Global Cyber Governance: Convergence and Discord

A THESIS SUBMITTED IN PARTIAL FULFILLMENT FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN THE DEPARTMENT OF POLITICAL SCIENCE

GOA UNIVERSITY

By

Monojit Das

D.D. Kosambi School of Social Sciences and Behavioural Studies
Goa University
Goa

AUGUST 2021

DECLARATION

I, Monojit Das hereby declare that this thesis represents work which has been carried out by me and that it has not been submitted, either in part or full, to any other University or Institution for the award of any research degree.

Place: Taleigao Plateau.
Date: 16-08-2021 Monojit Das

CERTIFICATE

I hereby certify that the above Declaration of the candidate, Monojit Das is true and the work was carried out under my supervision.

Dr. Rahul Tripathi
Research Supervisor &
Head, Department of Political Science

Acknowledgment

I would like to dedicate the work to my mother Smt. Rina Das and father Mr. Murari Mohan Das, they are the ones because of whom I am what I am!

I would like to thank my supervisor Prof Rahul Tripathi to have confidence on me and grant me the opportunity to pursue research under his guidance and also allowing me to get a diverse experience including the opportunity to work in close association related to ICCR (Indian Council of Cultural Relations) Ministry of External Affairs, Government of India and other international collaborations initiatives besides making me part of various departmental initiatives under Election Commission of India (ECI), Unnat Bharat Abhiyan (UBA) under Ministry of Human Resource Development (now Ministry of Education), rural development courses under GIPARD (Goa Institute of Public Administration and Rural development) besides participating in several conferences and seminars.

I thank the university students for electing me as their representative in the University Council for all three years of my stay in the university and giving me a boost to someday to plan in a wider scale.

I further thank to all my teachers from Defence and Strategic Studies fraternity across the country whose guidance have enabled me to reach here starting Dr. PA Ghosh (BMC Nashik) , Ramesh Raut sir (BMC Nashik), Dr Inderjeet Singh sir (PUP, Patiala), Prof. RN Mishra sir (PUP, Patiala), Dr Umrao Singh sir (PUP, Patiala), Prof Kamal Kinger sir (PUP, Patiala), Prof Uttam Kumar Jamadhagni sir (Madras University), Dr. E Prabhakaran sir (Madras University) and Dr. Venkataraman sir (Madras University).

I would like to express my gratitude to all well-wishers who saw me through this research work and provided support on several occasions I thank Dr Prakash Desai, Dr Alakananda , Ravaji sir for extending support always whenever needed.

My sincere thanks to Madam Reshma non-teaching staff at the department to guide with admission with Puja and Vinda maam for being there always when needed.

Special mention to Prof Shilpa Tripathi for being well-wisher and discussion on cyber security.

It will be incomplete without thanking my friends Rohit, Mukh Kaur, Naveena, Sunny for cooking delicious local Goan cuisines during the crucial times when I was writing the thesis,and Mikaila in particular for helping with designing, Reshma and brother Akshay for their support and good wishes.

Have the privilege to learn on the practical implementation of India's foreign policy from Shri Sudarshan Shetty sir, ICCR, MEA, particularly on cultural diplomacy.

I thank my funding agency ICSSR (Indian Council of Social Science Research), Ministry of Education, Government of India, for granting me doctoral fellowship, and Goa University for granting the research studentship by supporting during tough pandemic times.

I place my respect to all the front line workers who worked day and night for keeping us safe, and consider myself fortunate to be part of the front line worker team at the Directorate of Health Services (DHS), Panaji, for managing real time data of COVID positive patients in efficient operations and planning of COVID management in the state of Goa to contribute towards my share for the well-being of society in fighting the pandemic.

Last and not the least I beg forgiveness from all those whose names I failed to mention here who have been with me over the course of the years but will always remain in heart.

Finally, to the Bordermen family for securing our nation, I dedicate this work and hope it can be an ode to the duty they perform every day that is difficult even for the sake of an adventure activity by an ordinary citizen.

Monojit Das
PhD Research Scholar
Dept of Political Science
Goa University

Contents

List of Tables

List of Figures

Abbreviations

0G - Zero Generation

1G - First Generation

2G - Second Generation

3G - Third Generation

4G - Fourth Generation

5G - Fifth Generation

A4AI - Alliance for Affordable Internet

ACA- American Cyber Alliance

AFRINIC- African Network Coordination Centre

AI -Artificial Intelligence

AISA- African Information Security Association

AMN - Afghanistan Mission Network

ANZUS -Australia-New Zealand-US

APC - Association for Progressive Communications

APEC - Asia Pacific Economic Cooperation

AP-IS - Asia-Pacific Information Superhighway

APNIC - Asia Pacific Network Information Centre

APT - Advance Persistent Threat

APT - Asia Pacific Telecommunity

APT-SC - APT Symposium on Cyber security

APWG - Anti Phishing Working Group

ARF - ASEAN Regional Forum

ARIN- American Registry for Internet Numbers

ARPANET - Advanced Research Projects Agency Network

AS - Autonomous Systems

ASEAN - Association of Southeast Asian Nations

ASPI - Australian Strategic Policy Institute

AT&T - American Telephone and Telegraph

ATC- Air Traffic Control

AU- African Union

BBN Technologies - Bolt, Beranek and Newman

BEC - Business Email Compromise

BGP - Border Gateway Protocol

BIS - Bank for International Settlements

BOP - Balance of Power

BRI - Belt and Road Initiative

BRICS – Brazil, Russia, India, China and South Africa

CARICOM - Caribbean Community

CASC - Centre for Accountability and Systemic Change

CBM - Confidence Building Measures

CCC - Customs Co-operation Council

CCITT - International Telegraph and Telephone Consultative Committee

CCP - Chinese Communist Party

CEO - Chief Executive Officer

CERT - Computer Emergency Response Team

CI - Cyberspace Institute

CIA - Central Intelligence Agency

CIA- Central Intelligence Agency

CIRT - Computer Incident Response Team

CIS - Centre for Internet and Society

CIS - Commonwealth of Independent States

CITEL- Inter-American Telecommunication Commission

CLARA - Cooperación Latino Americana de Redes Avanzadas (Latin American Cooperation of Advanced Networks)

