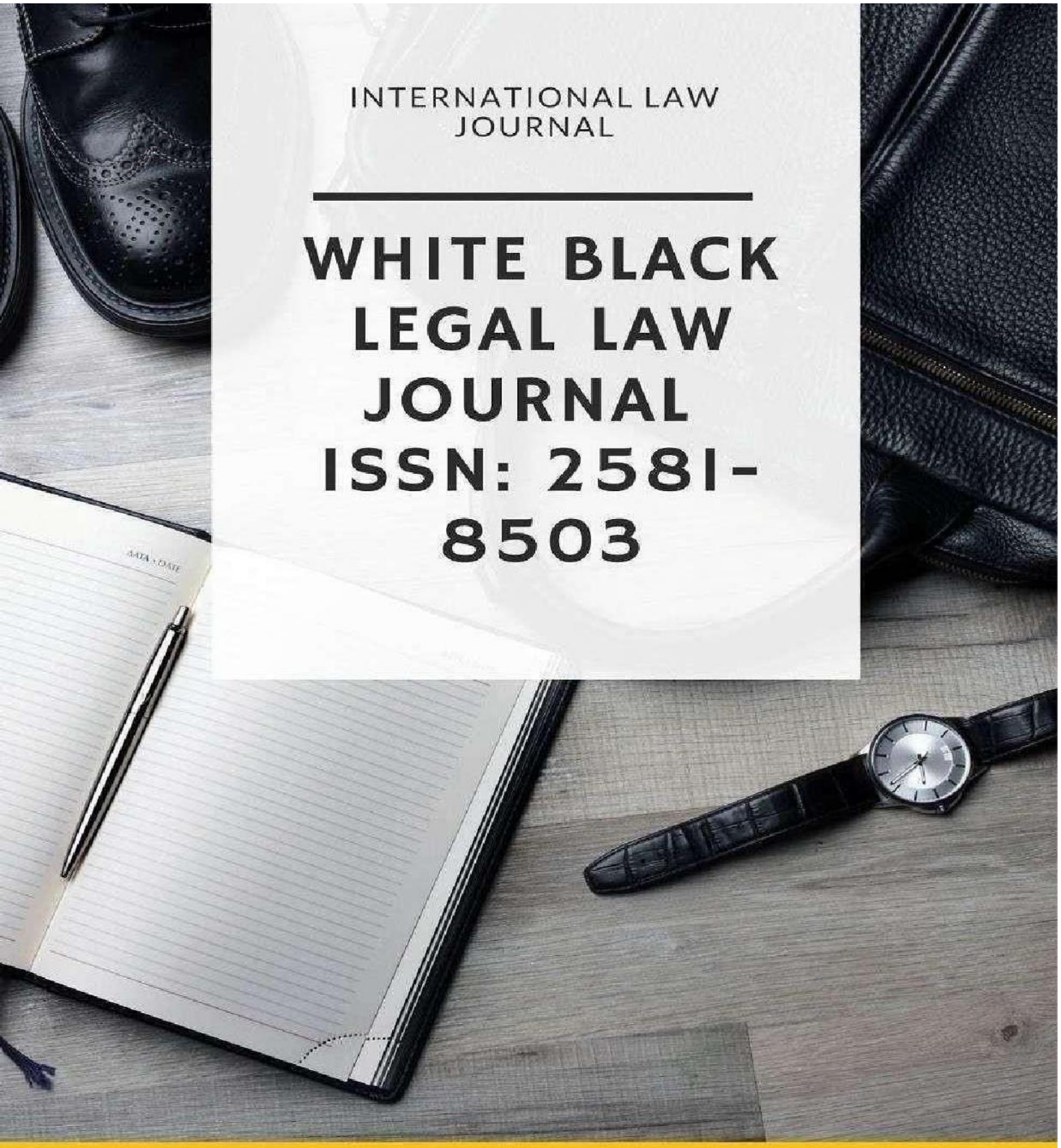


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

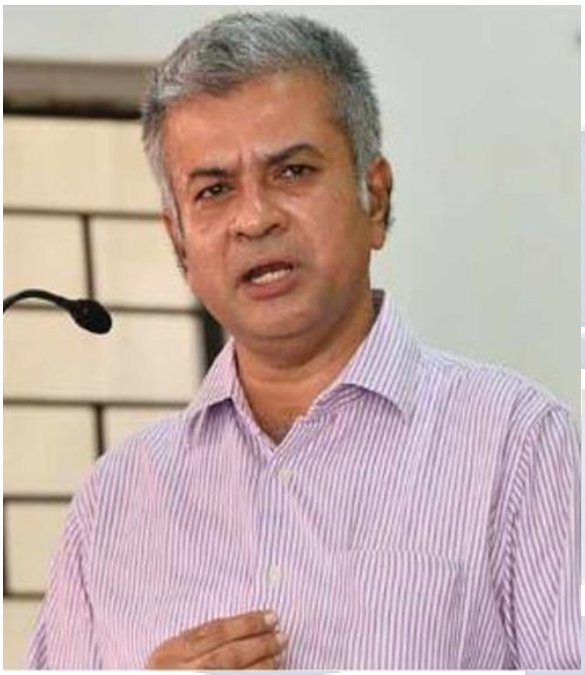
The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

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.

