A review and analysis of online crime in pre and post COVID scenario with respective counter measures and security strategies

Naresh KSHETRI[1] | Ajay SHARMA[2]

[1]Research Scholar, Dept. of Computer Science, University of Missouri-St. Louis, St. Louis, USA, nkbgy@umsystem.edu

[2]Research Scholar, Dept. of Computer Science, KNIT, Sultanpur, Uttar Pradesh, INDIA, uptecajay@gmail.com

[1]Corresponding author: Naresh Kshetri (email: nkbgy@umsystem.edu)

Abstract *The well-known pandemic, COVID-19 or coronavirus has affected the lives of every person in the world either directly or indirectly. As the cases of COVID-19 seem to increase day by day, so do the online crimes and attacks (as many sectors and organizations went 100% online now). Our study and research presented here focuses on the pre and post scenario of COVID-19 in terms of online crimes, security and online frauds, attacks. We have also outlined the background study and respective counter measures (with various ways to safeguard online works, online transactions, and online threats) for the increasing online crimes in the post-COVID era. We came up with the conclusion that, to slow down or end the ongoing online crime, cyber power nations should help under-developed and under-developing nations in combating cybercrimes, and to develop countermeasures. These under developing nations (mainly in Asia and Africa) are the major source and home of cyber-attacks and continuous threats to the entire world. We have also proposed a security model and major insights with major types of cybercrimes based on the four nations crime data, counter measures, increasing online crimes, attacks of the post COVID scenario.*

KEYWORDS: coronavirus, counter measures, online crime, security, cyber-attacks, frauds, post COVID era

I. INTRODUCTION

Online crime (also known as Cyber-enabled crimes or Internet crimes) is any sort of crime or online activity (that is illegal) performed using the internet. As we all know, internet crime is one of the major branches of cybercrime that includes (but not limited to) URL redirection, cyberstalking, scams online, credential phishing (asking for username and password) and identity theft. There are also online crimes in the form of "business schemes and various offers" to the customers by their respective organizations. The COVID-19 pandemic has resulted in a 600% increase in cybercrime worldwide [1] that includes "social engineering" as one of bold-bases of cyber-attacks. The extensive use of social media, online working from home (say WFH, work from home), less visit to public places, growing number of electronic internet-

connected devices etc. is increasingly leading to identity theft, online crime, which is also a source of cyber-attacks.

Cyber-attacks and online crime today vary from several dimensions (either individual, groups or in the scenario of a nation state). Every individual and nations are gathering data, analysing, processing, and refining those data to decide future goals and targets. The rise in online crime is also due to the rise in online involvement of several parties in the cyber space and due to this current pandemic situation. Everyone in the online space is worried about their own security, nation, systems, and people but lacks the initial ethics to be enforced before involving in the defence and destruction of networks / systems of the opponent party [2]. The code of ethics should be enforced (included) in every stage and phase

before taking a conclusion to attack others in the name of protecting one's own, which can be also a major point in combating online crime in cyberspace. People are spending more and more time at home, computers, and less time in public. The pandemic may affect victimization differently depending on the crime type as street crimes seem to decrease while domestic crimes may be increasing. As a result, work from home, e-learning, online shopping has increased and several companies are facing cyber-attacks in an increased manner. The number of consumers who were victims of identity fraud seems to increase more than 3 million every year and cybersecurity attacks have become a serious problem [3] [4] [5]. We can easily predict the disturbed lifestyle of an individual and the increasing cyber-attacks because of pandemic. The rates of online attacks, cybercrimes are still unreported in many developed countries as the victim / user are not fully aware about such scams, and fraud. Cyber criminals are now focusing on different financial accounts, such as loyalty and rewards programs and retirement accounts. Within identity theft, almost one-third were for scams involving government benefits applied for or received.

Our study is structured as follows. In *Section II*, we present a brief overview of background study, past works and try to identify the rise of online activities due to the current pandemic. Although online crime and online attacks seem to rise in non-COVID era too, we have focused on the COVID outbreak times. We then discuss in *Section III*, about the online crimes and online attacks (including losses reported of the last five years) for the four nations - USA, Canada, Australia, and India followed by the countermeasures and security strategies (based on online crimes and attacks) in *Section IV*. We have proposed the security model to secure online data and information in *Section V* with possible limitations and solutions of our study in *Section VI*. In *Section VII*, we point out the conclusions of our study and findings along with the possible future scope in *Section VIII*.

II. BACKGROUND STUDY

In [6], **C. Tran** (2020), summarized some common knowledge about phishing and cybercrime, and then gave some recommendations for ordinary users to avoid getting phished and cybercrime risks. As the COVID-19 is quickly spreading across the world (globally to all countries), so do the cybercrime levels. The outbreak has a huge impact on the global economy and other aspects of our life (besides our health and creating global crises). The unwilling stay

at home order was passed, which makes the economy extremely go down, countless people lose their jobs due to mass layoffs. The author provided some common cybersecurity concerns related to domain spoofing attacks when working from home. The author also presents several recommendations to ordinary internet users on how to mitigate phishing and cybercrime risks. During this crisis, not only big companies but also the small organizations all rely more than ever on computer systems, mobile devices, and internet to work, communicate, make payments, and exchange information as a method of practicing social distancing.

In [7], **MK Kagita et. al.** (2020), reviewed the online crimes on the Internet of Things and found the reasons for cyber-attacks as (i.) Countries having weak cyber securities (ii.) Cybercriminals use new technologies to attack and (iii.) Cybercrime is possible with services and other business schemes. Cyber-attacks have become a part of IoT and affect the society of users in innumerable ways. The authors have also identified the types of cyber-attacks on IoT devices, smart homes and its subsystems. Several challenges (such as testing drawbacks, default passwords, IoT ransomware etc.) for the current approaches, along with recommendations for cyber hygiene of IoT devices are outlined in the review by the authors.

IoT makes the world so small. Every human being relates to each other by using the internet. Lots of transactions are done over IoT and chances of crimes have increased as cybercrimes are not bound to a particular location or country.

In [8], **James Hawdon et. al.** (2020), investigated how the pandemic has affected rates of cyber victimization, while treating the pandemic as a natural experiment. The authors compare pre-pandemic rates of victimization with post-pandemic rates of victimization using datasets designed to track cybercrime. COVID-19 will influence victimization rates as people alter their routines and spend more time at home and less time in public. Yet, the pandemic may affect victimization differently depending on the type of crime as street crimes appear to be decreasing while domestic crimes (with online crimes) may be increasing. After considering how the pandemic may alter routines and affect cyber victimization, we find that the pandemic has not radically altered cyber routines nor changed cyber victimization rates. However, a model using routine activity theory to predict cyber victimization offers clear support for the theory's efficacy both before and after the pandemic.

