International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

From Digital India to Digital Economy: Understanding India's Cyber Infrastructure and Cyber Security

Roshan Rai

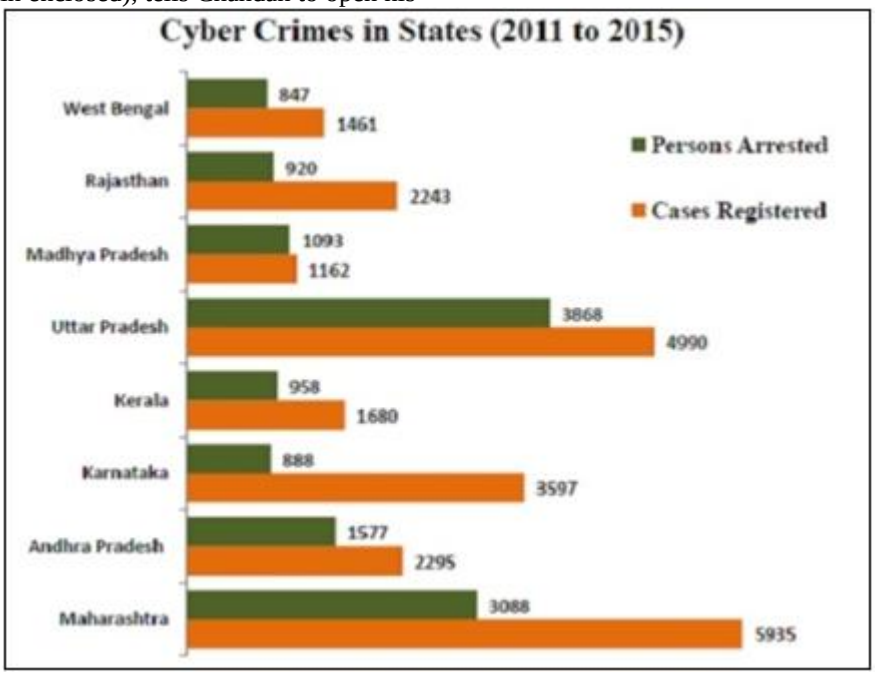
Abstract: ***Cyber security has become important security paradigms of the 21st century. It is a non - traditional security issue that has come into the limelight, fostering states to strengthen it. In today's world data has become indispensable; every actor from state to non - state wants data for various purposes, as Clive Humbly proposed that data has become the new oil. As India is moving towards a digital platform and the challenges are enormous emerging from the implementation of digital India. India's cyber infrastructure is not well equipped with advance detection and anti - malware system. With the introduction of digital India, digital economy has started gaining preference, people have moved their transaction on digital mode, to which many cyber criminals have taken the chance to dupe people through various strategies.***

Keywords: CII, STUXNET, CERT - IN, ATO

1. Introduction

The advent of the 21st century has brought tremendous change in the communication and technological sector. Technological change has always been closely linked to social change (Heywood, 2011: 138). The rise of modern tools and technologies has made human lives more feasible. The problem arises when technologies are developed rapidly without a human understanding of the former, the latter floods the market. As Michael Hayden (former director of National security Agency) argues "in today's globalized world, technologies are developing extensively and without understanding the prior technologies, new technologies come outs, this is where the technological gap is created". He further adds that this technological gap is exploited by criminals.

Chandan (name change) a master student gets an anonymous call from an individual stating that he is an employee of a bank (identity to remain enclosed), tells Chandan to open his online payment app and claim his cash back by accessing the link, which is sent to his online payment app. Chandan, a well - educated man and a product of modernization, knows it's a fraud call, but his intuition drives him to open an online payment app. He saw a notification visible on the icon, he opens and taps the link, and the next thing to open on his screen is to enter his four - digit security pin. Once he enters the pin, a certain amount of money will be deducted which will be the same amount of money that is provided in the link. He refrains from doing it and hangs up the phone, thus saving his money. The deal is there are lots of people in India who fall into these types of scams. According to national crime records bureau data, in 2019, Bengaluru recorded the highest number of cybercrime among all metro cities in India with 10, 668 cases (Dev, 2021); (look at the fig1.1). The strengthening of cyber security and various awareness programs can be a viable solution to deal with this type of situation.