 ISSN: 2581-8503

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

www.whiteblacklegal.co.in
Volume 3 Issue 1 | Feb 2025 ISSN: 2581-8503

INTERNATIONAL CYBER LAW AND GOVERNANCE

AUTHORED BY - DR. KANIKA KESAR, Assistant Professor (Law)
SICMSS, Rashtriya Raksha University (Lavad) Gandhinagar, Gujarat

Abstract:

International cyber law and governance are increasingly indispensable in a society characterized by fast technological progress and pervasive presence of digital networks. This paper reviews the history of cyber law, which focuses on the urgent need for well -rounded institutions capable of capturing the complexities of cyberspace. In line with the development of legal norms and governance structures in relation to international cooperation with respect to cybersecurity, the situation grows urgent as complexity and sophistication build upon hacking, data breaches, and cyber warfare. The existing patchwork collection of national laws commonly results in jurisdictional conflict and impotency in addressing cross-border cyber incidents.

The following paper enumerates some of the major concerns of international cyber law. These are critical infrastructure protection, cybercrime regulation, and rights in privacy and data protection. The role of international organizations such as the United Nations and the Council of Europe will be discussed as having the capability to bring cooperation between nations together to formulate treaties to create a coherent approach towards cyber governance. Importantly, the discussion brings up issues that are relevant to developing countries and their need for capacity building, as well as public-private partnership.

The paper then discusses future challenges in artificial intelligence, blockchain technology, and the Internet of Things (IoT), the need to adapt legal responses, and innovative regulatory frameworks. This therefore requires an international posture that not only immediately addresses security concerns but endeavors to promote a stable digital environment with open doors for economic growth and innovation.

An analysis of these dimensions reveals the need for robust international cyber law and governance frameworks that can respond to the dynamic challenges of the digital age. This will enhance security at the global level and also protect the rights of the individual and establish

trust in digital transactions.

Keywords: International Cyber Law, Cyber Governance, Cybersecurity, Cybercrime, Data Protection, Critical Infrastructure, International Cooperation, Public-Private Partnerships, Emerging Technologies, Digital Right.

Today, the term "cyber" or "cyberspace" refers to everything related to computers, the Internet, websites, emails, networks, software, storage devices (like hard drives and USBs), and electronic devices such as cell phones and ATMs. In simple terms, cyber law is the "law that governs cyberspace." While cybercrime isn't specifically defined in law, the Information Technology Act outlines what constitutes a computer, computer network, data, and other key elements related to cybercrime. Cyber law is different from traditional laws that apply to physical nations; it includes various laws like computer law, internet law, and information technology law[1]. Cybercrime refers to the intentional misuse of information technology by cyber terrorists to cause harm to people or property. It often involves criminal activities where computers or networks are either tools used to commit crimes, targets of crimes, or locations where crimes take place. This type of crime doesn't respect national borders and can include traditional crimes facilitated by technology[2].

Cyber law encompasses the regulations governing online activities and environments. This domain includes a wide range of components, such as computers, networks, software, data storage mediums (like external drives and flash drives), the web, online platforms, emails, and electronic gadgets including smartphones and ATMs. Regulations are put in place by governments and must be adhered to by people in a jurisdiction or an area. Violations of regulations bring about various governmental penalties, which may be in the form of imprisonment, fines, or mandated restitution[3].

Cybercrime describes criminal activities that involve computers either as tools or as targets. The rise of e-commerce and other online digital business and transactions has led to a significant increase in these crimes. Electronic signatures serve as a means of digital document

[1] "What Is Cyber Security? Definition, Best Practices & Examples" (Fortra's Digital Guardian)<https://www.digitalguardian.com/blog/what-cyber-security>.
[2] JP Mishra, An Introduction to Cyber Laws (1nd Edition Reprint 2012, Central Law Publications).
[3] ibid.

authentication, with digital signature being a variant of the former. These signatures meet three important legal requirements: identifying the person signing, confirming the message's origin, and maintaining the content's integrity. As they are based on technology and can be trusted, digital signatures are often considered more secure than a traditional handwritten signature. Intellectual property this encompasses the creations emanating from human intellect, like stories, music, artworks, and designs. Cyber law encompasses issues in the digital platform related to intellectual property, like copyrights on software and websites, cases for trademark dispositions on domain names and hyperlinks, and the whole patent regulations on both hardware and software[4].