In [9], **H. L. Lallie et. al.** (2020), analysed the COVID-19 pandemic from a cybercrime perspective and highlights the range of cyber-attacks experienced globally during the pandemic. Cyber-attacks are analysed and considered within the context of key global events to reveal the modus-operandi of cyber-attack campaigns. The analysis shows how following what appeared to be large gaps between the initial outbreak of the pandemic in China and the first COVID-19 related cyber-attack, attacks steadily became much more prevalent to the point that on some days, 3 or 4 unique cyber-attacks were being reported. The analysis proceeds to utilise the UK as a case study to demonstrate how cyber criminals leverage key events and governmental announcements to carefully craft and design cybercrime campaigns. The authors presented the timeline of COVID-19 related cyber-attacks and its impact on the workforce across eight different categories (information governance to lifestyle).

In [10], **K. Kumar and B.P. Pande** (2021), discussed the rise of online teaching and learning processes during the COVID-19 pandemic. This widely transmittable disease has affected all the spheres of our lives such as economy, business, manufacturing, health sector, education, and livelihood. The pandemic has deeply affected the educational systems all around the globe,

and they have been derailed from their normal operations. The outbreak of the pandemic caused schools, colleges, and universities to remain closed for an indefinite period. The authors have also presented the features of online teaching and learning processes along with a comparative analysis of digital tools available to aid online teaching and learning processes (with brief survey reports and conclusion as to the substantial growth of online teaching and learning methods).

In [11], **M. Hijji and G. Alam** (2021), studied a systematically directed Multivocal Literature Review (MLR) related to the recent upsurge in social-engineering (SE) based cyber-attacks / threats since the emergence of COVID-19 pandemic. The authors discovered that the major SE based techniques used (during COVID-19 pandemic) are phishing, scamming, spamming, smishing and vishing (in combination with socio-technical methods - fake emails, websites and mobile apps used as weapon platforms for conducting successful cyber-attacks). Three types of malicious software frequently used (for system and resource exploitation) are: ransomware, trojans and bots. The authors also emphasized the impact of cyber-attacks performed on different organizations and critical infrastructure (in which hospitals / healthcare were on top targeted during the pandemic). The authors lastly identified the open challenges, general recommendations, and prospective solutions for future work by using the latest technology (such as AI, Blockchain, and big data analytics).

In [12], **S. Monteith et. al.** (2021), concluded that Psychiatrists should be aware of potential aftermath of cybercrime on mental health, and the increased patient risk since the pandemic, including from online mental health services. After the pandemic, there has been a dramatic shift online for routine activities including work, school, shopping, entertainment, and doctor visits. Technology provides powerful tools, but these tools must be used with the appropriate safety measures. Human factors are a central component of cybersecurity as individual behaviours, personality traits, online activities, and attitudes to technology impact susceptibility. The authors also provide recommendations to recognize the increasing risk of cybercrime along with examples of USA organizations that provide advice about cybersecurity for consumers.

III. ONLINE CRIMES AND ONLINE ATTACKS

Every sector / region in the world, including business to education are facing the challenges of online attacks and crimes into their systems. We have categorized the reported cyber-attacks and online crimes for the four nations states: USA (+1), Canada (+1), Australia (+61) and India (+91) in context of the last five years' data. Many of the online attacks still go unreported due to various reasons, say complexity of scenario and unknown state of the victim worldwide.

A. UNITED STATES OF AMERICA

We all are familiar with the current scenario of post-COVID era and the ongoing vaccination around the world. The “stay-at-home” orders and “no mask no service” are now taglines at many places. Although this current scenario has left street crime to be decreased, online crime seems to be increasing. Like the rest of the nations around the world, the USA also shifts to the virtual (online) world by upgrading various security measures. This online shift creates new opportunities for offenders to engage in various online crimes, as millions of people start work

/ study from home [3]. We are living in the era of uncertainty, and we cannot measure every possible online crime nor predict cyber victimization as social distancing continues but we can apply counter measures (security measures) and theories (from the previous experiences of customers) to help us to counter the post-COVID situation.

Even customers today barely identify the type of attacks he/she faced online, the scope and dimensions of online crimes and online attacks vary from time to time and state to state. Identity theft and consumer fraud is the main reason that businesses face everywhere in the states. The number of data breaches and cybercrime is a current and rising problem (as COVID-19 resulted in 600 % rise in online crime worldwide) in the United States (and all over the world). The five most common cyber-attacks (although there exist more than 05 types of attacks) experienced by US companies, provided by Statista reports, include phishing (38%), network intrusion (32%), inadvertent disclosure (12%), stolen devices or records (8%), and system misconfiguration (5%) in 2019 [4].

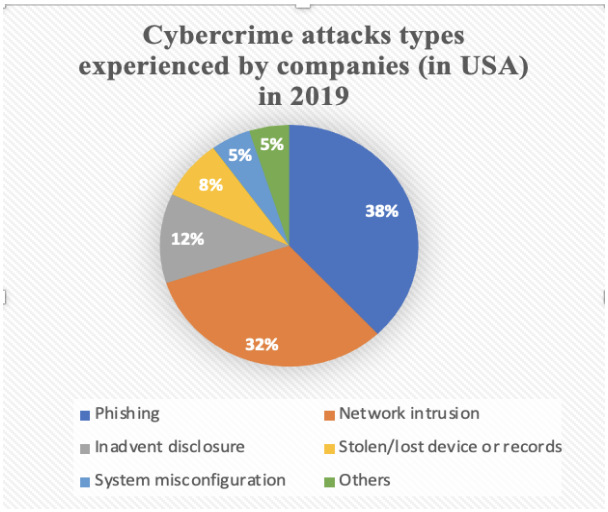


FIGURE 1. Most common types of cybercime attacks in USA (experienced by companies in 2019) [4]

Also, identity theft has many subtypes, ranging from credit card frauds (related to new accounts as well as existing accounts) to loan or lease (personal loan, auto loan, and business loan too). There are several complaints filed online and offline to the Internet Crime Complaint Centre (ICCC) in the United States (US). The below table illustrates the number of cybercrimes complaints from the year 2015 to 2020 along with the losses reported in US Dollars (USD) [5].

S N	Year	No. of Cyber Crimes (in USA)	Losses reported (in $ billions)
1.	2015	288,012	1,071,000
2.	2016	298,728	1,451,000
3.	2017	301,580	1,419,000
4.	2018	351,937	2,706,000
5.	2019	467,361	3,500,000
6.	2020	791,790	4,200,000

TABLE 1. Cyber Crimes and losses reported in USA for 2015-2020, based on complaints submitted to Internet Crime Complaint Centre (ICCC) [3] - [5]