CLNP - Connection Less Network Protocol

CoE - Council of Europe

COG- Cyber Observer Group

COMESA - Common Market for Eastern and Southern Africa

COP - Child Online Protection

CPKF- Cyber Peace Keeping Force

CSC- Cyber Sanction Committee

CSEC - Communications Security Establishment Canada

CSG -Creation of Cyber Security Guard

CSIRT - Computer Security Incident Response Team

CSNET - Computer Science Network

CTO - Commonwealth Telecommunications Organisation

CTU - Caribbean Telecommunication Union

T-CY - the Cybercrime Convention Committee

DARPA - Defense Advanced Research Projects Network

DCEP - Digital Currency Electronic Payment

DCU - Dublin City University

DDoS - Distributed Denial-of-Service

DND - Do Not Disturb

DNS - Domain Name System

DOD- Department of Defence

DoS - Denial of Services

DOT Force - Digital Opportunity Task Force

DPA - Data Protection Authority

DRN - Defence Restricted Network

DSL- Digital Subscriber Line

dSLOC - digital Sea Lines of Communication

E2E - End-to-End

EC3 - European Cyber Crime Centre

ECCAS - Economic Community of Central African States

ECEG - Electronic Crime Expert Group

ECOSOC - Economic and Social Council

ECOWAS - Economic Community of West African States

ECSO - European Cyber Security Organization

EDGE - Enhanced Data rates for GSM Evolution

EEZ - Exclusive Economic Zone)

EFF - Electronic Frontier Foundation

ENIAC - Electronic Numerical Integrator and Computer

ENISA - European Union Agency for Network and Information Security

ESCAP - Economic and Social Commission for Asia and the Pacific

EU- European Union

EuroDIG - European dialogue on internet governance

EWI – East West Institute

FBI - Federal Bureau of Investigation

FDI - Foreign Direct Investment

FIGI - Financial Inclusion Global Initiative

FVEY - Five Eyes

G77- Group of 77

G8 - Group of Eight

GANs- Generative Adversarial Networks

GATT - General Agreement on Tariff and Trade

GCC - Gulf Cooperation Council

GCI - Global Cybersecurity Index

GCSC - Global Commission on the Stability of Cyberspace

GDPR - General Data Protection Regulation

GGE - Group of Governmental Experts

GIC - Global Internet Council

GIGF - Global Internet Governance Forum

GIP - Global Internet Project

GIPC - Global Internet Policy Council

GOSIP - US Government OSI Profile

GPRS - General Packet Radio Service

GPS - Global Positioning System

GSM - Global System for Mobile communication

HCSS - Hague Centre for Strategic Studies

HUMINT - Human Intelligence

IAB - Internet Advisory Board

IAB- Internet Architecture Board

IANA (Internet Assigned Numbers Authority)

IAPP - International Association of Privacy Professionals

IBM - International Business Machines

IC3- Internet Crime Complaint Center

ICANN - Internet Corporation for Assigned Names and Numbers

ICAO - International Civil Aviation Organization

ICDA - International Coalition for Development Action

ICPC - International Cable Protection Committee

ICRC - International Committee of Red Cross

ICSPA - International Cyber Security Protection Alliance

ICT - Information and Communication Technologies

ICT4D - Information and Communication Technology (ICT) for development

IESG - Internet Engineering Steering Group

IETF - Internet Engineering Task Force

IFWP- International Forum on the White Paper

IGF - Internet Governance Forum

IGOs - Inter Governmental Organizations

IHL - International Humanitarian Law

IIC - International Internet Council

INTERPOL - International Criminal Police Organization

INWG - International Network Working Group

IOCTA - Internet Organized Crime Threat Assessment

IoT - Internet of Things

IP - Internet Protocol

IPRs - Intellectual Property Rights

IPU - Inter Parliamentary Union

IPv4- Internet Protocol version 4

IPv6 - Internet Protocol version 6

IR – International Relations

IRT- Incident Response Team

IRTF - Internet Research Task Force

ISAC - Information Sharing and Analysis Center

ISC - Internet Systems Consortium

ISF - Information Security Forum

ISF - Internet Social Forum

ISIS -Islamic State of Iraq and Syria

ISO - International Organization for Standardization

ISOC - Internet Society

ISP - Internet Service Provider

ISS - International Space Station

ISS -International Space Station

ISSA - Information Systems Security Association

ISSA - Information Systems Security Association International

ISU - Internet Service Unit

IT – Information Technology

ITRs - International Telecommunication Regulations

ITU - International Telecommunication Union

IUF - Internet Ungovernance Forum

IXP- Internet Exchange Point

JPL - Jet Propulsion Laboratory

JWICS - Joint Worldwide Intelligence Communication Systems

LACNIC - Latin America and Caribbean Network Information Centre

LAN - Local Area Network

LATAM- Latin America

LAWS - Lethal Autonomous Weapon Systems

LEO - Low Earth Orbit

LGPD - Lei Geral de Protecao de Dados

LOAC - Law of Arm Conflict

LTE - Long Term Evolution

M^3AAWG - Messaging Malware Mobile Anti Abuse Working Group

MCI - Microwave Communications, Inc.