Laws about data protection and privacy attempt to bring together the interests of individual privacy rights with the requirements of those entities dealing with data, like financial and health institutions. Regulations in these matters deal with the issues of privacy resulting from gathering and maintaining data that these technologies have made easier. Cybercrime has recently escalated in developing countries, fueled by increased internet accessibility and electronic commercial activities. Technology is weaved into daily affairs, influencing everything ranging from governmental functions to small-scale businesses that employ computers. Due to high reliance on such devices, losing a smartphone can create a sense of disconnection[5].

Cybercrime is not specifically defined in the Information Technology Act of 2000 or its 2008 amendment, nor in any other Indian laws. Instead, various offenses are outlined in the Indian Penal Code, 1860, and other laws. The internet brought many complex legal issues that existing laws could not cover. There was no law in India that recognized online activities, like emails, as valid. In response, the UN adopted the UNCITRAL Model Law on Electronic Commerce on January 30, 1997, to help guide countries in establishing their own cyber law[6].

The Government of India created the Information Technology Act, 2000, to legalize e-commerce and recognize electronic records as valid evidence, based on UNCITRAL's e-commerce framework. After identifying issues in this law, the Information Technology (Amendment) Act, 2008, was passed to address these problems and enhance legal

[4] ibid.
[5] ibid.
[6] Rohas Nagpal, "Introduction to Indian Cyber Law." (Asian School of Cyber Laws 2008).

recognition for electronic transactions, digital signatures, electronic document filing, data storage, and electronic fund transfers. This aimed to modernize India's legal framework for digital communications and transactions[7].

These laws aim to tackle privacy issues related to the collection, storage, and sharing of data through new technologies. In developing countries, cybercrime has rapidly increased due to widespread internet use and the digitization of businesses. Technology has become so ingrained in daily life— impacting everything from corporate governance to small shops using computers for billing—that it's hard to imagine a day without computers or mobile phones. Losing a mobile feel like being isolated![8]

In a special case in 2021, the Supreme Court of India ruled that cyber-attacks and data theft are crimes under the Information Technology Act (IT Act) of 2000 and the Indian Penal Code (IPC). Since the IPC is over 150 years old, the IT Act of 2000 is the main law dealing with cybercrime today. This act was India's first major cybersecurity law, created by Parliament and managed by the Indian Computer Emergency Response Team (CERT-In). It sets rules for cybersecurity, data protection, and covers areas like e-governance, e-banking, and e-commerce. The Information Technology Amendment Act of 2008 improved the original IT Act, adding necessary updates to help with the growth of technology. This amendment expanded the definition of cybercrime, validated electronic signatures, and made companies responsible for protecting data[9].

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 is one of the essential components of cybersecurity regulations. The framework includes guidelines for intermediaries and amendments with respect to penalties against offenses, which could range from fraud to the unauthorized distribution of private images. This also includes dictating how entities in India treat sensitive information and the process of maintaining data security. The National Cyber Security Strategy of 2020 has been a government initiative to support the strengthening of cybersecurity. At this point still under evaluation, it is also meant to provide guidance for decision-makers and enterprise heads in relation to preventing cyber attacks and other forms of terrorist activities.

[7] ibid.
[8] JP Mishra, An Introduction to Cyber Laws (1nd Edition Reprint 2012, Central Law Publications).
[9] ibid.

Therefore, with ever-increasing tech usage in the country and even worldwide, cyber regulation needs to be updated from time to time. The rise in remote work caused by the pandemic has heightened the demand for greater application security. It is thus imperative that the battle against cybercrime be undertaken collectively by the legislators, internet service providers, financial institutions, and e-commerce websites. However, it is not possible to secure online safety entirely without the collective efforts of the stakeholders[10].

The increase in harmful online activities and advances in cyber technology have prompted countries to think about how international law applies to actions in cyberspace. A country should be actively involved in global efforts to establish guidelines for responsible behaviour in cyberspace and is committed to applying international law to cyber activities. This approach is believed to be fundamental to the maintenance of global stability and security[11]. International Humanitarian Law (IHL) is applicable to cyber actions in international armed conflicts and internal armed conflicts. It dictates the manner of hostilities conducted and protects the victims. In armed conflicts, parties cannot select means of warfare that are not bound. Cyber actions can be termed attacks under IHL if they have a reasonable likelihood of causing injury or damage. Such actions must follow rules about distinguishing between military and civilian targets, ensuring proportionality, and taking precautions during attacks[12].

