Indo American Journal of Multidisciplinary Research and Review (IAJMRR)
ISSN: 2581 - 6292 / Impact Factor: 6.885 / Website: www.iajmrr.com

DEEP LEARNING FOR SECURITY OPERATION CENTERS: LEGAL PERSPECTIVE

Dr. Arti
Assistant Professor, Faculty of Legal Studies, University Institute of Law, Desh Bhagat University, Mandi Gobindgarh, Punjab

Cite This Article: Dr. Arti, "Deep Learning for Security Operation Centers: Legal Perspective", Indo American Journal of Multidisciplinary Research and Review, Volume 5, Issue 1, Page Number 25-30, 2021.

Copy Right: © IAJMRR Publication, 2021 (All Rights Reserved). This is an Open Access Article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract:

Cyber security knowledge is very significant for dealing with a good digital society. New technology has played a greater role in building Artificial Intelligence rather than increased a lot of the problems concerning data security. It is a big challenge before the digital world i.e. Fraud automation, the Internet of Things, cross channel fraud, etc., and what ethics should be carryon and adopted by the new digital era. The paper is focus to analyze deep learning techniques of cyber security and find out what the legal effort has been held by the domestic government. We all know all things are prevailing and working well being in the society on the ground rule and regulation as a norms etc. During & after the Pandemic, it is very needed to stimulate focus, thinking, and search for strong cyber security in the country so utilized data for the welfare of the state and generates new ability, education system, good governance, and evolutes friendly ecosystem in National and International Level. The method of the study is a non-empirical used literature review, data from the ministry of the government of India, and other legal documents. The results are cyber security is dependent on the deep and active role of security operation centers as well as the deep learning of the public at large themselves. The legal effort is played a crucial role in the development of the norms of deep learning regarding cyber security and Artificial Intelligence technology.

Key Words: Cyber Security, Ethics for Artificial Intelligence, Deep Learning & Self-Learning, Legal Framework, Cyber Security Education

Introduction:

Anyone when discusses the term cyber is already connected with some words security, risk, vulnerabilities, exploits, encroachment, offensive, or war. Indeed, it is a concern with the unconfident areas and unfriendly[1]. Cyber security is indicating national security and a burning phenomenon in the digital era. The Securities and Exchange Commission recognizes that cybercrime is currently the fastest rising economic crime, in line with the findings under the national security policy for 2017-2022.[2]Data learning are including many aspects of correlated knowledge of digital or internet. The Philippines government has estimated Super Vision 2025 regarding Cyber security and data breach and framework on Cyber security of regulation entities issues[3]. How the need for deep learning for security operation centers is a very attractive question, it is concerning to basic principles of transparency, security, responsibility, protection of intellectual property which is a cornerstone in good governance and democratic society. Transparency theory is also demanded Cyber security basis of data effectiveness and standards of the governance. Trust in aviation Cyber security will only come with increased transparency. It depends on the contract and system design. The essence of Responsibility is also talked about technology is a very power itself without responsibility it's going the wrong way. As an analogy, in the finance arena, users rely on banks and other financial institutions to be responsible for key aspects of their monetary transactions, including payments lending, and savings though, of course, users have their responsibilities as part of the system[4].

Theory of Security is also supported government should be firstly worked on security of all aspect of the people including cybercrime against him. According to Larry Hanauer Cyber security is very needed for the deep growth of the nation and enhances strong relationships between partners. It also enhances the nation's abilities to address shared threats and to operate more effectively with U.S.A and regional counterparts[5]. So regional centers are played a crucial role and impart fundamental national security analysis skills. It is a significant part of the deep learning for security operation centers. Before 3 years only 41 percent of leaders are expended more than 20 percent of their Cyber security budgets on advanced technologies. Today, spending finance on Cyber security 82 percent[6] for the technologies.

Protection of Intellectual Property is a fundamental right of every citizen of the country. Infringement of Copyright is against the freedom of speech and expression and it is also affected the ability

[1] Heather M. Roff, Cyber Peace: Cyber security Through the Lens of Positive Peace, New America (2016) p.2.