MNC - Multi National Companies

MoG- Monitoring Group

MOU - Memorandum of Understanding

NAPs - Network Access Points

NASA - National Aeronautics and Space Administration

NATO - North Atlantic Treaty Organisation

NBA- News Broadcasters Association

NCH -National Cyber Helpline

NCO- Network Centric Operations

NCSI - National Cyber Security Index

NCTAC- National Cyber Threat Analysis Centre

NFC -Near Field Communication

NGO - Non Governmental Organization

NIST - National Institute of Standards and Technology

NPCI - National Payments Corporation of India

NRO- Number Resource Organization

NSA - National Security Agency

NSFNET - National Science Foundation Network

NTT - Nippon Telegraph and Telephone

OAS - Organization of American States

OAU - Organisation of African Unity

OC3 - Office of Coordination of Cyber Crime

OECD - Organisation for Economic Cooperation and Development

OECS - Organisation of Eastern Caribbean States

OEWG -Open-ended Working Group

OHCHR - Office of the High commissioner for Human Rights

OIC - Organisation of Islamic Cooperation

OPM - Office of Personnel Management

OPM - Office of Personnel Management

OSCE - Organisation for Security and Co-operation in Europe

OSI- Open Systems Interconnection

OTP - One Time Password

OWASP - Open Web Application Security Project

PAI - Partnership on AI

PAN - Permanent Account Number

PAN -Permanent Account Number

PEACE - Pakistan and East Africa Connecting Europe

PIL - Public Interest Litigation

PIR- Public Interest Registry

PNG - Papua New Guinea

PPP -Public Private Partnership

PPPs - Public Private Partnerships

PrepCom - Intergovernmental Preparatory Committee

PRISM - Planning Tool for Resource Integration, Synchronization, and Management

QUAD - Quadrilateral Security Dialogue

R&D - Research and Development

RIPE NCC - Réseaux IP Européens Network Coordination Centre

RIPENCC -Réseaux IP Européens Network Coordination Centre

RIR - Regional Internet Registry

RMB- Ren Min Bi

SADC - Southern African Development Community

SAIL - South Atlantic Inter Link

SCADA -Supervisory Controlled and Data Acquisition

SCO - Shanghai Cooperation Organization

SDG - Sustainable Development Goals

SEO - Search Engine Optimization

SIPRNet - Secret Internet Protocol Router Network

SIT - Security, Infrastructure and Trust

SMS - Short Messaging Service

SOC - Security Operation Center

SOC- Security Operation Center

SRI - Stanford Research Institute, California

SSD - Solid State Device

SSGC - Secretariat Study Group on Cyber security

Tallinn 2.0 - Tallinn Manual

TAT- Transatlantic

TCP/IP - Transmission Control Protocol/Internet Protocol

TEL - Telecommunications and Information Working Group

TLD - Top Level Domain

TRIPs – Trade Related Aspects of Intellectual Property Rights

TRP - Television Rating Point

TV - Television

UCLA- University of California, Los Angeles

UCSB - University of California, Santa Barbara

UK – United Kingdom

UN - United Nations

UN CEDAW - United Nations Convention on the Elimination of all forms of Discrimination Against Women

UNCIC - United Nations Centre for International Crime Prevention

UNCSTD - United Nations Commission on Science and Technology for Development

UNDP- United Nations Development Programme

UNECE - United Nations Economic Commission for Europe

UNESCAP- United Nations Economic and Social Commission for Asia and the Pacific

UNESCO - United Nations Educational, Scientific and Cultural Organization.

UNGA- United Nations General Assembly

UNHRC - United Nations Human Rights Council

UNIDP- United Nations International Drug Control Programme

UNODA - United Nations Office for Disarmament Affairs

UNODC- United Nations Office on Drugs and Crime

UNPKF- United Nations Peace Keeping Force

UPI - United Payment Interface

URL - Uniform Resource Locator

USA – United States of America

USD - United States Dollar

USSR - Union of Soviet Socialist Republics

UUV - Un-Manned Underwater Vehicles

VPN - Virtual Private Network

VR - Virtual Reality

W3C - World Wide Web Consortium

WB - World Bank

WCO - World Customs Organization

WFH- Work from Home

WHO - World Health Organisation

WICAN - World Internet Corporation for Assigned Names and Numbers

WiCyS - Women in Cyber Security

WiFi- Wireless Fidelity

WIPO - World Intellectual Property Organisation

WOMCY - Women in Cyber security

WSC- Women's Soceity of Cyberjutsu

WSIS - World Summit on the Information Society

WTO - World Trade Organization

WTO -World Trade Organisation

WWW -World Wide Web

XSS- Cross Site Scripting

Chapter one
Introduction

1.1 Background

The invention of internet by United States' initially in a small room for connecting devices and networks together for military purpose now has expanded globally catering the vast civilian population as well for their daily activities empowering individual, societies and boost economy. The virtual world created by linking devices across globe using internet is widely referred as "cyberspace" the term popularized by William Gibson (Cumming, 2014) that has not only redefined the information and communication technology (ICT), but has contributed towards an increasing digitalisation where almost all devices are being made "smart" particularly with IoT (Internet of Things) (Malik, 2017) in order to connect with cyberspace for enhancing its functioning to serve people. In the attempt towards digitalisation we are becoming dependent upon the information or data which forms the backbone in the functioning of cyberspace domain getting it recognised as the new oil (Arthur, 2013) and nations are in race to ensure their domination on data over other belligerent nations. The race in acquiring control over the digital oil is therefore leading the domain towards militarization and getting recognized as the fifth domain of warfare after land, air, water and space as nations making cyberspace as a part of debate and discussion in international relations (Seebeck, 2019).

The expansion of cyberspace from a limited user network from the United States' premier research establishment ARPA (Advanced Research Projects Agency) later renamed as DARPA (Defense Advanced Research Projects Agency) in 1972 to today's 21st century world of borderless global domain is due to the ARPANET (Advanced Research Projects Agency Network) programme that laid the foundation for connecting devices across globe in a single network (Tarnoff, 2016). The expansion of network has created a dual impact, where on one hand have removed the distance barrier in the world whereas on the other hand made a tool of disruption to global peace and harmony when exploited with malicious intentions by actors ranging from individual to state sponsored. As cyberspace is becoming one of the preferred medium for diplomacy with the foreign ministry officials understanding the impact of cyberspace on global users switching to private owned social media platforms like Twitter for conveying their message or sending protest notes over traditional methods like press conference, TV or next day newspaper as it seen to be more accessibility making it a "cyberization" of

international relations (Below et al., 2014), therefore incidents like posting or promoting of poorly fact checked misinformation including comprising of accounts by criminals to spread hate messages can lead to serious global consequences. Therefore the disruption caused using cyberspace is capable of influencing the global politics and relations between nations thereby urging the scholars to apply existing IR theories in understanding cyberspace that can help in creation of a global cyberspace governance as today's global digital village has been possible with contribution from multiple sectors and no single agency or organization can claim supreme authority on the global cyberspace(Eriksson & Giacomello, 2006).

1.2 Cyberspace Governance

The terms internet and cyberspace are often considered as synonym of each other although Oxford dictionary defines both as different where internet is helping to create the larger environment of 'cyberspace' (Coe, 2015) that is why cyberspace has been used for terms like cyber security, cyber crime and cyber terrorism to define as providing security of cyberspace, crime committed within cyberspace and large scale disruptive activities in cyberspace respectively. The internet is the connecting media that helps in creating the virtual world of cyberspace globally by harnessing the idea of first transatlantic telegraph cable laid on 1858 (Geere, 2011), and deploy advanced underwater submarine cables across globe for allowing more users to join from different region across globe.