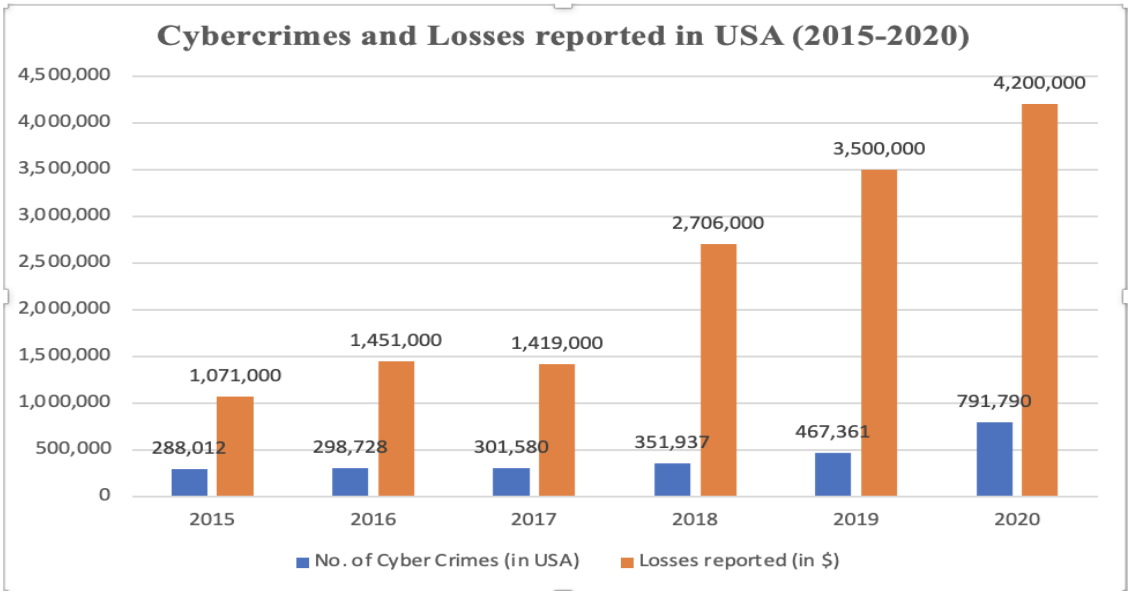


FIGURE 2. Bar graph representation of cybercrimes and losses reported in the USA, from 2015 to 2020. The cybercrime and losses reported ($ billions) are based on complaints submitted to ICCC [3] - [5]

B. CANADA

Like the USA, people are using the internet to commit crimes more than ever before in Canada too. The women of Canada were listed as the victims in around 70% cybercrime cases reported in 2018. Most of the cybercrime cases are still way under-reported and unsolved, despite several efforts of the Canadian government. The major cyber related violations (via Statistics

Canada) are Fraud, Child pornography, Harassing and Uttering threats. The Canadian Anti-Fraud Centre (AFC) released cyber complaints in 2020 by more than one-third over the previous year.

SN	Year	No. of Cyber Crimes (in Canada)	Losses reported (in $)
1	2016	23,996	17,500
2	2017	27,829	30,400
3	2018	32,968	41,600
4	2019	44,136	83,800
5	2020	66,752	160,100

TABLE 2. Number of Cybercrimes and losses in CANADA for 2016 - 2020 [13] - [16]

The Anti-Fraud Centre of Canada estimates that only five percent of victims file reports of cyber fraud. Meanwhile the COVID-19 also played a major role in cyber fraud, with cyber criminals trying to exploit people by clicking on the malicious attachments by offering medical benefits and vaccinations scams. Another example also includes, victims overseas trying to immigrate to Canada reporting a fraudulent website that offers to assist them in the immigration process, where these websites / suspected companies claimed to be in Canada too. The below table illustrates the number of cybercrimes reported and complaints in Canada, from the year 2016 to 2020 along with the losses reported in US Dollars (USD).

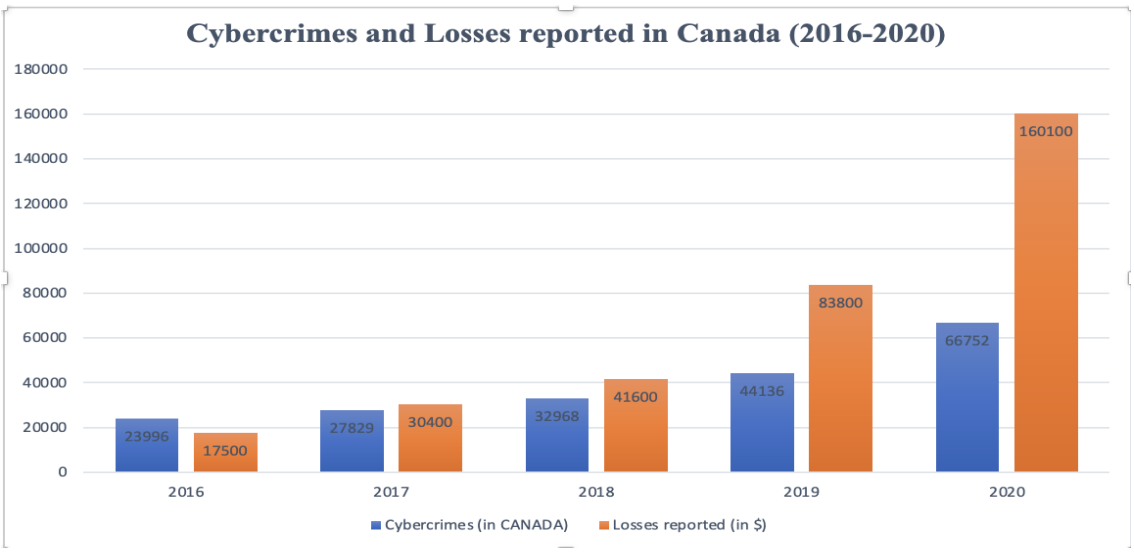


FIGURE 3. Bar graph representation of cybercrimes and losses reported in CANADA, from 2016 to 2020. The cybercrime and losses reported (in $) are based on cyber complaints to Canadian Anti-Fraud Centre (AFC) [13] - [16]

C. AUSTRALIA

Like other countries, in Australia cyber-crimes increase with different dimensions year by year. A cybercrime is reported, on average, every ten minutes in Australia as reported by Australian

Cyber Security Centre's (ACSC) annual cyber threat report [27]. Cyber criminals use a variety of methods to undertake to cheat Australian families out of their data and money. Within the last year, ACSC categorised 40 percent of 60,000 reports as frauds, specifically romance, investment or shopping scams. Cyber criminals use a high level of online connectivity and increasing delivery of services through online channels that make it attractive and profitable for cybercrime.

Australia's systems of national interest and demanding infrastructure are liable to malicious cyber activity. Computer Emergency Response Team (CERT) Australia responded from July 2014 to June 2015 there have been 11,073 cyber security incidents affecting Australian businesses, 153 of which involved systems of national interest, critical infrastructure, and government [28]. Top five non-government sectors assisted by CERT Australia in relevance to cyber security incidents were: energy, banking and financial services, communications, defence industry, and transport. Between July 2015 and June 2016, CERT Australia passed through 14,804 cybercrimes reports affecting Australian businesses, 418 of which involved systems of national interest (SNI) and significant infrastructure. Between 01 July 2016 and 30 June 2017, ASD – who takes the lead within the ACSC on incidents impacting government – undergone approx. 24,000 cybercrimes reports. Between July 2017 to June 2018 there have been approx. 53,567 cybercrime reports are recorded and there have been various newer styles of cyber-attacks considered during this era. There have been 64,567 cybercrime reports recorded between July 2018 to June 2019 increased from last year. Within the period of July 2019 to June 2020 there have been 59,806 cyber-crime reports at an average of 164 per day or approximately one report in every 10 minutes has been recorded. This can be a decrease from the previous year, with identical 64,567 between 01 July 2018 to 30 June 2019 [29].