[2] Guidance For Regulated Entities on Establishing and Maintaining A Cyber security Framework, Securities and Exchange Commission, Philippines, (15 December 2020).

[3] Super Vision 2025, available at:https://www.sec.gov.ph/about-us/plans-and-programs/supervision-2025/(last visited on 24/12/2020,11:43AM).

[4] Frankin D. Kramer &Robert J. Butler, Cyber Security: Changing the Model, Atlantic Council (2019) pp 1-21, available at: https://www.jstor.org/stable/resrep20932.2 (last visited on 20/12/2020, 06:54PM).

[5] Larry Hanauer, Stuart E. Johnson, Christopher J. Springer, Chaoling Feng, Michael J. McNerney, Stephanie Pezard and Shira Efron, Evaluating the Impact of the Department of Defense Regional Centers for Security Studies, RAND Corporation(2013) pp 79-108.

[6] Kelly Bissell, Ryan M. Lasalle, Paolo Dal Cin,Third Annual State Of Cyber Resilience, Innovate for Cyber Resilience, Lessons from Leaders to Master Cyber security Execution, Accenture (2020).

of experts and researchers. So Cyber security is fundamental for the development of educational research. The internal challenges before Cyber security are international affairs, national security and defense, criminal law, civil liability, data protection, privacy, and personal responsibility.

The theory of Responsibility is a very valuable aspect of Cyber security. The operation centers are also responsible for data security. So deep learning is very important for them. Next, the greatest challenge of developing a comprehensive Cyber security governance framework on a national level is a highly complex problem, pervasive and interrelated across many aspects of government, the private sector, and society[7].

In the context, the International Civil Aviation Organization (ICAO) 1944 has a greater witness to core agreement and civilian steps regarding political and technical in the context network of passenger and freight carriage[8]. It is significant to understand the development of bringing coherence to global aviation Cyber security cannot be underestimated[9]. Department of Homeland Security and the Federal Bureau of Investigation has also announced Cyber security is a very key point for the good governance of dealing with technology. Cyber security is complex, and it requires expert engagement[10]. At present time, critical elements of the effective coordinated partnership include the development of advanced technology and the use of effective operational approaches including cloud technology, automation, and Artificial Intelligence[11], it is indicated rethink and focused deep learning about the security system on cyberspace.

Literature Review:

Deep learning is a very discussing phenomenon at present time for the effective and responsible aspect in Artificial Intelligence as well as invited open-world learning which is appreciated research, security, and progress of the technology. In the paper named open-world Learning for radically autonomous agents, Pat Langley has said open-world learning is essential for autonomous systems (Artificial Intelligence /Digital system) to overcome outmoded expertise in changing environments[12]. No doubts Open-world learning invites new challenges to the Artificial Intelligence society but also holds great promise. It encourages researchers to develop systems that can identify when their expertise is inadequate, identify the flaws responsible for Artificial Intelligence and operation centers[13].