Source: Factly.2016. Dubbudu, Rakesh.

Cyber security refers to the protection of the internet - connected system, including hardware, software and data from cybercriminals (Seema et al, 2018). Cyber security as a non - traditional security issue has become an integral part of national security. It has become an integral part of many policy making processes, and have been a major stack in protecting the national asset. As the government of India has launched a digital India programme for fostering growth there is a critical asset like banking institutions that have to be protected, as [29] put it "digital India cannot do much without the protective wall of cyber security.

This paper is written through extensive use of secondary sources like journals, books and news articles. The study is based on descriptive analysis. The paper deals with an understanding of India's cyber security and cyber infrastructure and its critical role in digital India initiatives. Further, the article argues how India can strengthen its cyber security in the backdrop of attackers originating from transnational.

What is Digital India?

Digital India is a flagship programme of the Government of India with a vision to transform Indian society into a digitally empowered society (Boro, 2017: 922). The digital India program was launched on July 1st, 2015 with a vision to empower every citizen through digital access to information, services and good governance (CNBC TV18, 2021). The core prospect of digital India is to build and strengthen digital infrastructure for the utility of citizens, governance and service for the people and the digital empowerment of citizens. The mission of digital India is to build a participative, transparent and responsive government that can reach out to the citizen and support them by providing service through mobile apps and cloud computing.

The historical trajectory of the digitization of India can be traced back to the period after liberalization, after the incumbent period of liberalization in the 1990s, India veneering change in the technological sphere marked a new beginning in the information and technology sphere. The Implementation of e - governance started to get priority as a vital element of the urban reform agenda in many government sectors. E - governance refers to the technologies used by government agencies that can transform relations with citizens, businesses and other arms of government (NISG, 2012: 16). The idea of digital India does not stand in a vacuum, there are multiple legislation and policies initiated by the Government of India to transform India into a digital hub.

Digital India program has witnessed agrowth trajectory with its various initiated bodies, there are a plethora of initiatives which include the development of broadband highways, universal access to mobile connectivity, public internet access programmes, e - governance to name a few. Many major schemes and projects such as Aadhar, Smart Cities Mission, BHIM UPI, RuPay, GSTIn, GeM (Government e - Marketplace), and DigiLocker come under the aegis of the Digital India programme (Dataquest, 2020). Digital India initiative is built on nine pillars these are; (1) the government of India aims to provide nationwide information infrastructure with the help of optical fibre especially focusing on the rural areas, which will help the rural people to get information. (2) Universal access to mobile connectivity: To achieve a vibrant digital India, it must ensure that connectivity reaches to all. India needs wireless information connectivity that can be provided by mobiles to all the masses that are not in the purview of digital reform (Boro, 2017: 923 - 924). (3) Public internet access programmes in today's world have become an integral part of society. Everything has moved online from minor to major industry operating systems. Therefore, it is necessary to have access tothe internet for the larger benefit of society. (4) E - governance: India has moved its governing system towards digitization, bio matrix thump in transaction and Aadhar linkage with bank account has become mandatory for safety and security purposes. The government of India aims to improve the processes and delivery of service through e - governance. (5) E - Kranti: it is an initiative toaware people of the benefit of e - governance by providing services through various sectors which deal with health, education, farmer, security, financial inclusion and another service. (6) Electronic manufacturing: Prime Minister Narendra Modi vision of 'make in India' propagates the idea of manufacturing electronic devices in India rather than importing from outside, this will primarily uplift the domestic manufacturing sector of India. (7) IT for jobs: This project involved training 0.5 million rural IT workforce in five years and setting up of BPOs in each northeast state. (8) Information to all: The basic motive of this initiative is to provide the citizen of India with all the information they need. It also enables communication with the government in a much easier way. (9) Early harvest programme: This comprises numerous programmes including a mass messaging platform for broadening information concerning government programmes (journal of India, 2021).

