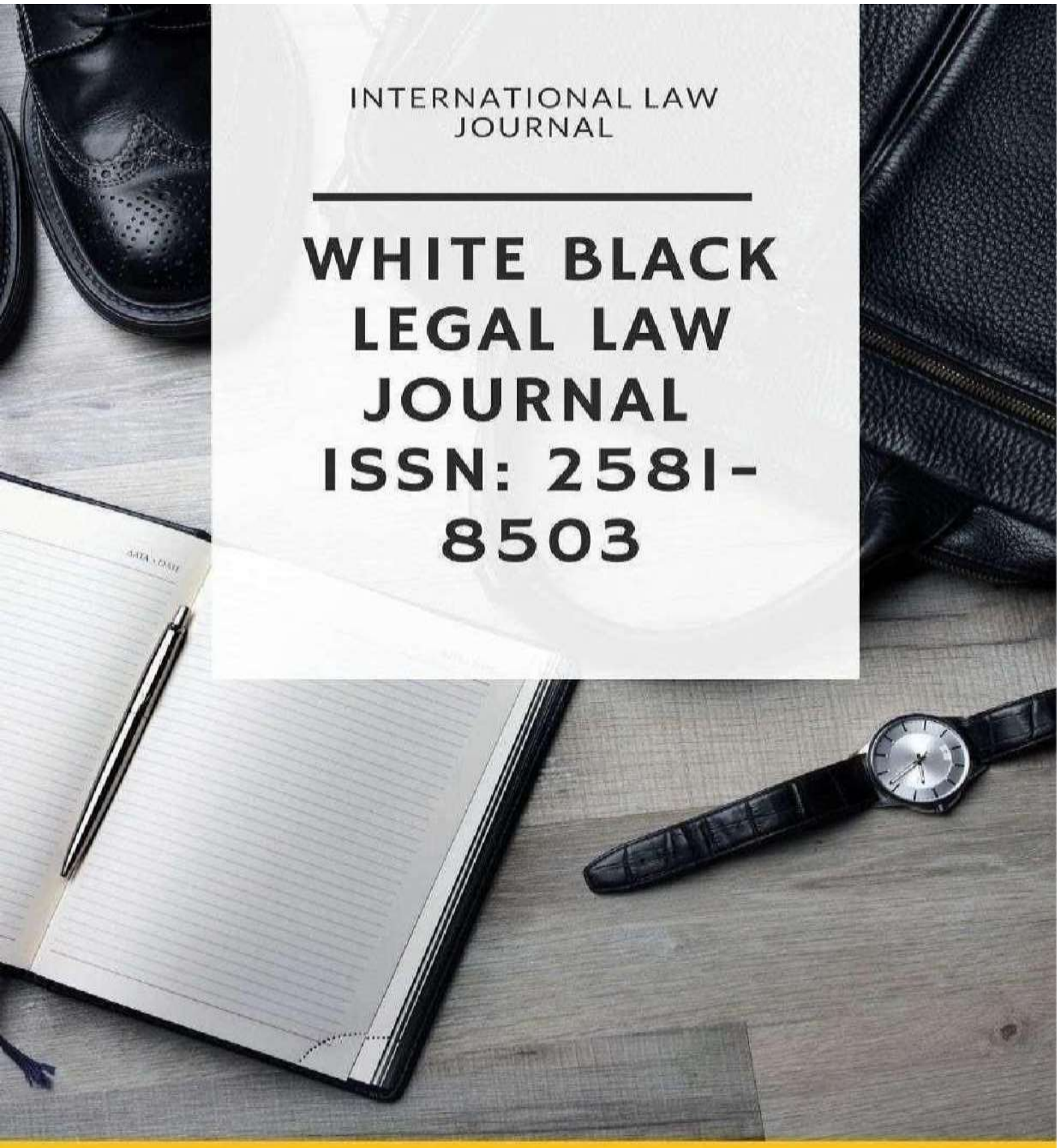

INTERNATIONAL LAW JOURNAL

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

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.