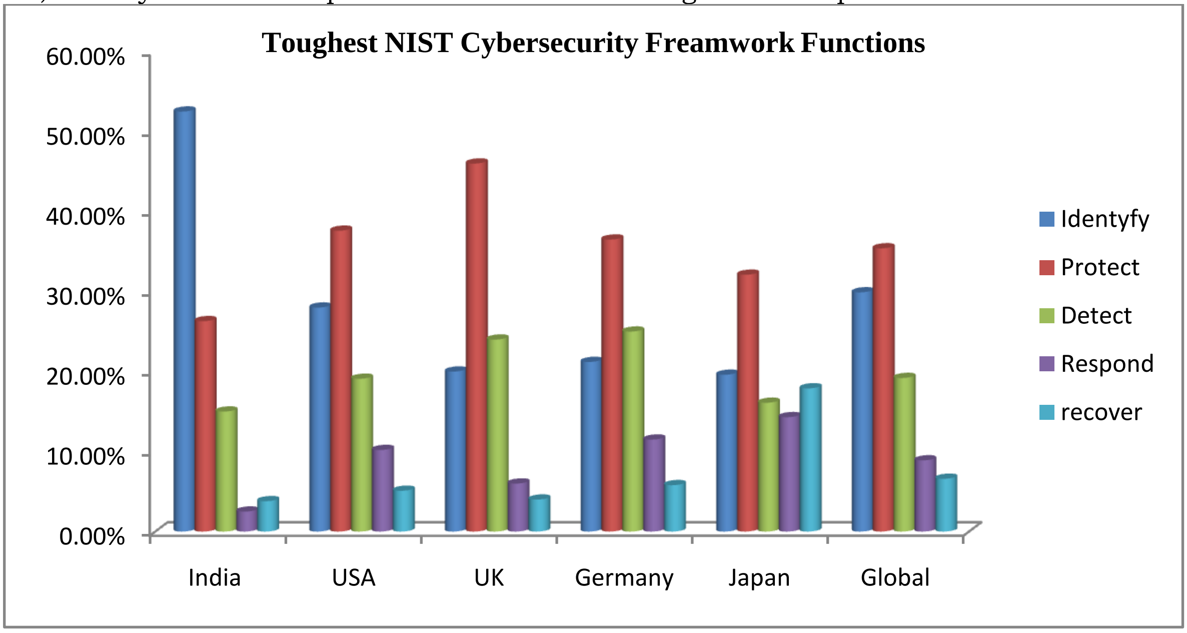

Chart I: Toughest Challenge for IT security operations by NIST Cyber security Framework

The Report of Center for Cyber and Homeland Security, the George Washington University has appreciated deep-learning neural networks are worked very well and a larger commercial anti-virus firm bought the company because they understood that innovation and managing in machine learning is critical to combating current and future threats[14]. The literature is indicating deep learning for security operation centers, Artificial Intelligence, and technology is very well and effective for the future generation. Technology is reaching the whole sector of society, without deep learning we cannot making responsible Artificial Intelligence. Deep learning can start new boosting power to deal with Artificial Intelligence and increase employment. Micro Focus cyber edge Group has realized report on 2020 State of Security

[7] Carrie Cordero and David Thaw, Rebooting Congressional Cyber security Oversight, Center for a New American Security (2020) 1-6, available at: https://www.jstor.org/stable/resrep27475(last visited 20/12/2020, 08:22PM).

[8] The History of ICAO and the Chicago Convention, available at: https://www.icao.int/about-icao/History/Pages/default.aspx (last visited on 20/12/2020, 07:16 PM).

[9] Pete Cooper, Simon Handler and Safa Shahwan, Aviation Cyber security: Scoping the Challenge, Atlantic Council (2019)pp V-VII.

[10] Ibid.

[11] Ibid.

[12] Pat Langley, Open-World Learning for Radically Autonomous Agents, Institute for Defense Analyses, (2019),p.10.

[13] Ibid.

[14] Michael Brett, George Duchak, Anup Ghosh, Kristin Sharp, Frank J. Cilluffo and Sharon L. Cardash , Artificial Intelligence for Cyber security: Technological and Ethical Implications Issue Brief Series on Trends in Technology and Digital Security, Center for Cyber and Homeland Security at Auburn University (2017),pp.8-12.

Operations[15] and mentioned maximum 90% of organizations have shortages in their security operations staffing shortage 98% and the education system have shortage100%. The report has explained NIST and the Cyber security framework has defined five activities the organization can perform to manage their Cyber security risk. They are Identify, protect, detect, respond, and recover. The report has also given percentage criteria fulfill the USA, India, UK, Germany, Japan, and Global and mentioned below Chart I.

It is also mentioned many challenges facing by the IT security operation team like investigating or validating security incidents, monitoring security across a growing attack surface, taking advantage of Cyber security by threat intelligence, lacking skilled security operation personnel, having too many unintegrated point solutions[16]. All challenges are attracting a deep learning process for security operation centers. We all know that IT is a basic part internet of things infrastructure and implemented by the Security Operation Centers[17].

Another thing focused by the 2020 State of Security Operations is skill needs to staffing in IT sector about the attack detection and analysis, incident response, security awareness training, vulnerability assessment, and patching, compliance reporting, etc. it is contributing to resolved problems regarding Cyber security[18]. At present time, enhancing the development of technology is in many fields tremendously for example health care, technology, government, telecom, manufacturing, finance, education, and retail. It is an increased deep learning system for the mange of Artificial Intelligence.