While referring to administration of the continuous evolving cyberspace we prefer to use governance over government as the challenges and issues in cyberspace will not be solved by applying existing traditional national institution mechanism or government where it needs a relatively has less hierarchical order and polycentric in nature found in governance (Fasenfest, 2010); cyberspace requires transnational cooperation for multiple purpose like ensuring coordination between its standards developer, network operator ,online service provider, users, government and international organizations for solving the complexities while at same time retaining openness and interoperability. The need for a creation of global cyberspace governance are mainly for the following reasons:

- Cyberspace holds potential to multiply and amplify the quantity in the voices raised thereby often complicating any policy formulating decisions which further reduces exclusive state control in decision making process.

- It accelerates spread of information (both accurate and fake) like wildfire as the authenticity is verified much later thereby often leading to serious impact on peace and stability of a state.

- Cyberspace has enabled to transform traditional diplomatic services to be delivered relatively faster than before.

The digitalisation is contributing towards expansion of society where the hurdle of language is not a factor anymore owing to instant translating applications and at same time making vulnerable to multiple threats like that of DDoS (Distributed Denial of Service) (Emmons, 2021), where skilled attackers might use the flaws in application for getting access to those unprotected devices and further create problems. The targets of cyber attacks today do not remain confined to only one sector it varies from corporate firms to nations thereby making the governments proceed towards defining borders and apply defensive measure in cyberspace for both defence and offensive purpose.

Increasing attempts by stakeholders in influencing the governance further challenges on existing regulations and policies that are in force for administration of cyberspace based on various dimensions like technical, security and governance.

1.2.1 Technical Dimension

The advancement in technology has embedded words like 'WiFi' and 'cloud' in our everyday usage giving us opinion that the communications are happening in a vacuum or somewhere up in the sky, but in actual these clusters of user based networks are dependent on hardware devices that transmits data stored in a solid state device (SSD) located inside data center of a country might be far that travels to its destination following internet address or IP (Internet Protocol) to our device that can be either carried using long fiber optics cable laid underwater or through satellite. Similarly, the WiFi that enables us connecting wireless is actually backed by devices that convert data into radio signals which can then be received and read by other WiFi enabled devices.

The technical development has made it possible to introduce mobile phone revolution where the 0G (Zero Generation) that had cars with radio telephones mounted on them for basic voice communication then with 1G,2G,3G and 4G that made people connect to each other in this

virtual world of cyberspace much easier and presently with today's progress towards revolutionary 5G (fifth generation), which is expected to connect virtually human and machines with virtual reality (VR), Internet of Things (IoT) and artificial intelligence (AI) has initiated the competition between nations and nations are trying to bring the technical dimension under their supervision (Brenner, 2020).

The technical dimension holds key to functioning of internet as the we move closer to big data powered automated replies to our incoming mails for easy response (Bridgwater,2016), other stakeholders debate on the data security as the lack of governance framework and majority of technical contribution from private players has made them powerful enough to even pose challenge to governments besides belligerent nations also use private companies to their advantage in obtaining data.

1.2.2 Security Dimension

As cyberspace is connecting daily utilities of citizens in the form of cloud computing and IP based infrastructure that includes smart phones, computers, CCTV, internet of things (IoT) etc it brings unwanted threats alongside that includes surveillance in finding social life and interests by nation-states and also the compromised devices are also used by cyber criminals for spamming, distributed denial-of-service (DDoS) to both civilian and government networks. Since cyberspace is also officially considered as fifth domain of warfare after land, air, sea and space where USA's has announced its digital infrastructure as "strategic national asset" (Bain, 2009) and NATO (North Atlantic Treaty Organization) declaring for a full scale war in retaliation to attack on critical assets of any member nations in cyberspace asking for collective security (Paganini, 2016). Few nations have fortified their security infrastructure like the Great Firewall of China that implements a censored cyberspace for their citizens trying to confine or regulate people's online browsing. Other countries like North Korea its intranet named "Kwangmyong" (Williams, 2015) and Russia with its RuNet -Russia Network (Coalson, 2019) have also made their own set of rules and preemptive defence mechanisms on pretext of safeguarding their citizens including critical assets in case any cyber war is attempted on it. The offensive actions do include cyber hacks on belligerent nations using their cyber soldiers or APT (Advance Persistent Threat) on critical infrastructures famous being USA and Israel's Stuxnet attack on Iran's nuclear plant at Natanz (Nakashima & Warrick, 2012).

The security in cyberspace also includes preventing individuals from getting over

inclined or addicted to cyberspace as that can result in change of human behavior creating in cyborg referring to fusion of animal and machine explained in the book An Analysis of Donna Haraway's A Cyborg Manifesto (Pohl, 2019), security also includes preventing teen users from falling prey to killer games like blue whale and others that provokes in committing suicide and attempt to kill others, this type of games are serious concern for a nation if not stopped they can slowly be transformed to radical terrorists causing widespread chaos (Zaki, 2018), the cyborg and predator games might not be topic of direct concern for policy makers and IR scholars but can definitely serve as an easy prey for cyber criminals or attackers backed by nation states to ruin belligerent nation's future.

1.2.3 Governance Dimension

The governance dimension in cyberspace is referred to set of norms, rules and policies that pivots the functioning of global cyberspace, as cyberspace is a large interconnected network of sub networks connected using several protocols that are designed, developed and maintained by experts from multiple stakeholders. Similarly, various stakeholders having contribution in development and smooth functioning of cyberspace which includes government, international organizations, business community, civil society, technical community and academia are further involved in framing of governance proposals in form of models to enable a stable cyberspace.

a) National governments

National governments do not have sovereign control over cyberspace but increasing threats from the domain has led government in adopting higher security to safeguard its citizen's data irrespective of their view on administration of cyberspace of being managed by either multi stakeholder or multilateral form of governance. Government's role is like that of a fighter jet in the aerial defence where modern commercial passenger aircraft representing other stakeholders can only be used for reconnaissance purpose but for securing national assets against foreign belligerent countries fighter aircraft or government can retaliate.