SN	Duration (Year)	No. of Cyber Crimes (in AUS)	Losses ($)
1	July 01, 2014 - June 01, 2015	11,073	20,000
2	July 01, 2015 - June 01, 2016	14,804	187,000
3	July 01, 2016 - June 01, 2017	24,000	388,000
4	July 01, 2017 - June 01, 2018	53,474	493,000
5	July 01, 2018 - June 01, 2019	64,567	597,000
6	July 01, 2019 - June 01, 2020	59,806	634,000

TABLE 3. Number of Cybercrimes reported and estimated losses in AUSTRALIA (from July 01, 2014, to June 01, 2020) [27] - [31]

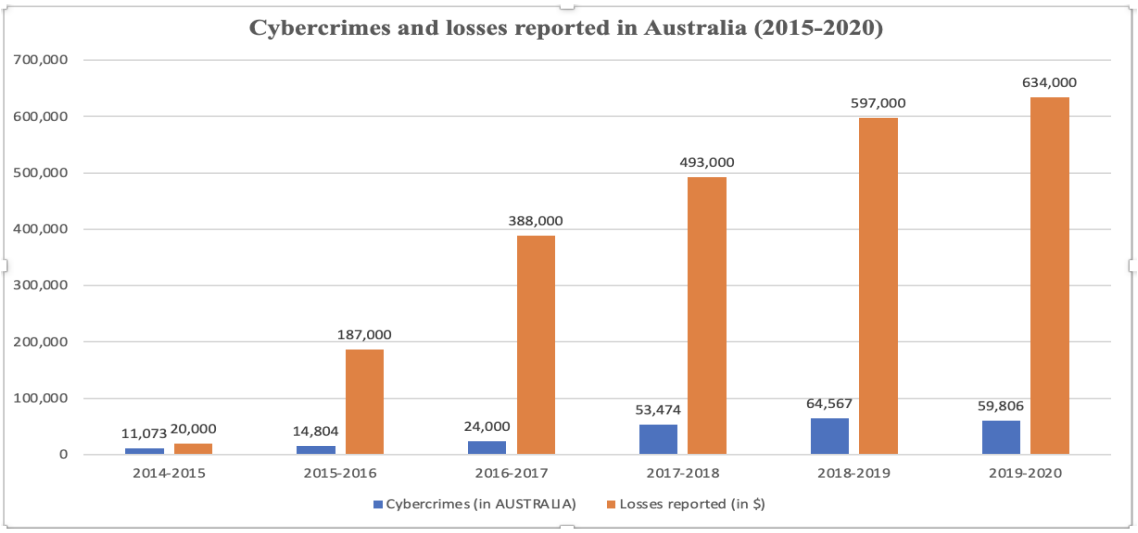


FIGURE 4. Bar graph representation of cybercrimes and estimated losses reported in AUSTRALIA, from 2014-15 to 2019-20. The cybercrime and losses reported (in $) are based on reports of ACSC and CERT [27] - [31]

The cybercrime by 2025, will cost approximately $10.5 trillion annually round the world, up from $3 trillion in 2015 [32]. Several reports by ACSC and CERT claimed that Australia has increased cybercrime of 13% per annum. In step with the study by Accenture, in Australia small businesses faced 43 % of cyber-attacks whereas only 14% were prepared for defence. The shortage of resources and finances are the main reasons to deny investment in adequate backups and cybersecurity programs by small and medium businesses which result in easy targets for cyber criminals. The attacks faced by small businesses mostly included phishing & social engineering attacks (57%), compromised or stolen devices (33%) and credential theft (30%). The foremost common category of cybercrime reported is ‘fraud’ which relates to criminals obtaining benefit through deception, like investment, shopping, or romance scams [30]. Identity-related crimes incorporating the theft and misuse of private information was the second most typical category followed by ‘cyber abuse’, While the numbers show that fraud is the commonest category, the ACSC assesses ransomware because the highest threat. This assessment is since, ransomware requires minimal technical expertise, is low cost and may end in significant impact to an organisation, potentially crippling core business functions. This can be the explanation why cyber-attacks are recorded less in 2019 – 2020 compared to 2018 to 2019 but as we see comparatively year by year cybercrimes increase and cybercriminals find other ways to accomplish it. Within the twelvemonth 2019 – 2020 after all cyber-attacks are recorded as approx. 5,000 cyber-attacks decreased but compared with previous year approx. 11,000 cyber-attacks record increases which is relatively 50% less decrement as cyber-attacks increase year by year.

D. INDIA

As we know that many countries of the world have been affected by the COVID-19 pandemic, India is also one of them. In this pandemic all offices, services (import-export etc) get stopped. Employees of companies do their work from home (WFH). In this disastrous situation where the CORONA virus increases day by day; the online crime and cyber-attacks are also at their

peak. The cybercrime and security report of Statista shows Uttar Pradesh state as most cybercrime cases with more than 2 million USD cost of data breach in 2020 [33] [36]. During the lockdown period, the online criminals and hackers do online frauds in different ways (almost 300% rise in cyber-attacks, without elaborating the attacker's profile). Here are some types of cyber-attacks used by them as follows [33]:

(a) Corporate Ransomware attacks
(b) Cyber Stalking
(c) COVID family research and COVID vaccine
(d) WFH approach and accessing of VPN

In the pandemic era, there are many ways used by online criminals rather than the above list. India (with many internet users) has seen a 37% increase in cyber-attacks in the first quarter (Q1) of 2020, as

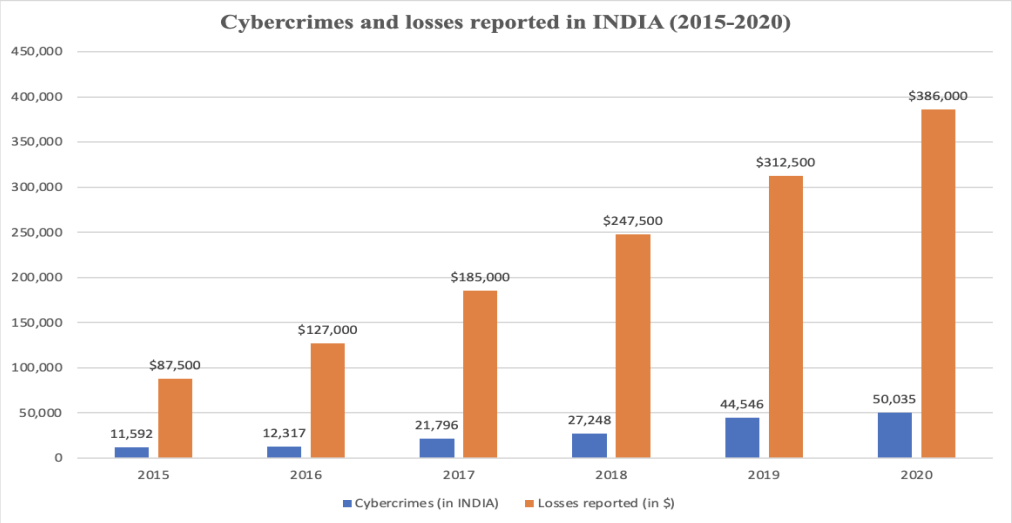


FIGURE 5. Bar graph representation of cybercrimes and estimated losses reported in INDIA, from 2015 to 2020. The cybercrime and losses reported (in $) are based on reports of NCRB and Statista [34] - [40]

compared to fourth quarter (Q4) of 2019 [34]. The smartphone users are being targeted more due to mass consumption. Risks like data leakage, connection to unsecured wi-fi networks, phishing attacks, spyware, apps with weak encryption (broken cryptography) are some common mobile threats.