Moore's law is significant to understand the recent success of Artificial Intelligence techniques such as deep learning and deep neural networks is attributed to the improved performance of algorithms thanks to the increase in computing power[19].

Cyber Security: Deep Learning & Self Learning

Deep learning and self-learning are promoted self ability about data protection and facilitate the development, promotion, administration, and maintenance of application systems[20]. Deep learning provides knowledge and awareness regarding managing accessibility, the integrity of the communication system, and data and records of electronic mechanisms. In 2018 the National Institute of Standards and Technology has appreciated self-assessing Cyber security risk with the framework and to explain how the Framework can be used by organizations to understand and assess their Cyber security risk, including the use of measurements[21]. It is recommended all organizations and institutions should be thoughtful, creative, and careful about data security measurements to advance use, and ignoring fake artificial indicators, and progress in improving Cyber security risk management[22]. The self–learning and self-awareness of Cyber security tool is helpful for the users to safe yourself and data security.

Need to deep learning about Sentry MBA or SNIPR is a cracking technology which is aware to users for the criminals who are takeover account. It is very significant to knowledge about it at present for dealing with legitimate business activities; automation makes it possible to do a lot, a lot more quickly. Want to verify thousands of stolen usernames and passwords in minutes? Use an automated account checking tool[23]. Vertex and open bullet are also cracking tools which are used by the cybercriminals to hacking account.

The everyday life, Internet of things devices have become a significant part and more cyber criminals are going to find ways to exploit them. So need to deep learning about the device, hardware, and software driving system and helping to prevent fraud. Cyber security today is serious business. Nations compete for dominance, and Cyber security is looking a lot more like warfare, and business as usual is simply insufficient[24]. The Center for Internet Security has given Top 20 Controls and the National Institution of Standards and Technology Cyber security Framework is a very effective means to help construct defenses against the most common 80% of threats[25]. But it is not sufficient for Cyber security and Artificial Intelligence also needs awareness & deep learning of technology.

Cyber security education is helping to deep learning about the internet, websites, and software. In 2016 Center for Cyber and Homeland Security has recommended Cyber security courses should be appreciated within all undergraduate criminal justice programs, and specialized master's programs should be increased for cyber investigation and forensics[26]. It has also recommended the state and local governments should be working on Cyber security education.

[15] 2020 State of Security Operations, A Survey of International IT Security Operations Professionals on the Challenges they face and the best Practices and Technologies they Embrace to Meet these Challenges, A cyberedge Research Study Sponsored by Micro Focus (October, 2020) p.12.

[16] Id. at 11.

[17] Natalia Miloslavskaya, Security Operations Centers for Information Security Incident Management, Conference Paper on 4th International Conference Future Internet of Things and Cloud, Vienna (Austria,2016).

[18] Supra 15.

[19] Shashi Shekhar Vempati, India and The Artificial Intelligence Revolution, Carnegie Endowment for International Peace (2016) p. 21.

[20] Super Vision 2025, Securities and Exchange Commission, Philippines, available at:https://www.sec.gov.ph/about-us/plans-and-programs/supervision-2025/(last visited on 24/12/2020,12:35PM).

[21] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cyber security,(2018) available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf(last visited on 24/12/2020, 12:55PM).

[22] Ibid.

[23] Current State of Cybercrime (2019), available at: https://www.rsa.com/content/dam/en/white-paper/2019-current-state-of-cybercrime.pdf (last visited on 19/12/2020, 11:59PM).

[24] Gregory Conti and Robert Fanelli, How Could They Not: Thinking Like a State Cyber Threat Actor, Vol. 4, No. 2, The Cyber Defense Review , Army Cyber Institute (2019), pp. 49-64.

[25] Ibid.

[26] Center for Cyber and Homeland Security, The George Washington University, Cyber security for State and Local Law Enforcement:: A Policy Roadmap to Enhance Capabilities, Auburn University (2016) pp 1-7.