Revelations have shown that cyberspace is used for global surveillance on citizens and political leaders (Shahwan, 2019) therefore nations are working towards ensuring their control that includes framing policies at both national and regional level to push for getting it implemented at global level as governments have limited options as the services majorly

available are provided by private players who mostly belong from other countries and implementing any strict laws becomes long process.

b) Business organizations / Private companies

Business organizations / Private companies are providing services to all users in exchange for profit and they have been playing role in governance of cyberspace with their terms and condition agreement that forms the primary guideline for do and do not for users who uses the platform. It is worth mentioning that private companies today own giant data centre and underwater cables that help the data to travel and they are also playing instrumental role in removing digital gap by deploying satellite, but the complexity arises when multinational companies who operates in both extremes like country which supports freedom of speech and one which denies makes difficult in abiding rules of the nation where it is operating and even its self censorship also is questioned (Corr, 2019).

c)Intergovernmental Organisations

Intergovernmental organisations both general and specialized comprising representatives of national government at international level are using cyberspace to connect with people and promote development across regions, thereby forming key components in framing regulations for cyberspace. Initiatives like the IGF (internet Governance forum) that was initiated under UN General Assembly (UNGA) to address issues related to privacy remains acknowledged as the first collective step towards eradicating crime from the cyberspace. At the regional level the alliances of nations often bring out regulations that serves as additional layer of safety for the users like the European Union (EU)'s GDPR (General Data Protection Regulation) that influences other regional organisations and countries to introduce a strong safety measures for protecting user data (Dayman, 2018), whereas at the same time regional organisation comprising authoritarian nations can be more strict in terms of granting basic rights to user in terms of freedom of speech therefore varying in cyber governance architecture in region.

d) Civil Society

Civil societies popular with general audience as Non Governmental Organizations (NGOs) represent the people's voice that are the largest section in society but are less heard, civil

societies are mostly nonprofit organizations and sometimes with international presence often funded by government agencies but acts independently from their control providing consultative role to governments and international organisations. NGOs take efforts to ensure both poor and rich are connected to cyberspace (Willmer, 2016), and they are among first responder to victims of cyber attack to ensure that the victim returns to use internet facilities in future but with more cautious and secured way.

e) Technical community

Technology forms the backbone of cyberspace and till date the development comes from them whether it is the introduction of mobile devices, IoT , AI etc since the early day's technical communities like the Internet Architecture Board (IAB) acted as a guide to ensure constant growth and innovation in the technology and undertaken roles for managing various Internet Engineering Task Force or IETF registries for providing solutions to operation and technical challenges arising in internet before nations initiated the effort to develop a cyberspace governance according to their own will. The technical community is constantly working in developing tools and utility which can make the working and experience with cyberspace better with every passing day.

f) Academic Community

Academic value as whole comprising academic community and academic institutions have a role in development of internet from beginning days and its management which today is referred as governance. Study related to internet has been introduced as disciplines in top institutions across globe as internet studies or internet science through masters and doctoral programme, the study of all proposed and existing models can help towards finding solutions to this increasing complex debates arising on governance of cyberspace.

1.3 Models for the global cyber governance

Cyberspace governance or cyber governance being an emerging topic has become an essential tool for daily life and stakeholders are trying to ensure safety of their interest, the increasing dependency of people on cyberspace and the threats associated with it invites the government to intervene in their attempt to ensure betterment of its citizen, this often attract positive and negative comments as countries have differences over others in cyber offensive and

cyber defensive capabilities besides culture and their vision of leading the nation. The difference in opinion often brings convergences and discourse related to application of suitable governance architecture that ranges from involving all stakeholders to handing the controls exclusively to government. The following are the various proposed model(s) of cyberspace governance:

a) Multi stakeholder model of governance

The multi stakeholder form of governance is an open ended form of governance architecture that supports open and inclusive process with cooperation and participation from all stakeholders to address the interconnected network of devices across globe. The internet is argued to be developed initially in a multi stakeholder approach at a room with efforts from government, private, academia and civil society that now has expanded across borders which now need transnational cooperation from all stakeholders.

Cyberspace has always been credited to be an open and borderless arena for everyone to explore its potential in that process often makes it prone to disruption if got compromised by cyber criminals or attackers. This rapid rise in the users and their devices are threats to society that comprises government, private companies, civil society and academia, which needs global attention and with passage of time it is seen that international organizations are also adopting multi stockholder approach where ICANN (Internet Corporation for Assigned Names and Numbers) did handover its control (Lee, 2016) and importantly the 2005 UNGA agreeing to proceed in multi stakeholder way for WSIS (World Summit on the Information Society) (Ermert, 2015), since then multi stakeholder model is being encouraged for efficient management of cyberspace leaving few authoritarian nations apart who believe in exclusive nation control over cyberspace.

b) Multi lateral model of governance (Also known as the state controlled)

Cyberspace being transnational in nature the governments are constantly trying to keep up to challenges by ratifying its national policies, forming alliance whenever necessary besides keeping cyber warriors popularly known as APT (Advanced Persistent Threat) groups to defend nation's computer network and also use it to attack if required, nations having advanced technologies have conducted cyber offensive operations like Stuxnet (Fruhlinger, 2017) and largest surveillance mission like PRISM (Planning Tool for Resource Integration, Synchronization, and Management) (Lempert, 2013) that which can be used as tool to penetrate into belligerent nation's network to obtain classified information as part of

espionage or spread propaganda to disrupt peace in that nation.

Cyberspace today has potential to disrupt real life functioning as it can now go beyond just shutting down of computers but can now halt transportation, economy and critical resources that are connected to internet, therefore nations as a part of preventive measures want it to be administered under government. The multi lateral model of governance is also filled with difference in opinion when democratic nations support open internet whereas authoritarian nations want a censored cyberspace inturn creating different threat perception towards cyberspace making it difficult to have a similar opinion for cyberspace governance.

c) The WGIG model of internet governance (de Bossey, 2005)**:**

- **Model 1 -** The first model proposed for creation of a Global Internet Council (GIC) comprising member representatives in an equal representation across all regions and stakeholders, besides the model also suggested measures towards ensuring less influence from any particular nation by proposing removal of the governmental advisory committee of ICANN.

- **Model 2 -** The second model suggests for creating a body similar to an IGF or Internet Governance Forum which will have participation from all stakeholders where all issues will be discussed and try for making solution.

