26 53 percent of Millennials in the UAE experienced at least one incident of cybercrime in 2015. A further 2.53 million consumers in the country fell victim to online criminals.27

VIII. THE COST OF CYBERCRIME

• The global cost of Cyber Crime is estimated to reach $2 trillion by 2019, a threefold increase from the 2015 estimate of $500 billion.28
  • $14 billion: The amount the U.S. government spent in 2017 on cybersecurity. The government intends to spend 19 million in 2017.29
  • $2.1 trillion: The total global annual cost of all data breaches by 2019, as suggested by Juniper Research.30
  • $158 billion: The collective amount of money consumers lost globally in 2015 due to cybercrime. The U.S. accounts for $30 billion of that loss.31
  • $16 billion: The Javelin Strategy & Research 2017 Fraud Report discovered that 15.4 million U.S. consumers (17.5 percent increase) lost $16 billion to identity fraud in 2016. This marked a rise from 2015 when 13.1 million victims lost $15.3 billion.32
  • $50 million: The total cost of cybercrime across 237 major companies in 6 countries.33
  • $530 million: The cost of the January 2018 Coincheck hack, the biggest cryptocurrency heist to date.34

IX. Cyber Security commitment of various Countries.

The commitment of countries for cyber security is measured by International Telecommunications Union, a specialized agency of the United Nations. A survey was conducted in 2016 and covers 193 countries. Global Cybersecurity Index 2017 has measured the commitment of member states towards cybersecurity in order to raise awareness. The overall picture shows improvement and strengthening of all five elements of the cybersecurity agenda in various countries in all regions. However, there is space for further improvement in cooperation at all levels, capacity building, and organizational measures. As well, the gap in the level of cybersecurity engagement between different regions is still present and visible.

The Heat Map of National Cybersecurity Commitments with dark green being the most committed and red the least (Source ITU)
With mobile changing the way organizations interact with consumers, the number of fraud attempts through mobile channels is dramatically increasing. The types of cybercrime taking place are evolving, as is the way cybercriminals communicate.

A look at the chart below would show that the percentage of transactions originating from a mobile device is increasing and so are the frauds.

A representation of the cybercrime trends seen in the mobile channel. (Source: RSA)³⁷

INDIA- The State of IT Security


In the global EY survey listed above, out of the 1,735 CXO respondents, 124 were from India. This report breaks out data from these participants to create a view of cybercrime as it relates to Indian businesses.

Key findings:

- As a result of the occurrence of large cyberattacks, companies are investing more in their corporate shield
- Organizations are also focusing more on their abilities to see threats coming
• Most companies continue to lag behind in preparation to react to a breach and appear to ignore the fact that they more than likely will be or already have been attacked

In 2015, professional services firm KPMG conducted this survey that focused solely on cybercrime in India. It examines industry perception, which area of organizations is affected by cybercrime, and what measures companies are taking. There were 250 participants included CIOs, CISOs, and CAEs, among other executives from a range of industries.

Key findings:

• Almost all respondents view cybercrime as a major business threat but fewer than half see it as part of the boardroom agenda
• A large majority of CXOs believe the Banking, Financial Services, and Insurance (BFSI) sector is a top target for cybercrime and the majority believe directors and management are most vulnerable
• Most organizations lack cyber risk management strategies, such as risk assessments and incident response plans
• A large majority of companies have experienced a cyber-attack in the past year and most believe there was external involvement

X. HOW CAN WE COMBAT CYBER CRIMES?

Many methods for securing data over networks and Internet have been used like anti-virus software, firewall, and encryption; however cyber criminals find new ways to attack network systems.

Since cyber intrusions are not localized, legislation alone in a country cannot completely check the growing menace of cybercrimes. What is required is an innovative approach instead of applying conventionally fixed algorithms which seem to be ineffective against dynamically evolving nature of cyber-attacks. We have to try and harness methods of Artificial Intelligence that may provide the flexibility and learning capability to software to assist humans in fighting cybercrimes. One keeps hearing about Computational Intelligence36, Artificial Neural Networks37, Data Mining and Pattern Recognition38 which are already playing an important role in cyber crime detection and prevention.

A system called AI² developed at MIT’s Computer Science and Artificial Intelligence Laboratory, reviews data from tens of millions of log lines each day and pinpoints anything suspicious. A human takes it from there, checking for signs of a breach. The one-two punch identifies 86 percent of attacks while sparing analysts the tedium of chasing bogus leads. According to the research paper, AI² invokes the intersection of analyst intuition and an artificially intelligent system. The system highlights any typical signifiers of an attack. An extreme uptick in log-in attempts on an e-commerce site, for instance, might mean someone attempted a brute-force password attack. A sudden spike in devices connected to a single IP address suggests credential theft. “The human analyst provides feedback as to what was and wasn’t a legitimate threat, and the system uses that information to fine-tune it’s monitoring the next day.”40

Cyber security needs much more attention. Given human limitation and the fact that computer viruses and worms are intelligent, what seems very important is the presence of cyber sensors (computer generated forces) which will detect, evaluate and deal with cyber attacks in a timely fashion. Future research and careful planning in every country and their centers of computer learning is the need of the hour. It seems foreseeable that the artificial intelligence shall provide superior to human intelligence to counter the intelligence of cyber criminals. It is an advancing field with a lot of expectation.

5. ACKNOWLEDGEMENT

This research article has been written under the guidance of Dr. A. Prabaharan Ph.D., Dean of Nehru Memorial College, Puthampatti, Trichy, Tamil Nadu, India- Pin 621 007, An Autonomous institution with NAAC “A” Grade.

6. REFERENCES

[1] https://www.techopedia.com/definition/2387/cybercrime
[7] Cybersecurity Ventures is the world’s leading researcher and publisher covering the global cyber economy.
[8] SECURITY BYTES, Justin Dolly is EVP, Chief Security Officer and CIO of Malwarebytes.
Aniket Kumar Gupta is a student of Grade 11 (IBDP) at Singapore International School, Mumbai. He is passionate about computer technology and at an early age had devised a technological platform (Eshikayat) for grievance redress which is currently used by people in the villages of the state of Uttar Pradesh, India. Having learnt Programming for Mobile Apps at Stanford University in 2017, Aniket is learning Data Science with Python and scheduled to attend course at Harvard University, US in 2018. He created the School Mobile App for Singapore International School, and is used by faculty and students.