Deep learning is started with machine learning it is similar to neural net learning means procedures for representing inputs (data points) as loads on net-input layer nodes[27]. Keith A. Roberts has said deep learning and surface learning respectively[28]. Deep learning is to provide a platform to solved unwanted problems concerning the net. Giles Hooker, Cliff Hooker has clearly said machine learning provides all the authentic input-output relationship. Deep learning is also concerned with new directions for dealing with computer activities and operation centers.

Deep Learning in Artificial Intelligence: Ethics & Resilience:

At present all sectors are dealing with Artificial Intelligence and Cyber security has become a top concern for central banks, ministries of finance, and other financial supervisory authorities[29]. In the context ethical behavior are very significant to make potential the cyberspace and workplace of Artificial Intelligence. It is needed to operate on trust, ethics, and in a unique environment. For security, it provides unique career development opportunities and motivation to work ethically and learned the value of Artificial Intelligence in the life of data security. Ethical theory is also concerned promotion and development of the person so effective Cyber security should be considered the promotion and development opportunities to employees[30].

For effective Cyber security should be considering a few key points of the operation center's career path planning, upskilling, public-private partnerships, hiring requirement exemptions, work-based learning, rotational programs, etc. It is appreciating to the development of ethical behaviors of the employers as well as increases the employment in the field of cyberspace. Lyndon Nelson was rightly said a regulator is little more than its staff. The recruitment, development, and retention of the staff must be the number one priority[31]. He was also a supported specialist of the operation centers who enjoyed learning from each other. Internet society is also demanding the code of conduct of the user and operation centers that can talk about Cyber security in the society.

Legislative Effort in Democratic Countries:

From 2017 to 2019 cyber attacks are increasing 138, 232, and 280 till 2019 in the business ecosystem mentioned Chart II[32].

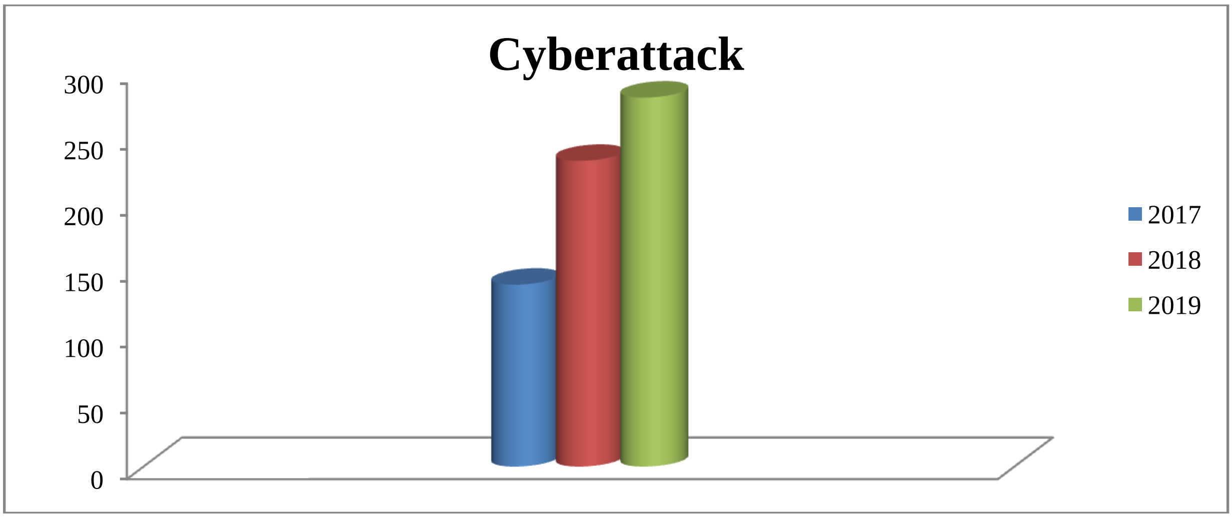

Chart II: Cyber attacks (2017-2019)

It is a very serious phenomenon or problem and challenges for the good governance of the IT sector as well as the corporate sector. Legal effort can be made an effective tool to control cybercrime and reduce hacking, exploiting data, unauthentic interruption, fake information, etc. the Artificial Intelligence has needed positive role of everyone including the legal system, government, and public. Passive and active countermeasures can then mitigate and defeat threats. In some cases, intruders can be sent to honey pots (false data) while then activating cybercrime law enforcement or cyber-warfare countermeasures[33].