- **Model 3 -** The third model proposes for establishing an International Internet Council (IIC) functioning as a multi stakeholder entity with national governments taking the lead roles in policy formulation upon discussion with other stakeholders' advice.

- **Model 4 -** This model supports the idea of creating a government-led Global Internet Policy Council (GIPC) where other stakeholders can be observers thereby replacing the US government's influential role in cyberspace governance and also supporting the creation of Global Internet Governance Forum (GIGF) which will have discussions involving all stakeholders.

d) Lawrence Solum model of internet governance

Legal theorist Lawrence Solum expressed with his study (Solum, 2008) that hybrid models can govern the internet better than existing institutionalism methods using his five

models of internet governance that are as follows:

- There will be no control of government in preventing data flow across their sovereignty and neither can regulate it. The model also says no single country's legal institution cannot make law for whole of cyberspace.

- The introduction of a transnational quasi private co-operations or international organizations which will be operating under joint treaties and agreements between nations.

- The communications protocols and software responsible for functioning of internet to be central to the formulation of governance architecture as safe running of internet is considered as primary importance.

- Granting more power to government where required particularly for dealing with internet related crimes.

- There should be a model focusing on the expanding digital market.

1.4 Cyberspace and International Relations

The implication of cyberspace is not just confined to everyday use but has started influencing international politics, transnational social relations and global economy. The increasing dependency of IR actors on internet and cyberspace where later has now managed to connect almost all equipments with it as IoT making it often referred as 'cyberization of international relations" (Below et al., 2014). This increasing blending of cyberspace on different components of IR has brought in scholars from interdisciplinary like IR, security studies, ICT studies and philosophy to understand increasing cyberization of IR to relate with existing IR primary theories like liberalism and realism alongside other theories like theory of constructivism and other critical theories that can help in creation of a global governance regime.

As debate between multi stakeholder and multi lateral form of governance is becoming a tension between nations scholars like Joseph Nye Jr has suggested for application of regime complex theory to initiate the framework of uniting nations to collaborate against mutual threats leading a path for nations to frame a mutually acceptable norm. The hindrance that come in framing an uniform cyber regime includes increasing cyberskeptics who stands firm that the threats from cyberspace are not much and it is not capable of causing physical harm to anyone it

is just a trick to divert form real world challenges thereby ignoring threats to critical infrastructures as well (Rid, 2013).

1.4.1 Existing regimes

There are already several exiting collaborations where nations are maintaining alliances to ensure their national interest, threats like child abuse and cyber attack on civilian resources can be added to make it more effective as the alliance is already an existing framework.

- The Five Eye intelligence sharing network comprising United States, United Kingdom, Canada, New Zealand and Australia working actively according to revelation made by NSA whistle blower Edward Snowden (Gallagher, 2018).

- Establishing hotline between nations that are used to prevent escalation of any troop aggression by either side can add cyberspace.

- Existing measures like the Wassenaar Arrangement works towards ensuring transparency in sharing of arms and monitored dual use technologies can keep a constant upgradation to the potential cyber offense utilities like artificial intelligence (AI), Big Data etc as many applications are now being exploited with their dual use nature (Cross, 2018).

- The Tallinn Manual (Tallinn 2.0) established after cyber attacks on Estonia in year of 2017 on application of international law for addressing cyber warfare and aggression.

1.4.2 Cyberspace and geopolitics

Coined by Swedish political scientist Rudolf Kjellen the word geopolitics refers to influence of geography on determining the politics and relations of nations, in this digital age where cyberspace is transforming international politics with actors from different region trying to influence the control of internet also occasionally turning the domain to a theater of confrontation makes cyberspace a tool of geopolitical conflicts.

As China has started to counter the US dominated submarine cable lines by establishing its own cable lines using its state owned Huawei Marine (Qingqing, 2019) aiming towards a digital silk route has led to increasing race for overseas bases. The three maritime choke points Luzon strait, Suez canal- Mandeb Strait and Strait of Malaccaare are also the choke points of submarine cables and these choke points are crucial to ensure global connection making them

always under contention (Halappanavar, 2020), it is quite obvious that having a landing ground will help in better maintenance for these cables therefore it is increasingly seen that nations are trying to get overseas bases close to the region so that the bases can further act as analysis centre as well besides ensuring security.

Having bases nearby the choke points can help in creating deterrence in multiple ways and further it can aid in securing the digital lines of communication which can also include establishing their own route to avoid such choke points. Once the dependency is reduced on these areas the nations can be on offensive mode as any action at the present situation could be a collateral damage triggering an immediate "splinternet" or balkanization of cyberspace where countries would be divided in major power blocks (Rajan, 2020).

a) Race in Oceania

The least populated region is seeing increase presence and investment by super powers like United States and China, interestingly this region has still one of the remaining four nations that recognizes Taiwan as legitimate China over People's Republic of China. The region is witnessing race in submarine cable deployment where on one side US and its allies are attempting to prevent Chinese entry to the region by investing heavily on submarine cables for connecting Oceania nations Papua New Guinea (PNG) and Solomon Island, Fiji, Samoa and Kiribati with Australia in a multiple projects, China on the other hand has secured the cable project of Solomon Island and supported creation of domestic internet cable system in PNG with advanced e-governance system in Vanuatu (Matsumoto, 2021) thereby turning the peaceful region into an underwater battle ground.

b) Race in Africa

China opened new front in Africa and came closer to US to boost its race in gaining control over internet network, Chinese using its state owned Huawei Marine Network telecom supplier has established various key submarine cables that includes 6000 km undersea submarine cable network between Fortaleza in Brazil and Kribi in Cameroon in association with the South Atlantic Inter Link or SAIL (Hardy, 2018) and has announced partnership between its another

state backed China Telecom Global with Angola Cables to establish link from Asia to Latin America which will connect members (China, South Africa and Brazil) from BRICS (Brazil, Russia, India, China and South Africa) through South Atlantic Cable System (SACS) (Tredger, 2020). US which once had control over this particular region is now finding itself in defence as China is coming closer to it and using its debt trap policy China has managed to reduce US influence (Kinyua, 2021).

c) Race in Asia

Asia has been a key interest for superpowers over years which can be understood how USA and its alliance spying on Asia to keep check on its competitor China and balance Indo-Pak ties besides maintaining presence at Hong Kong, Philippines, Malaysia, Indonesia that extended to Pacific from its base at Guam, where it maintains cables to Palau extending connectivity to Australia, New Zealand more appropriately to ANZUS (Australia-New Zealand-US) partner. China plans to counter the US's moves with venturing in Africa and Latin America region alongside using Pakistan to initiate digital silk road through PEACE (Pakistan and East Africa Connecting Europe) project that is being executed by Huawei Marine which will connect China from Pakistan to Djibouti, Egypt, Kenya, South Africa, France, Seychelles (Fouquet, 2021).

