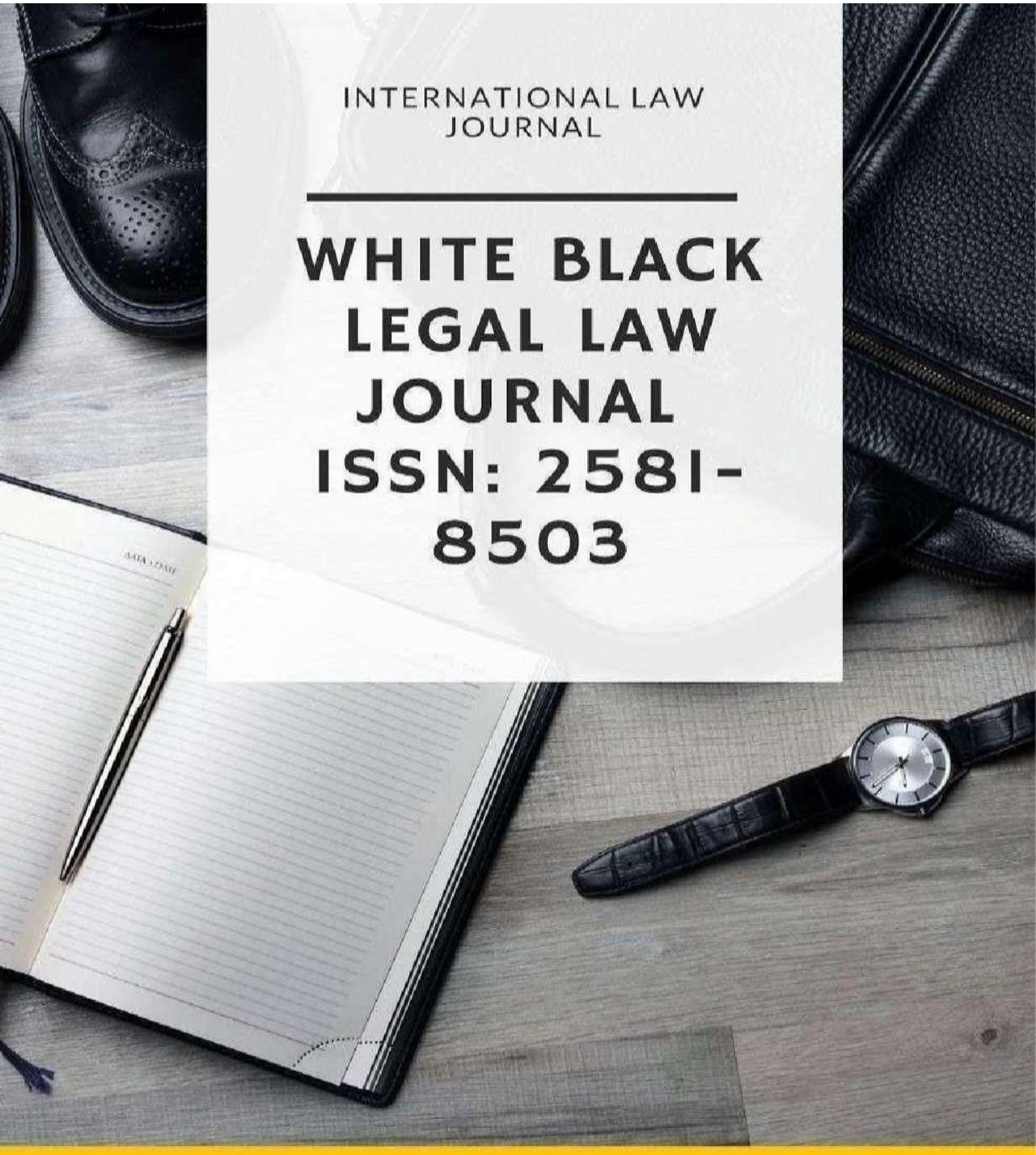

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

AI AND CYBER SECURITY: A TECHNO- LEGAL APPROACH

AUTHORED BY - DR. RAJU NARAYANA SWAMY IAS

The digitalisation of almost every area of society has changed the rules of our economy. Cloudification, IoT and BYOD (Bring Your Own Device to Work) are all giving rise to micro environments that contain a lot of sensitive data. If these devices fall into wrong hands, it could certainly lead to grave consequences. To put it a bit differently, cyber security - the technology, process and practice to protect networks, devices, programs and data from attacks, damages or unauthorized access - will not only become a crucial issue for the safety of our new digital critical systems, but it will also be a prerequisite for creating trust in our digital economy. The situation is further alarming when one considers the newer types of attacks, which are mostly machine engineered. Thus cyber security which was a war among humans has changed to a battle of human versus machine. In fact the old protection mechanism which was largely a "seal the borders" approach via firewalls, proxies, antivirus software, access controls and dynamic passwords is today grossly inadequate. A new approach is required to continuously monitor the large number of factors and detect what constitutes abnormal activity. This could be similar to our body's immune system where the white cells and antibodies are continuously scanning and neutralizing any organism that does not fit the normal functioning patterns within the body. This is where AI comes into play. It needs to be reiterated here that AI works in three ways - assisted intelligence, augmented intelligence and autonomous intelligence.

The primary targets for AI application in cyber security are network intrusion detection, malware analysis and classification, phishing and spam emails. Machine learning (ML) algorithms can recognize potential security breaches or attacks by continuously observing what is an abnormal behavior and given the authority, they can automatically shut down systems under perceived threat. In fact ML can revolutionize the way cyber security has been handled to date - whether it be in detection, protection, prediction or termination. There are broadly two categories of possible uses:-

a. Apply supervised learning to the massive amount of historical data to continuously

improve prediction capabilities.

b. Apply unsupervised learning to make some sense out of the massive amount of data through clustering and dimensionality reduction techniques.