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

INFORMATION AND COMMUNICATION TECHNOLOGY IN A GLOBALIZING WORLD.

AUTHORED BY - SHASHANK JOHARI

ABSTRACT.

This paper seeks to understand the role played by Information and Communication Technologies (referred to as ICT hereon) in the process of globalization. It touches upon the fact that the world has been connected by technologies such as the internet, dissolving territorial boundaries. The paper seeks to inform about the positive as well as the negative impacts of ICTs, and touches upon certain measures taken to regulate cyberspace in order to curtail acts of cybercrimes, cyberterrorism, and regulate content and data flow. It also understands the benefits of ICTs in globalizing world as well as the social and environmentalimpact it has had. The paper seeks to explain the concept of cybercrime and how it is relevantnot only to businesses in the global market but also individuals, countries, political ideologiesand that even crime has now no boundaries. The question asked is whether the steps taken bya few of the international actors have managed to somewhat regulate and identify the components of cybercrime, and whether there can be a proposed global policy that can benefit individuals, corporations, nations and data sovereignty at large.

INTRODUCTION.

The concept of communication in a globalized world has blurred the old school territorial lines and has led to the deterritorialization with the advent of new age communication.Events, which were earlier in isolation, can now be absorbed by a previously unaware audience. Communication and related technologies have played an important part in acting asa catalyst to realize a globalized economy. Connecting with people in any part of the world is now a much easier process than it was three decades ago. Globalization has had a direct affect on global communications, and that in turn has helped in increasing business opportunities, has removed cultural barriers, and has helped in developing the world as a global village, all the while changing

the environmental, cultural, political and economic elements of the world.[1] The efforts taken to efficiently communicate have been significantly reduced, as sharing information with different actors of a globalized world, in varied geographies, with the help of satellites, fiber optic cables and most importantly the internet.[2]

Even contemporary analysts have associated the term globalization with deterritorialization explaining that the geographical location has become an irrelevant factor when participants react to a global event.[3] Actions, interactions to situations by such participants and social

activities is now irrespective of their location in terms of latitude and longitude.[4] The internet has provided for instant communication among participants residing or incorporated in various parts of the world. Business can now be conducted via electronic commerce, television has given access to every event across the globe as they unfold.[5]

Other than the concept of deterritorialization, globalization has led to a growth in interconnectedness across existing geographical and political boundaries.[6] As a result of which distant events and forces have had an impact on regional activities as well.[7] As an example one can take the case of an encyclopedia available online, for which the only requirement is internet access, thus making social space irrespective of territorial lines.Interconnectedness can also be considered now as being regularized and predictable asopposed to haphazard.[8]

Globalization has also influenced the speed or velocity of social activities, and the rapid speed by which high speed transportation, communication and information technology has grown, having become the immediate source which blur the geographical boundaries as observed by theorists since the mid nineteenth century. Which has led to a fast flow and movement of people,

---

[1] Ahmed A, "The Effects of Globalization on Global Communication" (Bizfluent February 11, 2019) <https://bizfluent.com/info-8232542-effects-globalization-global-communication.html> accessed November 25, 2019.
[2] *Ibid*.
[3] Scheuerman W, "Globalization" (Stanford Encyclopaedia of Philosophy November 5, 2018) <https://plato.stanford.edu/entries/globalization/> accessed November 25, 2019.
[4] *Ibid*.
[5] *Ibid*.
[6] *Ibid*.
[7] *Ibid*.
[8] *Ibid*.

information, capital and goods.[9]

Transnational corporations have incorporated high speed technologies with great efficiency, wherein cross border transactions in cyberspace can now take place in the blink of an eye serving as a fine example of a globalized economy influenced by technology acting in territorial compression and reinvented time and space.[10]

NEXUS OF ICT AND GLOBALIZATION, POSITIVE IMPACT.