All democratic countries have passed legislation Security operation centers can be functioning peacefully which is promoting the deep learning process also. In 2019, the USA framed around five principles directs implementing agencies to prioritize sustained investment in Artificial Intelligence R&D including EO prioritizes artificial intelligent education and workforce development to train the next generation of Artificial Intelligence researchers. The National Security Commission was set up by the USA government it is an independent body to review advances in Artificial Intelligence, deep learning for security operation centers, machine learning developments, and associated technologies to mainly

[27] Giles Hooker, Cliff Hooker, Machine Learning and the Future of Realism, Spontaneous Generations: A Journal for the History and Philosophy of Science, Vol. 9, No. 1 (2018) 174-182.

[28] Keith A. Roberts, Imagine Deep Learning *Michigan Sociological Review*, Vol. 25 (2011), pp. 1-18.

[29] Tim Maurer and Arthur Nelson, International Strategy to Better Protect the Financial System Against Cyber Threats, Priority #4: Cyber security Workforce Challenges, Carnegie Endowment for International Peace, (2020),pp 11-125.

[30] Id. at 118.

[31] Id. at121.

[32] Kelly Bissell, Ryan M. Lasalle, Paolo Dal Cin,Third Annual State of Cyber Resilience, Innovate for Cyber Resilience, Lessons from Leaders to Master Cyber security Execution, Accenture (2020) p 10.

[33] Eric G. Troup, Growing Role of Platforms in Cyber security, The Cyber Defense Review, Vol. 2, No. 1 (Winter, 2017), pp. 61-70.

concerned the national security and defense[34]. The commission has also focused on many areas regarding Cyber security and Artificial Intelligence like international cooperation in Artificial Intelligence attract leading talent in Artificial Intelligence, ethical considerations in the technology era, establishing data standards, etc.

Joint Artificial Intelligent Center has constituted by the USA Department of Defense in 2018 for the development and research of Artificial intelligence as well as work on accelerating, delivery, and adoption of capacities of Artificial Intelligence and machine learning. In the Financial Year 2020 budget, the Joint Artificial Intelligence Center has received approximately $208 million in funding, for the development of learning ability regarding security operation centers[35]. In America, the Defense Innovation Board has supervised the importance of maintaining the benefit of the internet and technology in Artificial Intelligence. It is also ensuring these technologies are developed and used ethically and safely. Ethics is promoted self-resilience to a member of operation centers.

The next significant setup has been taken by the USA government about the deep learning for the security operation centers and Artificial Intelligence to constitute DARPA. Defense Advanced Research Projects Agency has a fund agency its area of functioning to accrediting software systems for operational deployment; build up the security and resiliency of machine learning, awareness of new technologies; enhancing the robustness and reliability of Artificial Intelligence techniques and reducing power, data, and performance inefficiencies. It is a very grater point to the motivation of deep learning in the field of security operation centers[36].

The American government has passed the Export Control Reform Act to maintain the foundational security of the technologies. The USA Department of Commerce Expert Controls for Artificial Intelligence is the best example of controlled unwanted technology disputes. It is focused on commerce control-related Artificial Intelligence. These steps are indicated the US government understands technology sensitization in the commercial sector which is the backbone of economic development. Nowadays digital platform is concerned to the representative technology category and very important and essential to the national security in America. So deep learning, machine learning, self-resilience about technologies, and computer visions have made an essential part of the legal system, economic system, scientific development as well as social growth[37].

One of the most important schemes has played an active role to manage and control unauthorized activities in Artificial Intelligence in America. It is known as the Office of Science and Technology Policy. It is organized many Artificial Intelligence projects and technology learning initiatives. It is also co-leading & managing the Networking and Information Technology Research and Development Program which concerned research related to machine learning and deep learning. The policy is also concern with the National Science and Technology Council which is promoted and working on Artificial Intelligence Research and Development Strategic Plan including deep learning for security operation centers. It is also promoted international discussions on Artificial Intelligence like the OECD and G20 Ministerial and delegates G7[38].