Before discussing cyber-attacks in COVID-19 period we must look at cyber-attacks of the last five years in India.

SN	Year	No. of Cybercrimes (in India)	Losses (in $)
1	2015	11,592	87,500
2	2016	12,317	127,000
3	2017	21,796	185,000
4	2018	27,248	247,500
5	2019	44,546	312,500
6.	2020	50,035	386,000

TABLE 4. Number of Cybercrimes and estimated losses reported in INDIA from 2015 - 2020 [34] - [40]

The graphical representation of above data also shown below, you can clearly see that from 2015 to 2019 cyber-attacks increase respectively. We have also compared the four nation states based on the following 10 dimensions from ISO code to Mobile and internet providers (Table-5). The table also illustrates cyber-attack executions rank (in the world), along with cybercrimes reported and losses due to cybercrime (for year 2019) also.

IV. COUNTER MEASURES

Several counter measures and security practices are adopted to secure online transactions, counter frauds on the net / phone, and reduce the impact of online crime. One in all the common security measures to adopt is to use the “cyber ethics”, before or after targeting others (nations or states), within the name of protecting oneself. The moral defence proposal proposed is that the integration of assorted phase-wise security defence models with computer ethics attached that are primary to secure people, nations, networks, and systems [2]. Although attackers are always trying to seek out the weak points within the security systems, the ethics embedded defence model can help to tackle such bad guys.

Another major reason for increasing online crime traffic daily is use of varied algorithms and techniques for Artificial Intelligence (AI), Machine Learning (ML), and Fuzzy Systems (FS). The majority government and non-government organizations round the world (either publicly or secretly) are heavily engaged in developing such algorithms for his or her systems. The nations are worried and afraid of the development and technology advancements adopted by the opponent nations. They are engaged in protecting their own military troops with the assistance of autonomous weapons systems (AWS) and autonomous vehicles (AV) [22]. Hence, the increase in AWS business and robot weaponry will create more ethical and social challenges, and an ultimate rise in online crimes and attacks (both online and offline).

Dimensions	US (+1)	Canada (+1)	Australia (+61)	India (+91)
1. ISO code / Internet TLD	US / .us	CAN / .ca	AUS / .au	IND / .in
2. Population / HDI	> 328 M / 0.93	> 36 M / 0.93	> 24 M / 0.94	> 1379 M / 0.65
3. Area / GDP rank	3,796,742 sq. mi / 1st	3,855,100 sq. mi / 16th	2,969,907 sq. mi / 19th	1,269,219 sq. mi / 3rd
4. Military spending (2019) [17]	$649 billion	$21.6 billion	$26.7 billion	$66.5 billion
5. Cyber Attack executions rank (2020) [18]	6th (82.6%)	12th (78.0%)	16th (73.9%)	02nd (89.5%)
6. Cybercrime reported [19]	467,361 (2019)	37,466 (2019)	55,688 (2019)	94,546 (2019)
7. Cyber-attacks (most common type) [20]	Phishing: 38%	Phishing: 58%	Malware: 57%	ID Theft & Ransomware: 46%
8. Losses (due to cybercrime) [21]	35,00,000 (in $)	52,600 (in $)	69,500 (in $)	33,70,000 (in $)
9. No. of internet users (2020)	284.05 M (Popn rank = 3)	35.32 M (Popn rank = 39)	22.31 M (Popn rank = 55)	696.77 M (Popn rank = 2)
10. Major mobile & internet providers	Verizon, AT&T, Spectrum, RCN, Xfinity	Telus, Sasktel, Bell, Videotron	Telstra, Optus, TPG, iiNet, Dodo	Airtel, Reliance, Jio, Vodafone, and BSNL

TABLE 5. Ten dimensions comparison between countries including cyber data, crimes reported, cyber-attacks (most common type), internet users and losses due to cybercrime (based on four nations for the year 2020)

Today, with the rising development and use of online data, information and communication networks, the amount of online attacks / cyber-attacks on them are increasing and attack methods and targets are diversifying. As these cyber-attacks are perceived as a significant threat

to national security, countries round the world are stepping up their efforts to develop national cybersecurity policies. Major countries round the world nowadays are investing for establishment, expansion, and upgrades of their soldiers (cyber forces) to actively answer online attacks and cyber-attacks. In other words, they are strengthening their military capabilities against cyber threats. The US has also stepped up its aggressive response to cyber threats at the DoD. The Cyber Strategy, announced by the DoD in 2018, has shown its willingness to launch pre-emptive cyber-attacks to fundamentally prevent malicious cyber activities, also the strategy includes ways to strengthen cyber operations capabilities to punish hackers [23]. This determination is reflected within the National Cyber Strategy supported the principle to preserve peace through strength.

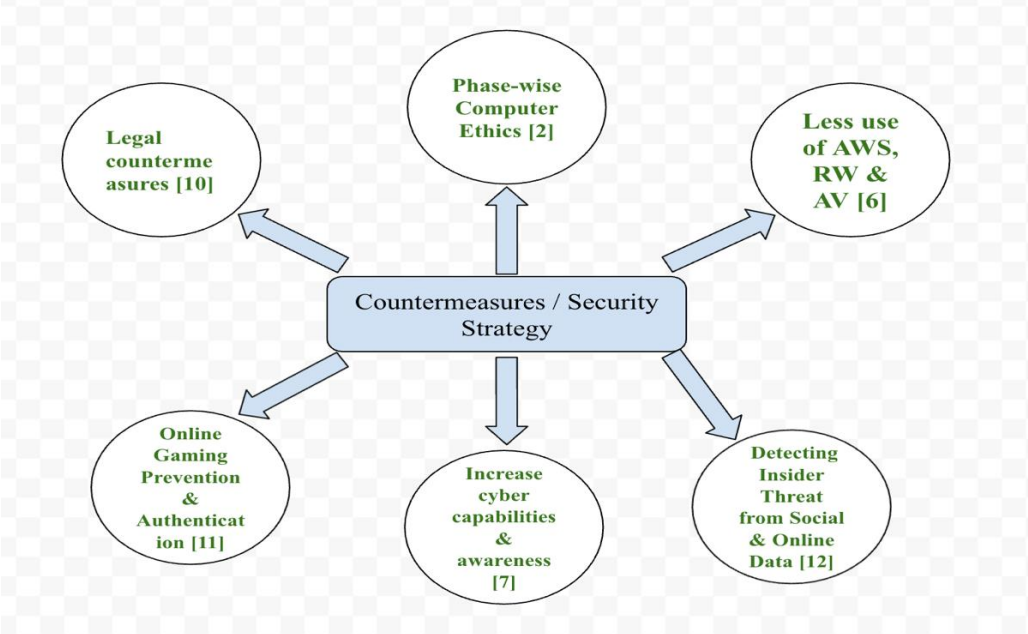


FIGURE 6. Various counter measures and security strategies (Based on online crimes and online attacks reported in POST covid scenario) [2] [6] [7] [10] [11] [12]