In the past two decades the term globalization has become a popular expression, but the term is a complicated one since the additional factors are highly integrated. It can be said that ICTshave had a great impact on the process of globalization, so much so that the answer to the question "why has globalization happened?" put forward by Langhorne in his book "The Essentials of Global Politics" has been provided and is, "because of the technological advances in global communication".[11]

Industrial developments led to further improvements in communication technologies and can be conceptualized in three stages. The first involved the invention of the steam engine and electric telegraph. The second stage involved the development of orbiting satellites and the telephone. The last stage comprises of the development of computer technologies and the internet. These three stages successively led to a revolution of communication in the globalization era.[12] The first two stages focused only on the aspect of communication, whereas the third stage is a combination of communication as well as information technologies.[13] In the 1970's switching, routing, transmissions became a part of technologicaldevelopments making it possible for ease in computer networks, further relaxed by fiber optics and laser technologies, increasing the capacity of the networks, constituting a global infrastructure for the networks.[14]

ICT have impacted the many aspects of globalization by their integration and relations, primarily:-

---

[9] *Ibid.*
[10] *Ibid.*
[11] Öztürk E, "A Comprehensive Approach to the Role of Information And Communication Technology (ICT) in Globalization" (2015) 8 Journal of International Social Research 359.
[12] *Ibid.*
[13] *Ibid.*
[14] *Ibid.*

1. Economic

The internet has provided for a safe and sustainable network which has led to economic globalization, as a large number of economic activities presenting itself on the global stage can be handled, by increasing the capacities of companies and nations.[15] The new economy has specifically been affected by ICT with respect to speed, low costs, flexibility, networks and applications.[16] It has reduced the emphasis on geographical distances and has made financial markets more transparent, as well as improving supply chains for business purposes.There has been a visible increase in "internet related firms in the 21st century and electronic business transactions in 2003 increased 30 times faster than those in 1998".[17] One of the driving factors of economic growth today is productivity. There is a correlation between ICT and productivity. "An indication of the relationship between technology, organizational change, and productivity can be provided by the 1997 study by Brynjolfsson of 600 large US firms, focusing on the impact of organizational structures on the relationship between computers and productivity. Overall, Brynjolfsson found that investments in information technology were correlated with higher productivity".[18] Thus a greater interconnectedness has been established, supporting decentralization, providing free interactions between the participants in the market, giving a relation between e-commerce and e-economy.[19]

"According to Capineri and Leinbach (2004: 646), "E-commerce implies transactions for a service, which is completed using the Internet from selectionto purchase and delivery or it involves 'distribution services' in which aproduct, whether a good or a service, is selected and purchased on-line but delivered conventionally[20]".

ICT have affected all the components of economy, and it now consists of components mainly, information, networks and global, advancing international trade and interconnectedness of financial markets.[21]

---

[15] *Ibid, Page 361.*
[16] *Ibid, Page 362.*
[17] *Ibid.*
[18] *Ibid.*
[19] *Ibid.*
[20] *Ibid.*
[21] *Ibid, Page 363.*

2. Social and cultural.

Interaction between people anywhere and communication between them have been affected by the advent of ICTs and the process has become a lot more cross cultural, combining various forms of cultural expressions, leading to a rise of a new global culture.[22] Language being an important part of cultural expression has been essentiallymade universal, by making English into a language for global communications.

America has been the pioneer in ICT and their culture has spread rapidly through products sold via such technologies yet have become less American with time as many corporations use feedback from customers and users all over the world and shape their products accordingly.[23]

People can now make social connections without boundaries, being informed and networked with other informed societies, assembled around shared values and concerns.[24] There is new emerging global pattern of social interactions which are more effective, making information society a reality, providing a cheap, easy and faster way of communicating, making social movements reach far corners.[25] Such social movements also have components of justice on various issues that have an effect on a global scale, now accessible, and attract public interest from all over the world.