Digital economy

The digital economy which is a subset of the larger digital India programme has become an integral part of society. It is estimated that India's digital economy has the potential to become a 1 trillion USD ecosystem by 2025 (Chakraborty, 2021). This will create multiple opportunities in various sectors like foreign investment; the growth of domestic digital infrastructure will also lead to the growth of medium and small businesses, but there are major challenges ahead for India's digital economy. The major challenges for the digital economy are the threat coming from the cyber world; various websites can be hacked in a blistering second by cybercriminals. The Ministry of Electronics and Information Technology in a written reply to Rajya Sabha informed that a total of 158 websites of Central and State Governments were hacked during the year 2018 and 2019 respectively (Shukla, 2019). People will fear sharing their data if the threat persists in cyberspace and jeopardize the government initiative. The challenges are far too comprehensive to detect because the attacker's identity remains largely anonymous. Digital India can harness promising outcomes only if resources and time are diverted properly (Dua, 2018).

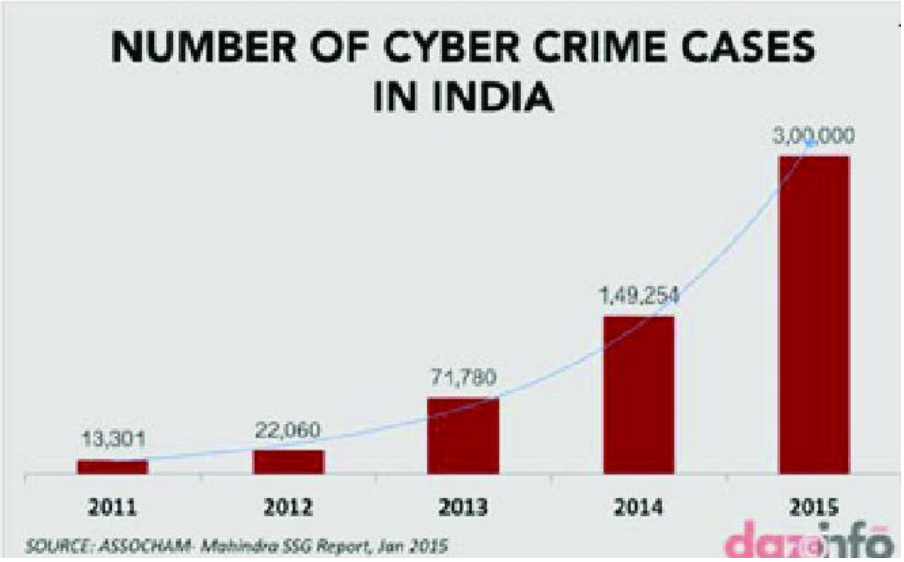
India's cyber infrastructure

India had modernized various sectors after the liberalization and the introduction of the internet in 1995, which had

marked a new beginning in India's internet paradigm (Dilipraj, 2021: 93). Today, the world has become more technology - driven with home delivery to work sitting in the home; therefore, it is necessary to have a strong cyber infrastructure for feasible purposes. Cyber infrastructure is a holistic sphere that brings intricate technologies (hardware, software, processing, and storage, communication) to facilitate a coherent end - to - end functionality in support of the application. The term 'cyber infrastructure' was coined in the late 1990s and the usage of this term pervasively began from 2003 with the publication of 'Revolutionizing science and engineering through cyber infrastructure (Stewart et. al, 2010). As (Natarajan, 2010: 148) points out cyber infrastructure are consisting of advanced computational engines (supercomputers), mass storage, high - performance next - generation network and services which are diverted to serve individuals and organizations for their better lifestyle. The viruses which are optimized for the attacking minuscule minutes can spread across countries causing widespread damage and potentially crippling cyber infrastructure (Kumar, Mukherjee, 2013). India's cyber infrastructure has also multiple loopholes; especially its critical information infrastructure (CII), there had been multiple attacks on the health sector, and financial sector to name a few.