Cybercrimes are within the process of accelerating development and are getting gradually routine. There is a historical development of cybercrime and legal countermeasures. Cybercriminal phenomena have developed almost synchronously with ICT [24]. The criminal resources decide the quantity of crime, while judicial resources decide the deterrence. When the balance is reached between criminal resources and judicial resources within the long run, the criminal phenomena are saturated at an equilibrium point. The above figure (Figure 6) shows the key counter measures and strategies based on the recent online crimes and attacks reported. Besides deploying legal countermeasures and increasing military cyber power, the phase-wise ethics, and fewer use of RW, AWS will obviously help to tackle online crimes and attacks.

The growth of online devices, online users and data technology ultimately boosted the web "spending habits" of each person within the essence of shopping to entertainment. In Asia and Africa (mostly), the web gaming industry is incredibly successful and outstanding. Knowingly

or unknowingly, online gaming also gives rise to online crimes. The teenagers and our society spend huge hours of their time in such online activity.

Also, there is a scarcity of legal regulation, security and privacy protection as many players are involved in online gaming. The prevention and suggestion for such online crime includes preventing ID theft (with popular authentication methods), and several factors like enhancing ID authentication mechanisms, using insurance to guard virtual property, register customer identity by cafes, restaurants, and public internet providers etc [25]. Entertainment should return to entertainment only, and additionally to profits the gaming vendor must think / act like a tutor.

Another important aspect of security strategy for online crimes is to detect insider threats from enterprises, which is that the significant security risk for organizations. The abnormal behaviour (email communication patterns and content) including social and online activity data (web browsing patterns, email frequency, file, and machine access patterns) of employees will be considered to discover insider threats. The statistically abnormal behaviour w.r.t. features using state-of-the-art anomaly detection methods (unsupervised data driven approach) and declare this behaviour as a proxy for insider threat activity [26]. A visualization dashboard (visualization tool) is there for managers and HR personnel to quickly identify employees with high-risk scores to require suitable preventive measures and limit security risk. The users are organized with reference to hierarchy within the visualization tool, and upon selection of the user, his threat scores are highlighted allowing quick identification.

V. THE PROPOSED SECURITY (EAMV) MODEL

The rise in online devices and online users ultimately leads to online attack and online crime (as shown in Figure 7 above). The more people are working from home online, there are more opportunities for hackers (cyber criminals or bad guys) to exercise their techniques more frequently and make money. Small organizations and business firms also rely more than ever on computer systems, mobile devices, and exchange data & information as a method of practicing social distancing. After the careful study and comparison of online crime data, losses reported, various counter measures and security strategies, from the four countries (USA, Canada, Australia, and India), security measures based on online crimes, online attacks reported, and case study of growing online crime in the post-covid era, we have proposed the following security model (say EAMV model) that will ultimately help to secure / protect online data and information.

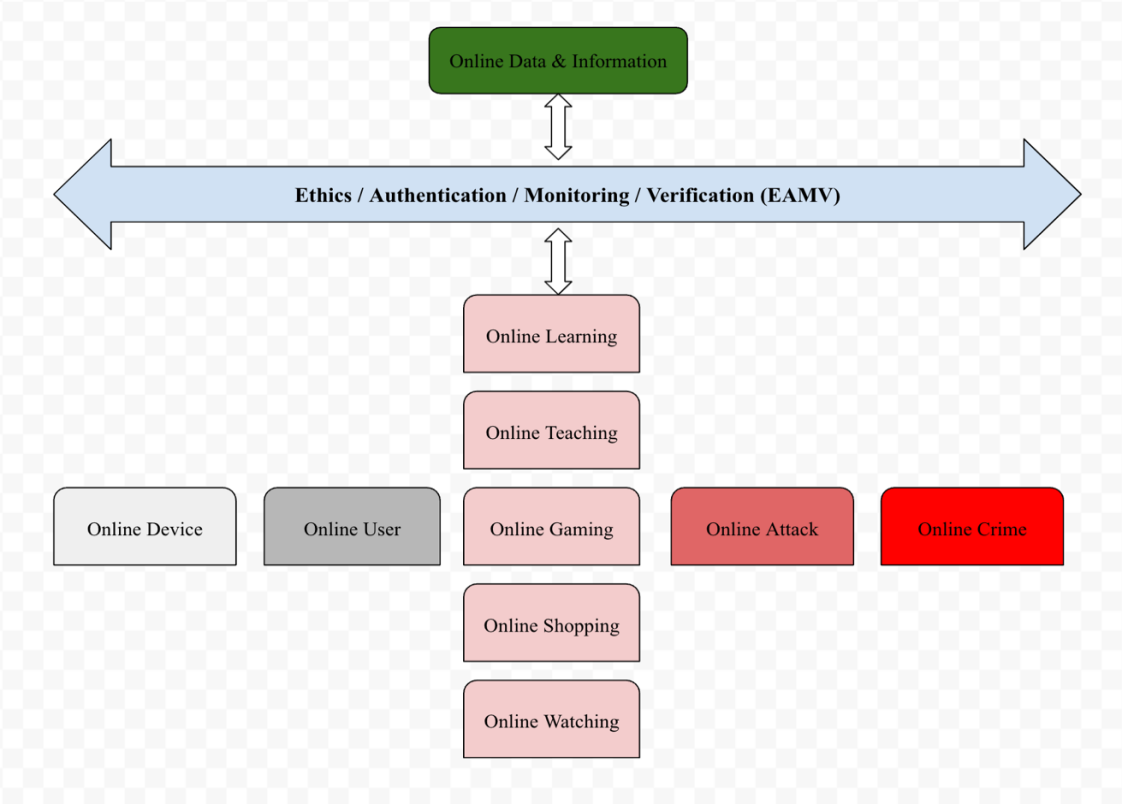


FIGURE 7. Our proposed security model i.e., Ethics, Authentication, Monitoring, Verification model (EAMV model) for prevention of online crime in post-COVID scenario

The rise in online devices in the ratio of users (say one user holding up to five internet-connected devices) is the symptoms (or green signal) of online attack and online crimes. People now are spending hours and hours of time, in the name of online learning, online teaching, online gaming and online shopping etc. Hence, we have requested the four firewalls / four security processes (EAMV model) as a must in our security model to counter the online request from the users. This proposed model seems to overcome the loopholes of existing security models with involvement of computer ethics, monitoring the source of request and performing the two-way verification process before giving access to the online data and information. The two-way authentication and verification (security-factor) is now with computer ethics / cyber ethics and continuous monitoring embedded.