As regards the former, the most talked about cases in the context of cyber security are malware classification and spam detection. In Gmail for example, the supervised machine learning algorithm scans countless variables such as the originating IP address and phrases in the email content to determine whether the email conforms to an abnormal pattern and then pushes it out of your inbox folder into the junk folder.

As regards the latter, context and expert knowledge base are two critical aspects to make sense out of raw data. For instance, rather than looking at network traffic logs in isolation, we need to add context to make sense of the data such as whether the device is supposed to respond to DNS queries. If it is a DNS server, then this is absolutely a normal behavior, but if it is not, the behavior could be the sign of an attack.

However, there is a hitch – machine learning lacks the general knowledge required to distinguish real threats leading to too many false alarms. A potential solution could be a hybrid human-machine collaborative approach such as the AI2 cyber security platform from MIT's Computer Science and Artificial Intelligence Lab. Here human experts handle the judgment related tasks of validating and classifying the threats and associating severity tags.

A major challenge here lies in defining what is not an anomaly. For example, starting from reading the morning news online to shopping to travel booking to carry our work-related activities, we use our laptopsin many different ways. There could also be infrequent patterns such as downloading a game or organising pictures from a vacation. In essence, the most potent security threats are not just statistical outliers.

Most cyber attacks follow certain attack phases that can be described as a cyber kill chain. Every attack sequence starts with a reconnaissance phase (in which an attacker tries to locate gaps and vulnerabilities of a target system). The weaponizing phase follows. This is followed by the

delivery phase when the malware is transferred to the potential target. After the malware is delivered successfully, the exploit phase occurs during which the malware triggers the installation of an intruder's code. Aim of ISA (Integrated Security Approach) is to generate early warnings before the exploit phase.

ANNs (Artificial Neural Networks: statistical learning models imitating the structure and function of the human brain) have been used successfully within all stages of ISAs. ANNs can be used to learn from past network activities and attacks in order to prevent future attacks from actually transpiring. DNNs (Deep Neural Networks: a more elaborate and computationally expensive form of ANNs) have been used not only to protect organizations from cyber attacks, but also to predict these attacks.

It must not be forgotten that machine learning is no silver bullet. Just as businesses are beginning to adopt AI systems, attackers are aslo finding ways to manipulate the same AI systems. They are focusing on finding ways to turn AI against its owners -from hacking chatbots to deliberately misleading pattern recognition algorithms. A classic example is Tay, a chat bot introduced by Microsoft to engage people through casual and playful conversation. Within 24 hours, a structured attack on Tay resulted in the bot shouting all sorts of misogynistic and racist comments.

To summarize, through AI powered cyber security is no panacea, AI will become a standard element of cyber security in the short term. But AI needs to deliver greater accuracy in detection and fewer false positives for it to earn the trust. A drawback of using AI within cyber security is the concern of data privacy. Moreover due to the unique and unforeseeable nature of AI, existing legal frameworks do not necessarily apply to this discipline. Cyber security being a back-and-forth game between attackers and defenders that will constantly evolve as technology grows, AI needs to be trained for all these varied scenarios. Attackers are already using AI to power their attacks – spear phishing tweets being classic instances – and we must deploy AI – driven defenses to keep up. As an example, the AI – driven defenses of tomorrow must be geared up to deal with the upcoming challenge of generative adversarial networks (GAN), a class of machine learning frameworks that can be used to generate deep fakes by swapping or manipulating faces or voices in an image or a video. In fact, offences on AI systems often appear in three areas – adversarial

inputs, poisoning training data and model extraction attacks.

The reality is that until now, AI alone has not proven overall success in cyber protection. Despite the great improvements that AI has brought to the realm of cyber security, related systems are not yet able to adjust fully and automatically to changes in their environment, learn all the threats and attack types and choose and autonomously apply dedicated countermeasures to protect against these attacks.

AI methods in Cyber security

Security function	DT	SVM	NB	K	HMM	GA	ANN	CNN	RNN	SNN
Intrusion detection	X	X	X	X	X	X	X	X	X	X
Malware detection	X	X	X	X	-	-	-	X	X	-
Vulnerability assessment	X	-	-	-	-	-	-	-	-	-
Spam filtering	-	-	X	-	-	-	-	-	-	-
Malware Classification	-	-	-	-	-	X	X	-	-	X
Phisting detection	-	-	-	-	-	-	X	-	-	-
Traffic Analysis	-	-	-	-	-	-	-	X	X	-

DT = Decision Tree; SVM = Support Vector machine

NB = Naive Baye's classifier

K= K- means clustering

HMM = Hidden Markov Model

GA = Genetic Algorithm (heuristic search algorithm employing the concept of genetics and natural selection)

ANN = Artificial Neural Network

CNN = Convolutional Neural Networks

RNN = Recurrent Neural Network

SNN = Siamese Neural Network

In the Indian context, the challenges are even more:

a. Large digital divide (Lack of digital literacy makes them vulnerable to phishing attacks and online scams)
b. Fragmented cyber security infrastructure: Responsibility for cyber security is distributed across various government agencies and private entities leading to a lack of coordination
c. Shortage of qualified cyber security professionals.

Needless to say cyber security is not only a technological issue, it is also about regulation and the way that security risks are dealt with. At the end of the day it is still the human factor that malters – not only the tools.