The term "critical information infrastructure" refers to the essential infrastructure, which provides essential support to the economy and social well - being of the people and forges the functioning of the key government responsibilities (Parid, 2021). Critical information infrastructure supports every economic activity and it is intertwined with various sectors. Critical information infrastructure refers to communication and information service whose availability, reliability and resilience are essential to the functioning of the modern economy, security and other essential social value. The interdependence of these infrastructures is necessary for supporting the economy of a nation - state ranging from power distribution to transportation and finance to governance (Sharma, 2017: 26). The critical information infrastructure has varied branches like telecommunication network, transportation (railways, air traffic control, city traffic control), financial service (credit card function, online payment system, electronic stock trading), industries related to energy and manufacturing (Parid, 2021). The definition of critical infrastructure varies from country to country; its definition has been discursive over the period.

Cyber attacks are generally used for taking down critical infrastructure; cyber attack refers to gaining authorisation by an unauthorized entity to have access over other computer systems or computer networks with the intent to cause damage. It can be launched from anywhere by any individual or group using various strategies (Pratt, 2021). The use of cyber attacks is carried out by both state and non - state entities, targeting a certain critical information infrastructure (CII) causing a kinetic impact (DSCI, 2020). From the state perspective, cyber - attacks are carried to gain leverage in international affairs, national security and pre - emptive measures, while non - state actors have their motive of launching cyber attacks, for example, economic benefits, espionage and propaganda. In 2007 Estonia faced a massive cyber attack, its vital infrastructure was taken down, no bomb, no explosion, the country was plunged into chaos, and news website to power system everything collapsed (ET, 2017). These showed that cyber attacks can cause huge disruption and panic in the public sphere also damaging property and lives. Cyber attacks are considered as a "next - generation threat", India is among the top five target countries of malicious activity, using the Internet that ranges from cyber defamation, denial of service attack, email bombing and hacking to an individual identity. The number of cyber attacks has been steadily rising from 23 in 2004 to 2, 565 in 2008 to 10, 315 to 13, 301 in 2011 and 62, 000 until mid - 2014 (Devi, 2019), fig 1.2 shows the crime cases, 2011 - 2015.



Source: research gate. A survey on cloud forensic challenge and solutions. Simov et. al.2016

In India, section 70 of the IT Amendment Act, 2008 describes CII as "the computer resource, the incapacitation or destruction of which shall have a debilitating impact on national security, economy, public health or safety" (Parid.2021). Despite several measures taken through a legal framework, cyber - attack has swiftly targeted many sectors.

India was the third most affected country by computer worm STUXNET. Many reports suggested that some 10, 000 infected Indian computers were corrupted, 15 were located at critical infrastructure facilities. These include the Gujarat and Haryana electricity board and an offshore state - owned ONGC (ET, 2017). Critical information infrastructure interconnectedness and interdependence with other infrastructure, which crosses the physical and political border has put the governance in dismay, regulation remains in dilemma. The strengthening of critical information infrastructure is the only option that remains for the state to tackle this problem.

Banking and Financial sector vulnerabilities

Banking institutions runs multiple servers which store an enormous amount of information and details of various operations such as credit card, ATMs and SWIFT service (the global financial messaging service banks use to move funds), among others (Reddy, Bhargavi, 2018: 65).