Asia also has India playing a significant role with one of its largest private player Reliance is now deploying submarine cables to reduce dependency on international sources (Basu, 2021), this deployment of submarine cable by India led company will lead towards creating a digital NAM (Non Aligned Movement) by refraining in joining any power blocks of splinternet cyberspace and also helping other smaller nations to join the digital NAM.

d) Race in Arctic path

The melting of polar ice caps in Arctic with global warming is perceived as another upcoming area of contention with its potential of becoming a strategic shipping that is not bound by any treaty which unlike Antarctica that is dedicated for peace and scientific advancement and not military use under the treaty of Antarctica 1959 (Hirji, 2015). Nations are trying to join the Arctic council as members for their chance in exploring the region, most interestingly being China although being distanced over 900 miles from the Arctic is now calling itself a "near

Arctic" suggesting the Russia-China cooperation on Northern Sea as Silk Road on ice (Mammadov, 2020). This shift by nations like China and Russia towards Arctic route also can be a sign of dominance in cyberspace in creating their own network or a separate cyberspace comprising like minded nations by deploying new submarine cables to remove dependency on other existing cables, then after declaring offensive underwater attack on old existing submarine cables to disrupt functioning of belligerent nations.

1.4.3 Cyberspace and Election manipulation

Involvement of cyberspace in election process is not new where efforts were made by hackers to halt Nelson Mandela's win in 1994 which involved hacking into networks of election commission to get in details and also create chaos as it was the first time when black people got their right to vote (Plaut, 2010). It happened at time when not every user were connected to cyberspace now with more people connected to internet brings more impact in form of spreading disinformation campaigns and manipulate votes, the tactics used in such campaign ranged from using misinformation to paid commentators who sitting on a foreign nation portrayed being local and influence the minds of people in influencing election process across world, like 2016 elections where people in North Macedonian town of Veles created websites to spread fake news related to 2016 elections in support of Trump (Synovitz & Mitevska, 2020).

A study conducted by freedom house finds more than 15 nations has experienced influence of cyberspace in their election campaign that eventually affected their election outcomes as well even when machines are not connected to cyberspace titled Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy (Kelly, Truong, Shahbaz, Earp & White, 2017). Russia is considered to be proactive for their involvement in election hacking (Satariano, 2019), and their alleged interference in 2016 US election is not unknown anymore where it was alleged to be involved by hacking networks and running propaganda campaign. Interference included that of leaking classified documents that reported candidate Hilary Clinton of violating government rules by having private server while still being the secretary of state and misusing government position for Clinton family business at WikiLeaks an international non-profit organization (Stein, 2016).

1.5 Threats to cyber security and efficacy of global cyber governance models

Stakeholders including nations have already started forming alliances to safeguard their

interest in the virtual domain of cyberspace, the increased collaborations aiming towards establishment of global cooperation often gets impacted with challenges from local and regional level. As cyberspace is a network of interconnected networks any changes introduced in a particular network by a stakeholder either state and non state actors can impact global regulations, the challenges faced towards creating a global cyber governance model are as follows:

1.5.1 Challenges in existing and proposed model of governance

The lack of law and order in cyberspace suggest for it being a state controlled multi lateral model that is backed by several authoritarian nations like China, Russia etc that pushes for cyber sovereignty which challenges the very nature of the connecting media i.e. internet on the following:

- Cyberspace sovereignty and nature of cyberspace – the very basic nature of cyberspace that calls it a borderless domain gets challenged as sovereignty will lead to fragmentation of cyberspace with nations having their own cyberspace that might be cut off from the rest of world.

- Cyberspace sovereignty and human rights – implementation of state sovereignty will in a way deny the fundamental rights of individuals related to freedom of speech as nations will censor their content and later punishing them if deemed.

- Cyberspace sovereignty and involvement of stakeholders- introducing state sovereignty in cyberspace will deny any position to other stakeholders that are equally essential for a progressive cyberspace governance and address all the beneficiaries.

In the ongoing debate between two (multi stakeholder and multi lateral) forms of governance where the idea of including all stakeholders in the multi stakeholder model is opposed by authoritarian nations citing cyberspace as a state affair discarding the requirement for any institutional overseeing thereby denying other stakeholders their share, this viewpoint further challenges models proposed by WGIG and Lawrence Solum's model which suggests for an institutional oversee the challenges in cyberspace. The proposed models also does not share any course of action on its application over hidden areas like dark web that stands as hub of criminals for sealing illegal items and crucial data obtained by un-authorised access.

1.5.2 Cyber security challenges

In cyberspace even ensuring security becomes a topic of contention as it is viewed as a threat to individual's privacy and existing infrastructure of internet is largely based on sharing information and providing security making it difficult to address both at same time time as today's digital era including business remains largely dependent on data sharing (Mitnick, 2017).

Advanced nation having their secured communication network like USA's own secret networks JWICS (Joint Worldwide Intelligence Communication Systems) and SIPRNet (Secret Internet Protocol Router Network) (Weinberger, 2010), and Russia's intranet "Closed Data Transmission Segment " or CDTS (Gerden, 2017) which is used for ensuring national security have not been able to assure protection from threats like large scale blackouts and damage that can happen to critical infrastructure systems which are increasingly getting linked with Artificial Intelligence (AI). Nations can employ cyber criminals who have already shown of the potential in disrupting utilities, penetrating critical critical infrastructures, concealing their footprints for causing damage to the digital assets of belligerent nation's including targeting innocent civilians as well as disrupt international peace and stability conducting false flag operations (Cunningham,2020).