In India, a major issue in cybersecurity is that the government still uses outdated or unclear laws for prosecutions, which can slow progress in creating effective cyber regulations. Organizations struggle to understand ambiguous laws and fragmented regulations regarding data privacy and cybersecurity. To have widely accepted cybersecurity standards, India needs to create clearer and more comprehensive cybersecurity laws. If this does not happen, the government and law enforcement may continue relying on old laws, leaving many cybersecurity problems unaddressed[13].

The law on cyber warfare is not well defined, but it is not a new issue either. New challenges arise in updating laws related to the use of force and conduct in cyber warfare, such as understanding differing cyber threat goals among countries—some prioritize

[10] ibid.
[11] Dr. Prasanna A., "Cyber Crimes: Laws and Practice", IMG, Thiruvananthapuram
[12] ibid.
[13] ibid.

information flow while others seek to control. Real-time identification of actions can be challenging since it is often difficult to classify them as either offensive or defensive, or even hostile attacks compared to intelligence operations. Verification of violations in cyberspace is complicated by technical and legal limitations, and attribution issues complicate the task of linking online actions to specific states, raising questions of state responsibility[14].

To protect fundamental freedoms and privacy in the digital space, the approach should be centered on several key initiatives. First, commitment must be there to support civil society organizations in their efforts to create safe and secure platforms that facilitate free expression and association. Individuals should be encouraged worldwide to harness the power of digital media to voice their opinions, monitor electoral processes, expose corruption, and organize social movements. In this context, it becomes very important to combat harassment and violence against those who make use of these technologies.

A culture of fear can lead to stifled participation and discouraging others from engaging in meaningful dialogue, so our cause should be to stand firmly against such threats. Second, ISPs will play a pivotal role in protecting, since they have often faced undue legal pressures that compelled them into censoring legitimate speech. The United States will actively campaign for the protection of free speech and will also support civil society, human rights defenders, and journalists in their digital endeavors. It is believed that for governments to focus on dealing with actual cyber threats rather than imposing restrictions that limit freedom of expression through undue pressures on companies is imperative[15].

Another important area that we envision as part of our plan relates to cybersecurity especially with civil society organizations and others. We expect that through consultation and collaboration, these groups of individuals will feel safer in securing their online undertakings. Therefore, bolstering cybersecurity activit ies must be addressed and promoted if one is guaranteed that every member will enjoy speaking and associat ing freely in cyber space. This focus on cybersecurity is crucial for activists and journalists, as they often run significant risks, and the cyber attacks against their accounts and data systems may even target them

[14] ibid.
[15] Dudeja V.D (2011); Cyber Crimes and Law: Crimes in Cyber Space – Scams and Frauds, Vedams eBooks (P) Ltd (New Delhi, India), Published by Commonwealth (2002-09-24) ISBN 10: 8171697089 / ISBN 13: 9788171697083.

specifically[16].

In the international realm of data privacy, privacy for the individual is key in maintaining the trust that underlies the internet. The United States has enacted robust privacy laws and is aggressively working to develop its data privacy framework to better keep pace with rapid technological advancements. Our objective is to foster mutual recognition of privacy laws worldwide and to collaborate on enforcement efforts that protect individual privacy while encouraging innovation. In addition, ensuring access to the internet for all is an important part of our vision. Users should be able to rely on the fact that their information will be transmitted accurately and securely, regardless of where they are. We are against any efforts to create isolated national networks that limit access to information from other countries, as such practices undermine the global nature of the internet[17].

Countries also maintain secrecy over their cyber operations and rarely disclose information about attacks due to the fearof exposing weaknesses. In this regard, a new comprehensive treaty is not in the near future, but instead, there may be updates to the already existing treaties, such as the International Convention on Cybercrime, which requires countries to enact laws against cybercrimes. Smaller agreements related to cyber defense strategies among the particular groups of countries may surface. In due course, law developments in future cyber warfare can be expected to evolve gradually over state practices without formal treaties; and this shall be even more slow than that of the old times because it is difficult for cyber warfare in nature to spot clear starting points and actions with ease. Although technology keeps advancing, formalizing clear law standards and procedures will take considerable time, in all likelihood rendering the discussions perpetually ongoing. Countries and their organizations will voice their own interests in the understanding of the law rather than truly negotiating[18].

[16] ibid.
[17] ibid.
[18] ibid.