3. Environmental.

On the face of it, it may seem that there is a paradoxical relation between environment and technology, however it can be said that ICT have provided solutions for various environmental problems by managing and monitoring data, created with statistics that have been calculated with the help of technology. For example, decision support systems or geographic information systems. Other secondary benefits being reduced use of paper and the provision for a consistent and networked online framework.[26]

Thus, seen as an informed society, ICT have played an important role as we are more global than ever, and yet with further developments, future social activities will be more planned and executed accordingly.

It can be ascertained from the above that the advent of ICT in a globalized market has not only

---

[22] *Ibid.*
[23] *Ibid.*
[24] *Ibid.*
[25] *Ibid.*
[26] *Ibid, Page 364.*

brought economies in nexus, but has also provided for interaction of social values, virtues and culture at a much higher speed. It has provided for a productive environment wherein people can share thoughts, ideas, instances and events without being border bound.

MISUSE OF ICT, A NEGATIVE IMPACT.

The model of globalization that currently exists, provides for rapid growth in the current economy, further fueled by the internet and an internet-based economy.[27] This can be seen by the fact that over 40% of the people us the internet as opposed to only 16 million in 1995,[28] which is evidence of the fact that the interconnectedness has led to certain dependency on such technologies.

Although the global economic growth has been driven by exponential increase in cross border internet traffic and digital communication, certain cyber security concerns have also been highlighted, which range from cybercrimes that have affectedmillions of users by either stealing their information or invasion of privacy or cyber attacks or terrorism influence online targeting governments and also posing a threat to national security. Massive data has been stored in cyberspace which the users have raised a concern with respect to operations and lack of security and privacy protections by most of the organizations in both private and public sector, which are involved in collection and process related to such data.[29]

The flow of data is being leveraged by these organizations and even though ICT provides a lot of benefits, the key players are involved in the global internet, no longertrust each other.[30]

1. THE PHENOMENA OF CYBER CRIME.

1.1 Definition

"During the 10th United Nations Congress on the Prevention of Crime andthe Treatment of Offenders, two definitions were developed within a related workshop: Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the securityof computer systems and the data processed by them. Cybercrime in a

---

[27] Jong-Chen Jde, "Spotlight on Cyber V: Data Sovereignty, Cybersecurity and Challenges for Globalization" (Georgetown Journal of International Affairs October 12, 2015) <https://www.georgetownjournalofinternationalaffairs.org/online-edition/data-sovereignty-cybersecurity- and-challenges-for-globalization> accessed November 26, 2019.

[28] *Ibid.*

[29] *Ibid.*

[30] *Ibid.*

broadersense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network."[31]

A wide range of offences are covered in cybercrime and it is not an easy task to classify them and a typology might not be consistent, but can be broadly segregated into offences of confidentiality, integrity, and availability of computer data and systems, computer and content related crimes and those related to intellectual property.[32]

1.2 Cybercrime in the 21st century.

By the 21st century new trends have emerged in relation to cybercrimes, with a more sophisticated method, involving like phishing as well as botnet attacks, and use of technologies that can evade the investigation authorities like cloud computing and voice over IP (VoIP) communication. Also, as the perpetrators were able to automate attacks, the number of attacks increased.[33]

1.2.1. Illegal access

Unlawful access or hacking as it is commonly known is one of the most common offences committed in cyberspace, examples of which include famous targets like NASA, pentagon or websites like Yahoo or Google or personal targets like website hacking, spoofing or even record keystrokes or gain unauthorized access to personal servers by gaining access to passwords of individuals. The motivations for suchattacks may vary like circumventing security measures, or political motivation like hacktivism. Further crimes may be committed by gaining such access like data espionage, manipulation of data or denial of service attacks.[34] The protection ofnetworks used in corporations have a higher security than private networks, leaving them comparatively vulnerable to crimes, where sensitive personal information can begained like banking and credit card details.[35]

---

[31] *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (ITU 2012), page 11.