VI. LIMITATION AND SOLUTION

Many individuals, companies, business firms, NGO, INGO, nation states etc. are the victims of data breach, fraud but online crime / online attacks against all of them are not included in this study. Although all sectors (including entertainment, gaming, education to work life) are affected, the healthcare industry was the industry with highest average data breach costs. We have also not included the attacks against the healthcare industry and research firms. The cybersecurity issues (for those working from home), training approaches of online security, challenges in investigating online crime are also not included. We have tried and focused our

best to collect / study the data of the last five years only of the four nations (included above), outlined the counter measures (based on online crimes and online attacks reported for the last five years), and proposed the security model (EAMV model) to safeguard the online data and information to prevent and/or reduce the growing online crime.

Ref.	Nation	5 major types of cybercrimes	Major insights, takeaways, and security steps *(to keep data safe either online data or offline data)*
[3] - [5] [12]	USA	Phishing, Network intrusion, In advent disclosure, Stolen devices, System misconfiguration	* Multiple phishing attacks discovered using Covid scheme * Street crimes seems decreasing, online crimes is increasing * Pandemic has not radically altered cyber routines nor changed cyber victimization rates * Provide a list of trusted sources and educate consumers on cybersecurity as a first step to increase awareness
[13] - [16]	CAN	Cyber fraud, Child pornography, Harassing, Uttering threats, Malicious attachments	* Around 70% victims are women in cases reported * AFC estimates that only 5% file reports of cyber fraud * Cybercriminals are trying to exploit people by clicking on malicious attachments (by offering medical benefits and vaccinations scams) * Fraudulent websites that offers immigration process assist, victim overseas trying to immigrate to Canada
[27] - [31]	AUS	Wire fraud & scams, Online frauds & shopping scams, Ransomware, Identity theft, Bulk extortion	* Cybercrime reported (by ACSC) on average of every 10 minutes (148 reports per day) * Out of 60,000 reports, 40% were “fraud”: specifically romance, investment or shopping scams * Beware of dodgy links, and use a variety of strong passwords * Limit the amount of personal information posted online (including your friends & family) * Total economic impact of cybercrime on Australian individuals (in 2019) was $3.5b approximately
[33] - [41]	IND	Hacking, Cross-Site Scripting, DoS Attack, Phishing, Spamming	* Lack of cybercrime awareness or mechanisms (actual figures could be under-reported). * Use a legitimate OS for your devices. * Keep browsers updated and use the latest version. * Never perform banking transactions using public Wi-Fi networks.

TABLE 6. Nation-wise five major types of cybercrimes (in USA, Canada, Australia, and India) with insights, and security steps (takeaways) to counter those cybercrimes and incidents reported

VII. CONCLUSION

This paper has compared the number of online crimes, cyber-attacks and losses reported within four nations: USA, Canada, Australia, and India. The pandemic has pushed the whole world under stress, worries for mental health, and quarantine. The cyber criminals and bad guys are even more active than before for stealing user's information duplicated, or sold etc. The rise in online devices, online users, and online work from home has ultimately given more space and opportunities for cyber criminals. We also request all internet users, not to click on unknown websites, links and not to respond / reply to unknown emails and follow the counter measures (if possible). We have also presented counter measures and security strategies based on increasing cybercrimes in the post-COVID scenario. Our study concluded that the number of online crimes (say, phishing or hacking etc.) is increasing rapidly after COVID-19 as the maximum number of online crime cases goes unreported in this quarantine time. We have also proposed the security model (EAMV - Ethics Authentication Monitoring Verification model) to protect and secure the online data and information. The basis of computer and cyber ethics must be taught in every schools and university curriculum. Users must be trained about the two-factor authentication process which is now followed by tech giants and many universities while logging in. User must also continuously monitor and verify the domain name and the URLs they are visiting or redirecting (in case of new links before clicking them).

VIII. FUTURE SCOPE

From the above overview, study, and comparison of four nation states based on online crimes, number of cyber-attacks and losses reported, several future works and scopes can be identified (that will support researchers and security professionals) in addressing challenges related to cybersecurity to propose and design new tools, security policies, frameworks with use of emerging technologies. In the future, we intend to provide a training and awareness framework, security standards for individuals, end-users, and organizations / companies / business firms at primary level to counter the ongoing and never-ending online crimes and cyber-attack.

Author Contributions: Conceptualization, NK; Background Study, NK, AS; Survey and Investigation, NK, AS; Writing - original draft, NK; Writing - review and editing, NK, AS. All authors have read and agreed to the published version of the manuscript.

Data Availability: The data presented in this study are available within the article and its references.

Conflicts of Interest: The authors declare no conflict of interest.

Funding: The author(s) received no financial support for the research, authorship and / or publication of this article.

REFERENCES

[1] Package Homer, 13 February 2020, Multiple Phishing Attacks Discovered Using the Coronavirus theme, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/multiple-phishing-attacks-discovered-using-the-coronavirus-theme/

[2] N. Kshetri, and K. Miller, A Study on Cyber-Defence Ethics, and Initiatives by Governments of

Under Developing Nations: A Study of Selected Countries, The International Journal of Analytical

and Experimental Modal Analysis (IJAEMA), ISSN No: 0886-9367, Volume XIII, Issue I, January/2021, Page 977-986

[3] I.C. Eian et. al., Cyber-attacks in the era of Covid-19 and possible solution domains, Preprints (www.preprints.org) (2020), Posted: 26 September 2020, doi:10.20944/preprints202009. 0630.v1

[4] Statista, Cybercrime and security, Most common cyber-attacks experienced by companies in 2019, https://www.statista.com/statistics/293256/cyber-crime-attacks-experienced-by-us-companies/

[5] Insurance Information Institute (III), Facts + Statistics: Identity theft and Cybercrime, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[6] C. Tran (2020), Recommendations for ordinary users from mitigating phishing and cybercrime risks during COVID-19 pandemic, axXiv:2006.11929 v1, May 2020

[7] MK Kagita et. al. (2020), A review on Cybercrimes on the Internet of Things, axXiv preprint axXiv:2009.05708, September 2020

[8] James Hawdon et. al. (2020), Cybercrime in America amid COVID-19: The Initial Results from a Natural Experiment, American Journal of Criminal Justice (2020), https://link.springer.com/article/10.1007/s12103-020-09534-4, June 2020

[9] H.S. Lallie et al. (2021), Cyber security in the age of COVID-19: A timeline and analysis of cybercrime and cyber-attacks during the pandemic, axXiv:2006.11929, June 2020

[10] K. Kumar and B.P. Pande (2021), Rise of online teaching and learning processes during COVID-19 pandemic (Chapter 14), Springer Nature Singapore Pte Ltd. 2021 P. K. Khosla et al. (eds.), Predictive and Preventive Measures for Covid-19 Pandemic, Algorithms for Intelligent Systems, https://doi.org/10.1007/978-981-33-4236-1_14, Chapter January 2021

[11] M. Hijji and G. Alam (2021), A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions, IEEE Access DOI: 10.1109/ACCESS.2020.3048839, January 2021

[12] S. Monteith et. al. (2021), Increasing cybercrime since the pandemic: concerns for Psychiatry, Springer Nature 2021, Psychiatry in the Digital Age, Current Psychiatry Reports (2021), https://doi.org/10.1007/s11920-021-01228-w, Published online: 03 March 2021

[13] Cybercrime is going up across Canada and most cases remain unsolved, https://www.blueline.ca/cybercrime-is-going-up-across-canada-and-most-cases-remain-unsolved/#:~:text=Statistics%20Canada%20compiled%20data%20gathered,per%20center%20of%20all%20cases.