The digitization of payment services and financial transactions has become the prime driver of the digital economy. Therefore, vulnerabilities may increase in this sector, careful analysis and concerted effort is needed for securing high paced transformation of the transaction process (DSCI, 2020). Humans have developed so immensely that conventional notion has become taboo, like in today's world we may not witness an armed robbery, where guns are used and hostages are held like classic cinematography. Today robbery can take place virtually in cyberspace. Cybercriminal has entered in the realm of skulduggery which includes stealing customer debit and credit card data. The phishing activity is another major threat to financial service, the criminal extract exclusive facts consisting of credit card numbers, username and password through masquerading as a valid enterprise. It is done through mobile phone and email spoofing. The Indian banks have myriad numbers of customers and each customer have their digital preference; these preferences are based upon the customer feasibility to operate the digital system, the perception of risk associated with the digital process and the nature of information service requirements are needed of the hour. Bank has to assure a hybrid custom interaction channel (Deloitte, 2020: 10). The Reserve Bank of India directed the bank to implement a security policy, which will deal with cyber threats and cyber - hygiene in 2016 (Bhargavi, Reddy, 2018: 66). In 2018 hackers managed to siphon off over Rs 94 corer through a malware attack on the server of Pune based cosmos bank and cloning thousands of bank debit cards over two days (PTI, 2018). It is also estimated that SBI has an unprotected server that gave access to the financial information of its million customers to anyone looking for it (ET, 2021). Mobikwik the digital credit and payment processing start - up reportedly suffered a data of nearly 10 corer users. The breach saw the compromise of sensitive data, including credit and debit information, with news reports suggesting that such data was consequently posted for sale on the dark web (Banerjee, Sohini; Menon, KS Roshan, 2021). The rise of account takes over (ATO) in the Indian context has created a serious data security breach and online financial fraud (Kumar, 2021). ATO refers to the control over the account of others to steal credit or debit information and other various cybercrimes. The government has to take major steps in dealing with banking and transactions institutions, people trust these institutions. The ineffectiveness of dealing with cyber threats will create a serious breakdown in economy and ones trust.

Is India ready for Digital Economy?

The introduction of digital India was a remarkable start to a holistic transition of various sectors into the digital sphere. There was a rapid change in governance, bureaucracy and functioning of various private sectors. The adoption of digital technologies and consumers adopting cashless payments is one of the attributes of the digital economy, a subset of digital India. The proliferation of data with the increased use of Smartphone has opened multiple opportunities for cyber fraud (Chudasama, 2021). India has made only modest progress in developing its policy and doctrine for cyberspace, looking at the interest of India geostrategic need, proper formulation of cyber policy is the need of the hour (The Hindu, 2021). The computer emergence response team (CERT - IN) recorded that last year, the cyber attack rose from 394, 499 in 2019 to 1, 158, 208 in the first quarter of 2021 (Chudasama, 2021). The threats to India's critical information infrastructure is immense and loaded, as it not only sustain the economy but also contains millions of data, which is important for a country, stealing and manipulating it will create a serious security concern as holistically and hampered economic growth. Information of patients, credit card details, government data and accounts of the high - profile people are at threat.

Therefore, to foster a digital economy without any hindrance, there has to be a proper implementation of cyber policy. The government has to fund R&D, proper investment should be made, encouraging the development of new software systems and firewalls and patronizing the white hackers. A partnership among both public and private sectors is needed and acknowledging the fact that cyber thieves are probably a step ahead and hence making citizens specifically aware of risks is the first step (Chakrabarty, 2020).

Strengthening India's Cyber infrastructure

The national critical information infrastructure protection centre (NCIIPC) duty is to take all necessary measures to refrain from any unauthorized access, modification, disclosure, disruption, incapacitation or destruction through strategic coordination, synergy and raising information security awareness among all stakeholders. NCIIPC provide a framework for the organization to create robust information infrastructure that can stop modern cyber attacks. The NCIIPC guidelines apply to any network or link between networks that can create exposure to the critical system that support the day to day operations of commerce and government (skybox, 2016). CERT - IN is also looking after the Indian cyberspace. The nodal agency is responsible for the collection, analysis and dissemination of information on the cyber incident and taking emergency measures to contain cyber - related incidents. It is mandatory to report to the CERT - IN in the following instance (i) targeted

intrusion or the compromising of the critical network system; (ii) unauthorized access to IT system or data; (iii) attacks on applications, such as e - governance and e - commerce (Agarawal, 2021).