[32] *Ibid, Page 12.*
[33] *Ibid, Page 13.*
[34] *Ibid, Page 17.*
[35] *Ibid, Page 18.*

1.2.2. Illegal interception

E-mails and uploaded data or external storage media can easily be targeted and may also include targeting the communication infrastructure. Increase in wireless accessall over the globe has left data exchange vulnerable even when it is said to beencrypted, and consequently gain access to sensitive information.[36]

1.2.3. Content related offences

Due to the anonymity that ICT may provide to criminal perpetrators there is a widespread exchange and sharing of material that is illegal, like pornographic material, xenophobic posts, or insults relating to religious symbols.[37]

Sexually related content was one of the first things to be commercially distributed,[38] and cyberspace provides unhindered advantage to retailers as well as to viewers who may or may not be influenced by such material. The law governing the exchange of erotic or pornographic material may vary, but preventing such access is a challenge asICT may provide a cloak of invisibility. Regular as well child pornography has been actively distributed, and not only is difficult to regulate the exchange of such prohibited material, the access of such material to minors, who may be influenced without being fully aware of its consequences is a legal void that all counties need to fill.

Other forms of illegal content may include forums for soliciting, incitement to commitcrimes, like terrorism recruitment and unlawful sale of products or offering information that may be used for destructive purposes like how to build a bomb.[39]

1.2.4. Cyberterrorism

Cyber attacks on a large scale is a recent phenomenon with the advent of newdevelopments and access in ICT. Taking as an example the recent attack on Sony Pictures with respect to the release of the movie The Interview, combined with the threat of physical harm. This has highlighted the

[36] *Ibid, Page 19.*
[37] *Ibid, Page 21.*
[38] *Ibid, Page 22.*
[39] *Ibid, Page 27.*

vulnerability present in the cyber defense of private companies as well as states.[40]

These occurrences are not a one-off incident and a *"dangerous and complex realm is emerging where the level of sophistication of terror groups and states is growing. Cyberterrorism and cyberwarfare have become a key national security threat."*[41]

"By way of some examples, in September 2014, various news outlets reported that jihadists in the Middle East, including leaders from both the Islamic State (also known as ISIS) and al Qaeda, were actively planning cyberattacks against Western countries, specifically targeting government servers and critical infrastructure. It was further reported that ISIS was planning to establish a "cyber caliphate" "intending to mount catastrophic hacking and virus attacks on America and the West."[42]

The increase in such attacks is primarily due to the availability of funds on the online platform, however many countries have been involved in creating a cyber defence system and devise mechanisms for internal as well as international cooperation between states and agencies in a cyber arena that is not only complex but also always evolving.[43]

The high speed at which globalization is progressing, and the complex situations that arise not only for corporations but also for individuals, the main issue that arises is locating the perpetrator of such crimes and sometimes even impossible to identify. There are vulnerabilities present as there are no restrictions on cyber space, making regulation of activities in the cyber realm a complex reality, requiring cooperation from across borders, in order to locate and eliminate such vulnerabilities.

CHALLENGES OF FIGHTING CYBERCRIME.

ICTs have inherent in their nature an ever developing and evolving concept which in time have resulted in innovative ways of committing cybercrimes but has also led to new methods in investigations incorporated by law enforcement agencies. They can use forensic software and key word-based searches to identify illegal activities. The main challenge comes in the way of investigation agencies is the growing number of users who are now heavily reliant on ICTs

---

[40] "Combating Cyberattacks In The Age Of Globalization" (*Hoover Institution*) <https://www.hoover.org/research/combating-cyberattacks-age-globalization> accessed November 26, 2019

[41] *Ibid.*

[42] *Ibid.*

[43] *Ibid.*

especially in the developing nations. There is an increasing ease of access and wireless availability and limiting such opportunities may be challenge for the investigation authorities. Taking as an examplethe cyber café rules taken out by Indian authorities after the information that the terrorist attack was planned in the confines of a cybercafé. The problem being that wireless availability has made these rules obsolete, since now restaurants, clubs, airports all have wireless connections, with an easy way around the current cyber security measures.