[14] Police-reported cybercrime, by cyber-related violation, Canada (selected police services), https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510000101
[15] Cyber fraud complaints in Canada took huge leap in 2020, IT World Canada, https://www.itworldcanada.com/article/cyber-fraud-complaints-in-canada-took-huge-leap-in-2020/441676
[16] National Cyber Threat Assessment 2020, Canadian Centre for Cyber security, https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf
[17] World Population Review, Military Spending by Country, https://worldpopulationreview.com/country-rankings/military-spending-by-country
[18] 2020 Cyber Threat Defence Report, CyberEdge Group, www.cyber-edge.com, https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
[19] Cybercrime in Australia, Australian Government, Australian Cyber Security Centre (ACSC), cyber.gov.au via Australian Cybercrime Online Reporting Network (ACORN)
[20] Share of organizations who were targeted by cyber-attacks in Canada, https://www.statista.com/statistics/827317/canada-companies-cyber-attacks-techniques-used/
[21] Consumer loss through cybercrime worldwide, https://www.statista.com/statistics/799875/countries-with-the-largest-losses-through-cybercrime/
[22] N. Kshetri, A Survey of Computer Ethics (w.r.t. AI, RW, FS, AV), The International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN No: 2278-3075, Volume 10, Issue 4, February 2021, Page 207-210
[23] Sang-bae Kim, "Cybersecurity strategies of the Trump administration: complex geopolitical responses to state-sponsored hacking", Journal of International Area Studies, vol. XXVII, no.4, pp. 1-35, 2018.
[24] J. X. Li, Cyber Crime and Legal Countermeasures: A Historical Analysis, International Journal of Criminal Justice Sciences (IJCJS) 2017, Vol 12 Issue 2 Jul-Dec 2017, Page 196-207
[25] P.S Chen and R. Song, Online Gaming Crime and Security Issue - Case and Countermeasures from Taiwan, Proceedings of the 2nd Annual Conference on Privacy, Security and Trust Canada National Research Council of Canada
[26] G. Gaurang et. al., Detecting Insider Threat from Enterprise Social and Online Activity Data, 2015 ACM. ISBN 978-1-4503-3824-0/15/10 ...$15.00. DOI: http://dx.doi.org/10.1145/2808783.2808784
[27]Australians report 160 cybercrimes every day, https://ia.acs.org.au/article/2020/australians-report-160-cyber-crimes-every-day.html
[28] ACSC threat report 2015 demonstrates that in 2014, CERT Australia responded to 11,073 cyber security incidents, https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2015.pdf
[29] ACSC Annual Cyber Threat Report, July 2019 to June 2020, https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf
[30] Cybercrimes in Australia more specifically focusing in 'fraud' by cyber criminals, https://www.cyber.gov.au/sites/default/files/2019-12/Cybercrime%20in%20Australia%20%E2%80%93%20July%20to%20September%202

019%20%28December%202019%29.pdf
[31] Australian Government, Australian Institute of Criminology, Statistical Bulletin 34, Estimating the cost of pure cybercrime to Australian individuals, https://www.aic.gov.au/sites/default/files/2021-07/sb34_estimating_the_cost_of_pure_cybercrime_to_australian_individuals.pdf
[32] KM Tech, Published on: 12th April 2021, Top 10 cyber security statistics and trends for 2021, https://kmtech.com.au/information-centre/top-10-cyber-security-statistics-and-trends-for-2021/
[33] Almost 300% rise in cyber-attacks (particularly during lockdown) in India in 2020, government tells Parliament, https://www.hindustantimes.com/india-news/almost-300-rise-in-cyber-attacks-in-india-in-2020-govt-tells-parliament-101616496416988.html
[34] Outlook, The News Scroll, 23 May 2020, 37% rise in cyberattacks in India in Q1 (first quarter) 2020: Report, https://www.outlookindia.com/newsscroll/37-increase-in-cyberattacks-in-india-in-q1-2020-report/1843637
[35] Statista statistics (04 February 2021), Incidents of cyber-attacks across India from 2015 to August (in 1000s) https://www.statista.com/statistics/1201177/india-number-of-cyber-attacks/
[36] Statista (10 March 2021), Published by: Sandhya Keelery, Cybercrime in India – statistics and facts, https://www.statista.com/topics/5054/cyber-crime-in-india/#dossierKeyfigures
[37] National Crime Records Bureau of India, Ministry of Home Affairs, Sharp increase of cybercrime in India during last decade (Recorded cybercrime cases in India from 2010-2018), https://ncrb.gov.in/en/crime-in-india-table-contents?page=43 [38] The Hindu, (September 15, 2021) India reported 11.8% rise in cybercrime in 2020; 578 incidents of 'fake news on social media': Data, PTI, New Delhi, https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece
[39] Business Today, NewsFlicks, Cost of Cybercrime: Indian consumers lost $18.5bn in a year, https://www.businesstoday.in/bt-newsflicks/photo/cybercrime-personal-data-protection-loss-consumers-5690-2018-08-06-1
[40] Statista, October 25, 2021, Published by: Sandhya Keelery, Number of cybercrimes reported across India from 2012 to 2020, https://www.statista.com/statistics/309435/india-cyber-crime-it-act/
[41] N. Kshetri, Cyber Strategy of Government of Nepal, SSRN Electronic Journal, DOI: 10.2139/ssrn.3552143, January 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3552143

AUTHOR(S) PROFILE



NARESH KSHETRI *(Student Member, IEEE) is currently a PhD scholar with the Department of Computer Science at University of Missouri – St. Louis (UMSL), Missouri, USA. He received MS (Cybersecurity) from Webster University, Saint Louis, Missouri, USA (2017) and Master of Computer Applications (MCA) from University of Allahabad, India (2014). He is currently working as a graduate teaching assistant / graduate research assistant for the computer*

science department, UMSL. He has more than seven years of experience in teaching and research. He has a total of five publications in reputed international journals and Conference Proceedings in his credit. His current research interests include online crime, blockchain technology, cyber defence, and computer ethics.



AJAY SHARMA *is presently a research scholar at Kamla Nehru Institute of Technology (KNIT), Sultanpur, India. He received Master in Technology (MTech Computer Science and Engineering) from KNIT, Sultanpur, Uttar Pradesh India in 2019 and Master of Computer Applications (MCA) from SVSU, Meerut India in 2013. His current research areas are Data mining and Image processing*