To deal with cyber security the government of India can take several measures like having a separate budget for cyber security. So, that more R&D and investment can be diverted to pool, empowering security leadership and strengthening security in both IT and OT environments. There is a lack of understanding between the public and private enterprises. The private industry is very sensitive to any cyber breach in their respective organisation. Therefore, both stakeholders should form entities to deal with the problems of cyber attacks. Cyber threat is a transnational problem, to deal with this transnational threat, India alone cannot do much, therefore, it has to forge alliances with other countries. For example, France and India have kick - started a bilateral cyber security technology partnership aimed at combating cybercrime, online rights and promoting digital commerce and innovation (Banister, 2019). India has also launched; centre of excellence of software development and training (CESDTs) in Cambodia, Laos PDR, Myanmar and Vietnam with enhancing digital cooperation (NDTV, 2020). India and the United States have also renewed their agreement to cooperate in the field of cyber security; the agreement was signed between the India computer emergency response team (CERT - IN), under the Ministry of Electronics and Information Technology and the Department of Homeland security Government of the United States (ET, 2017). The respective sectors and governments of India have to take cyber threats personally and have to recognize their potential threat, thereby inculcating a strong response to the attackers.

2. Conclusion

Cyber security over the years has become an important paradigm; the expansion of technologies has uplifted human beings to a new height. People all over the world use computers today for various purposes, it has made our life easier while at the same time it has also increased the risk of cyber threats. It is hard to predict a cyber threat because the identity remains anonymous and also due to its transnational nature. Cyber security is concerned with making cyberspace safe from threats, cyber security is no longer limited to security, it is now linked to socio – economic factors as well, which include politics, industry, health, education and critical infrastructure. To ensure smooth functioning of the country's digital market and to ensure the stability of critical cyber infrastructure, well - functioning cyber security should be at place. For the success of government initiatives like digital India, make in India and smart cities, cyber security is critical. The future of cyber security in India will improve in days to come but mere initiatives and policies will not do much to deal with myriad problems that are emerging in this domain. The various critical sectors are the backbone of Indian economy, without proper cyber security implication, it will create and open feast for cyber attackers. India trajectory to digital economy is holistic process. There are sectors that support digital economy like energy, healthcare and financial. All these sectors are intertwined and interlinked together for functioning of the nation economy. Therefore, implementation of pervasive pragmatic polices are needed in cyber realm, fostering better economic development without hindrances.

References

[1] Chakrabarty, Pradip. , n.d. Digital India cannot do much without the protective wall of cyber security, Higher education review.
[2] Banerjee, Sohini; Menon, KS Roshan. 2021. Why it is important to build cyber-resilience for finiancial entities in India. Financial Expres. URL https://www.financialexpress.com/brandwagon/writers-alley/why-it-is-important-to-build-cyber-resilience-for-financial-entites-in-India/2274549/lite/
[3] Reddy, Lokhanadha. Bhargavi, v., 2018. Cyber security attacks in the banking sector emerging security challenges and threats. International association of scientific innovation and research. ISBN (online) 2328-3696.p65.
[4] Parid, Ankit. 2021. What is critical information infrastructure: for dummies. MY LAWRD. https://www.mylawrd.com/what-is-critical-information-infrastructure-for-dummies
[5] Journals of India. Nine pillars Digital India mission. URL https://journalsofindia.com/nine-pillars-digital-india-mission. (Accessed 30-08.21)
[6] Natarajan, (vol 52, no 4). (December 2005). Cyberinfrastructure: an opportunity for education and implication for research libraries. p.148. Retrieved from http://nopr.niscair.res.in
[7] Deloitte. 2020. Cyber security the Indian banking industry: part 1 will 2020 redefine the cyber security ecosystem. Pp.05-08. URL https://www2.deloitte.com/content/dam/Deloitte/in/Document/risk/in-ra-cybersecurity-in-the-indian-banking-industry-noexp.pdf Accessed on 03-08.2021
[8] Sharma, Manish. 2017. Securing critical information infrastructure new. Institute for defence studies and analyses, New Delhi.p.26.
[9] DSCI. 2020. National cyber security strategy 2020. URL https://www.dsci.in/sites/default/files/document/resource_centre/National%20cyber%20security%20strategy%202020%20DSCI%20submission.pdf. (Accessed on 3-08.2021).
[10] ET online. 2017. Critical infrastructure on target: A cyber attack that could be worse than war. The economic times. URL https://m.economictimes.com/tech/internet/critical-infrastructure-on-target-a-cyber-attack-that-could-be-worse-than-war/articleshow/61508816.cmsAccessed on 1-08.2021.
[11] PTI. 2018. Cosmos bank's server hacked; RS 94 corer siphoned off in 2 days. The economic times. URL https://m.economic.com/industry/banking/finance/banking/cosmos-banks-server-hacked-rs-94-crore-siphoned-off-in-2-days/amp_articleshow/6539947.cms
[12] Banister, Adam. 2019. France and India strengthen ties through cybersecurity cooperation agreement. The daily swig, cyber security news and views. URL https://portswigger.net/daily-swig/amp/france-and-india-strengthen-ties-through-cybersecurity-cooperation-