One of the prominent challenges in fighting cyber related crimes is awareness, not only by the investigating authorities, but users with respect to remedies available when they are a victim of a cyber-attack.

The speed at which data is exchanged disadvantages the investigation authorities and they face other problems primarily relating to automation, vast available resources, anonymous communications and failure of traditional investigation instruments, especially when it comes to encryption technology.[44]

EFFORTS INVOLVING CYBER SECURITY.

Nations have struggled with these issues, with varied competitive response on how to manage cyberspace ensuring data sovereignty and data security starting to emerge.[45]

"In May 2011, the White House published its "International Strategy for Cyberspace". The paper envisions the Internet as a global network without borders, which enables the free flow of information and provides unrestricted cross-border commerce and communication. The position was consistent with the existing Internet governance model and American principles of free speech, free association, and personal privacy. The paper nevertheless made clear that the United States is prepared to retaliate against cyberattacks with military force if necessary.

Four months later, in September 2011, China, Russia, Tajikistan and Uzbekistan submitted to the 66th session of the United Nations General Assembly an "International Code of Conduct for Information Security." The document proposed a voluntary set of rules including strict enforcement of cyber sovereignty, which gives a government the legal right to enforce its own laws

---

[44] Understanding Cybercrime: Phenomena, Challenges and Legal Response (ITU 2012), Pages 79-81.

[45] Jong-Chen Jde, "Spotlight on Cyber V: Data Sovereignty, Cybersecurity and Challenges for Globalization" (*Georgetown Journal of International Affairs* October 12, 2015) <https://www.georgetownjournalofinternationalaffairs.org/online-edition/data-sovereignty-cybersecurity- and-challenges-for-globalization> accessed November 26, 2019.

within its own borders and control the flow of data."[46]

One of the prominent issues faced to data security and sovereignty was the Snowden case, who was a contractor to the National Security Agency, leaked information aboutthe United States surveillance program, which led to many countries reconsidering their position on cyber sovereignty and the question that started being asked was that how much information of users was accessible to the government, which led toquestioning the liability of private companies storing data.[47]

As a result, countries like Russia formulated their law in 2014 regarding cloud serviceproviders doing business in the country, complying with strict data residency requirement.[48]

The US under Barrack Obama signed an executive order in February 2015 at the Cybersecurity Summit held at Stanford University, responding to repeated attacks on business enterprises, promoting public and private sector collaboration on securityand sharing of information.[49] Similarly China and Russia revised their code of conduct for information security to include "policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities forinternational Internet-related public policy issues."[50] The policy also required a creation of "multilateral, transparent and democratic international Internet government mechanisms, which ensure an equitable distribution of resources, facilitate access for all, and ensure the stable and secure functioning of the Internet."[51]

PROPOSING A GLOBAL FRAMEWORK FOR CYBERSECURITY.

In the context of information security, some recommendations may be to

"Educate the end-user; Increase public awareness to enhance security user's behaviour; Give to the end-user tools and means to be responsible; Design an end-user centric security model within a given technical and legal framework; Information technology and content providers

[46] *Ibid.*
[47] *Ibid.*
[48] *Ibid.*
[49] *Ibid.*
[50] *Ibid.*
[51] *Ibid.*

should improve thesecurity of their products and services." [52]

Whereas in developing countries what can be proposed is an understanding of cybercrimes through a global lens, having a defined strategy, and developing awareness by promoting a cybersecurity culture[53]. In addition,