The United Kingdom is a developed and democratic country. In 2019 the UK has third-ranked to leading technology in Artificial Intelligence and policy with America and China. The legislative effort about Artificial Intelligence in the UK has passed the Data Protection Act, 2018. The Act has adopted the fair and lawful principle and regulates storage data, use of personal data, and collection of personal data. Sections 28, 29, and 36of the Act provides exceptions for personal data. Chief Information Security Officer is played a greater role to manage information assets and protected technology and having a lot of the responsibility for identifying, managing, and developing information technology and reducing risk regarding it. Centre for Data Ethics and Innovation has been set up by the UK for the industrial strategy and ensures ethical, safe, and innovative use of data, balancing privacy, and public benefit including Artificial Intelligence[39].

Indian Cybercrime Coordination Centre (14C) is fighting against cybercrime at the national level. It provides a program concerning cybercrime volunteers to bring together citizens to serve and contribute to the fight against cybercrime in the country[40]. National Cybercrime Reporting Portal of India also functions on cyber awareness for example financial fraud, job fraud, matrimonial fraud, safe use of social media platforms, identity theft, mobile application frauds, etc. it also provides a helpline number 155260, web portal www.reportphishing.in, advisories CERT-IN on https://www.cert-in.org.in for Cyber security[41]. In India, deep thinking about data security is started by the government after the Right to privacy case known as *Justice K.S. Puttaswamy (Retd.) v. Union of India*[42]. In *Justice K.S. Puttaswamy (Retd.) v. Union of*

[34] Martijn Rasser, Megan Lamberth, Ainikki Riikonen, Chelsea Guo, Michael Horowitz and Paul Scharre, The American AI Century: A Blueprint for Action, Center for a New American Security, (2019), p.38.

[35] Id.at 39.

[36] Ibid.

[37] Id.at 40.

[38] Ibid.

[39] AI, Machine Learning & Big Data 2020 United Kingdom, Global Legal Insights, available at: https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/united-kingdom(last visited on30/12/2020, 06:20PM).

[40] National Cybercrime Reporting Portal, available at: https://cybercrime.gov.in/Webform/cyber_volunteers_concept.aspx(last visited on 28/12/2020,4:46PM).

[41] Ibid.

[42] 2017 (10) SCALE 1.

India[43] the Apex Court has held that to make the right to privacy, it is the duty of the state to formulation a data protection framework which, while protecting citizens from dangers to informational privacy originating from state and non-state actors, serves the common good. It is this understanding of the state's duty that the Committee must work with while creating a data protection framework. The Indian government has announced NISPG, NATGRID, and Cybercrime Prevention against Women and Children Schemes for the prevention of cybercrime and promoted Cyber security. Artificial Intelligence technology has huge potential to outline economic system and national security future. India is followed by developed country's standards of technology and concerned deep learning process for security operation centers.

Concluding Result & Suggestions:

The result is Cyber security is a big challenge before our society and deep learning for the operation centers have a very helping tool to a resolved problem regarding misuse of personal data as well as institutional data. The author suggests that the first requirement to make regulations and standards of the institutions they have demonstrated knowledge regarding technology, mechanism, software, etc. the Communications Information sharing body should be trustable and responsible. People should be also aware of websites, Cyber security, and fake software. The government has considered effective Cyber security tools and building bridges of deep learning for operation centers. It should be also focused on Safety, security, enterprise, and finance Cyber security in the country. Most of the things about deep learning should be increasing transparency and trust in Artificial Intelligence. It should provide exposure in the job, responsibility for authority about a broad range of technical issues, and communication of true information in the society. Cyber security education should be started within a higher secondary school. Cyber society should be decorated with honesty, trust, transparency, and responsibility like human activities.

Acknowledgment:

I thank Aasha Devi for her appreciation and help to write the chapter and Jstor websites, Indian digital Library, Ministry of Home affairs are contributed.

[43] 2017 (10) SCALE 1.