agreement#aoh=16273777777852&referrer=https%3A%2F%2Fwww.google.com&amp_tf=From%20%251%24s. Accessed on 04-08.2021.
[13] NDTV. 2020. ASEAN-India summit focuses on cyber security during covid pandemic. URL https://www.ndtv.com/india-news/asean-india-summit-focuses-on-cyber-security-during-covid-19-pandemic-2309502
[14] Agarwal, Shubhangi. 2021. Cyber security in India. Retrieved from LEXOLOGY.
[15] Stewart et.al. 2010. What is cyberinfrastructure. SIGUCCS. Virginia
[16] Shukla, Manish. 2019. 158 govt websites hacked in last two years. DNA. URL https://www.dnaindia.com/india/report-158-govt-website-hacked-in-last-two-years-it-ministry-in-rajya-sabha-2803582. Accessed on 03-07.2021.
[17] Dilipraj, E. 2015. "Cyber security challenges for India: An assessment of its preparedness". Defence and Diplomacy journal, vol.4 no.4. p93.
[18] SKYBOX security .2016. Solution to protection critical information infrastructure in India. URL https://lp.skyboxsecurity.com/rs/skyboxsecurity/images/skybox_Brouche_integrated_business_managment.pdf . accessed on 03-09.2021.
[19] Heywood, Andrew. 2011. Global politics. PALGRAVE MACMILLAN, ISBN 978-1-4039-8982-6. P-138
[20] Pratt, Marry. 2021. Cyber-attack, tech target. URL https://searchsecurity.techtarget.com/definition/cyber-attack . Accessed on 05-09.2021
[21] Chakraborty, Pardip. 2020. Digital India initiative could raise GDP to $1 trillion by 2025, Dataquest.
[22] Devi, Sushma. 2019. Cybersecurity in the national security discourse. Kapur Surya foundation. P149 Retrieved from https://www.jstor.org/stable/102307/48531107 .
[23] ET Bureau. 2017. India, US renew agreement for cyber security coordination. The economic times. URL https://m.economictimes.com/news/defence/india-us-renew-agreement-for-cyber-security-coordination/articlesshow/5648102.cms
[24] Seema et al. 2018. "Overview of cyber security". International journal of advanced research in computer and communication engineering, vol 7, issue/1. P-125
[25] Chakrabarty, Pradip. , n.d. Digital India cannot do much without the protective wall of cyber security, Higher education review.
[26] Kumar, Sajeev. 2021. Seen more data breach case, financial travel from online platform in India: study. The Hindu, Chennai.
[27] Chakrabarty, Pradip. , n.d. Digital India cannot do much without the protective wall of cyber security, Higher education review.
[28] Kumar, Sajeev. 2021. Seen more data breach case, financial travel from online platform in India: study. The Hindu, Chennai.
[29] NISG. 2012. E-governance project life cycle. National institute for smart government, www.nisg.org . p-16.