"Train and inform on information and communication technologies and on security issues, and relevant legal provisions; Develop cyber security education; Propose a unified cybersecurity framework which includes, in a complementary fashion, the human, regulatory, organizational, economic, technical and operational dimensions of cyber security; Put in place organizational structures to support a national cybersecurity strategy; Create regional alert points for the provision of technical information and assistance regarding security risks and cybercrime; Create effective cybercrime laws that are enforceable at national and international levels (global and harmonized legal framework taking into account the right to privacy (Protection of public safety, with protection of privacy and civil liberties)); Redefine law enforcement and legal framework in order to bring cybercrime perpetrators to justice; Manage jurisdictional issues; Fight cybercrime (deterrence, detection, investigation, prosecution of cybercriminal activities, crime reporting, crime analysis, practices and experiences on search and seizure of digital evidence, organizing capacities to combat cybercrime, information sharing, promotion of effective public and private sector cooperation); Develop acceptable practices for ICT protection and reaction; Establish effective cooperation and promote cooperation and coordination at national and international levels."[54]

CHALLENGES IN CREATING A GLOBAL SOLUTION.

Nations have different value systems, and it is difficult for them to have a common setof systems, yet there are a number of common concerns which can be adopted in collaboration by countries to form a productive outline regarding cybersecurity. The process of such collaboration is a time-consuming process as it is difficult to keep up with the speed at which ICT and related technologies are growing.

"the European Union drafted its data protection directive in the early 1990s, and the United States

[52] Stein Schjolberg and Solange Ghernaouti-Helie A Global Treaty on Cybersecurity and Cybercrime, Second edition, 2011, Page 16.
[53] *Ibid.*
[54] *Ibid, Page 17.*

adopted the Electronic Communications Privacy Act in 1986. Countries created many of the existing laws for a different time—before smartphones and mobile devices, before most people had even heard of the Internet. It is also important to make the enforcement of the rules more efficient, and to keep in mind that technology will continue to advance rapidly.

In addition to laws and policies, governments have the option of adopting advanced security technologies for data protection and national security purposes. In many cases, investment in security-technology innovation and adoption of global security best practices would be better strategies than simply segregating data and restricting data flow. As an example, CESG, the British national information security assurance authority, has promoted the concept of "Secure by Default" and the use of IT security solutions based on global security standards such as the Trusted Platform Module (TPM), produced by the Trusted Computing Group, an international industry standard organization. Among other functions, the TPM enables hardware- based security to help provide full-disk encryption of computers and mobile devices in an effort to protect data no matter where it resides. The TPM also offers features such as generating encryption keys, enabling attestation between devices, and securing device identity and health to prevent unauthorized access."[55]

CONCLUSION.

In a fast-paced economy, the advent of ICT has made globalization a faster process. Even though the benefits of trade and transnational corporations, economies andinterconnectedness between international factors and actors are many, it is not withoutits downfalls. Globalization has made the world into a global village, cutting on territorial boundaries, and the development of computer technologies and internethave further enhanced the efficiency of global markets. On the other hand, a huge amount of personal and business data has been stored within the cyberspace and the vastness and boundarylessness of such data is difficult to regulate and control. As with every new technology comes new challenges to identify innovative methods of committing crime, the lack of awareness faced by users as well as the anonymity enjoyed by the criminal elements in cyberspace is aplenty.

---

[55] Jong-Chen Jde, "Spotlight on Cyber V: Data Sovereignty, Cybersecurity and Challenges for Globalization" (*Georgetown Journal of International Affairs* October 12, 2015) <https://www.georgetownjournalofinternationalaffairs.org/online-edition/data-sovereignty-cybersecurity- and-challenges-for-globalization> accessed November 26, 2019.

There is hence a requirement of collaboration between countries to formulate policies that can govern cybersecurity risks across borders, which in itself is a challenging taskdue to the speed at which development in ICTs is taking place. There is an evident increase in the number of users in third world countries as opposed to the first world countries, and yet there is a varied approach to issues relating to cybersecurity affecting developing as well as developed markets.

What is in essence required is adequate measures like those by the European Union orthe United States, to be implemented, and not imposed upon, developing countries with which the global economy interacts.

The current measures have been successful in identifying the problematic areas governing cyberspace and security, yet have not been able to keep up with the speed at which technologies are developing, thus a global collaboration of independent actors is required, to enhance the efficiency of cybersecurity measures all over the globe.