1.5.3 Regulating challenges in cyberspace

The existing legal frameworks are not prepared to address the complexities arising from ongoing advancements in technology where technologies are bringing revolutionary changes in daily life and at same time threatening with impacts that extends beyond online harassment and attacking. The lack of regulations for monitoring powers of tech giants like Google and Facebook are making them a larger player in decision making who are often making different policies for its users based on their region, like the WhatsApp regulation on their new data sharing policy excluded the European Union to comply with their GDPR (General Data Protection Regulation) guidelines for their business interest creating worldwide backfire to the company (Ahmed, 2021). Further it is also seen cyberspace is often used to conduct surveillance by nations over their own citizens making cyberspace to be often compared with George Orwell' work "Nineteen Eighty-four" first published in 1949 talked about surveillance and policing system.

Challenges in cyberspace regulations largely needs inclusion of threats arising to the

submarine cables that are actually responsibility in carrying the data across globe as these cables remain vulnerable to attack and if damaged there can be blackout in internet services, which will be no less than economic blockade as world is relying on digital transaction. Further alternate to submarine cables the low earth orbit (LEO) satellites are believed to fuel the space war with private players like Starlink launching satellite which can create global contention if it loses their control and clashes with other nation's satellite (Clark, 2021).

1.6 Literature Review:

The existing literature on global cyber-governance covers a range of issues focusing on multiple aspects of cyber-geopolitics, theoretical perspectives, and efficacy of cyber-governance institutions and case studies of cyber breaches that have had the potential to affect international relations.

Deibert Ron (2015) in his article titled "The Geopolitics of Cyberspace after Snowden" focuses on the surveillance of the world's most powerful signal intelligence agencies like NSA (National Security Agency), GCHQ (Government Communication Headquarters) and their allies over cyber activists or data thieves as according to him threat lies more from the government agencies than petty criminals. He pointed out in his work how a small scale information sharing network has been explored to make an infrastructure for whole planet. He identified three major trends which is modifying cyberspace i.e.: big data, state influence and control.

Jayawardane, Larik and Kaul (2015) in their article titled "Cyber Governance: challenges, solutions and lessons for effective global governance" gives an insight with its target audience being policymakers as how efficacy of cyber governance institutions be made successful and they raise two prime questions that *Who* should govern cyberspace, and *how*? The authors answer the first question by reviewing multi-stakeholder models of governance and for the second question they promote that cyberspace should be governed by a combination of both formal and informal approaches including capacity building measures.

Kenneth Oye (1986) in his book "Cooperation under Anarchy" address two very critical questions of international relations, 1) What circumstances favor the emergence of cooperation under anarchy? And 2) what strategies can state adopt to foster the emergence of cooperation by altering the circumstances they confront? The questions are answered by studying the variations among situations along three dimensions: the payoff structure states confront in a given situation,

the inclination of states to discount the future, and the number of states involved. Although the book did not have any intention in cyberspace but the model can be implied in cyberspace since today's cyber world is similarly complicated like the real world with many actors and stake holders trying to become the dictator.

Jospeh Nye (2014) in his very significant work on regimes for cyber-governance titled -The Regime Complex for Managing Global Cyber Activities published by Global Commission on Internet Governance in their 2014 paper series, builds up on the notion of 'regime complex' for better understanding of the issue. Regimes are like the accepted principles, norms and rules which stand as accepted rules and procedures that govern issues arising in areas of international affairs, whereas regime complex is a set of regimes linked together. Cyber governance does not have a single regime for its management, it is instead functioning with norms and guidelines framed by multiple institutions which may have a bearing on diverse aspects of technology, politics and laws interwoven together. A regime complex, by bringing in multiple actors also has the potential expand the areas of convergence and minimize the scope of disagreements.

Roy Jeffrey (2005) in his article "E-Governance and International relations: a consideration of newly emerging capacities in a multi-level world" explores the profile of international relations in the cyber era. He analyzes as how powers have evolved beyond and within national systems and explains about the role of e-governance in this multi-level order. The article does give some ideas on the expectations and possible directions for future governance in digital age where the involvement of transnational activity will be high due to technological advancement.

FireEye (2013) FireEye a network security company published a delivered a report titled "World war C: Understanding Nation-State motives behind today's advanced cyber-attacks" authored by Geers, Kinlund, Moran and Rachwald it depicts the energy and resources spent by governments in cyber warfare. The paper projects a comprehensive study on the various methods employed by governments in cyberspace to have an edge over the adversaries. The paper advocated the use of multi layered approach to uncover the attacker.

Azmi Riza(2015) in his article "What is a border in cyberspace" discusses the various challenges that persists in the international law that makes difficult for taking a legal action against the attacker who has done from a different country. The article gives various examples where it

raises question about the authority or power of law in making justice to cases which has a complex boundary issues based on the attackers and victim's geographical identity. He further urges everyone to stand united in cyberspace as it is a common place for all individuals.

DiploFoundation (2017) in their paper "Towards a secure cyberspace via regional cooperation" jointly with Geneva internet platform (GIP) provides an overview on the international steps initiated about Confidence Building Measures (CBM) in cyberspace. It focuses in identifying the factors for observing peace and security in cyberspace where it discusses the challenges related to applying of existing international law to cyberspace. The paper also does critical analysis of the existing international bodies like UN, ASEAN and their role in cyberspace alongside suggesting few measures for better cooperation.

Martin Moore (2018) in this book "Democracy hacked: political turmoil and information warfare in the digital age" explains his audience as how an election process is interfered by hackers to de-establish democratic processes; authoritarian governments are found to be behind disrupting democracy. The book discusses very concurrent issues like data mining, psy-ops, mercenaries, Silicon Valley, trolling, surveillance – and impact on users. As modern world is now becoming increasingly dependent on data where life has migrated online and existing laws are not able to cover what is happening in virtual world there is an urgent need to change the system otherwise it might be delayed as by then hackers under contract of authoritarian governments or moneyed elites will be able to exploit digital infrastructure in democratic system to influence global politics and elections which will then be leading way for an unprecedented swings of public opinion too.

The Global War for Internet Governance (2014) book by Laura DeNardis defines to audience from a multi dimensional aspects including technical, historical and policy making as how the borderless domain has become a place of contention with every passing day, author argues about the challenges that exist in framing the internet governance that largely includes powerful actors. The books attempts to address the governance challenges particularly the technical aspects that include control internet resources, setting up standards like file transferring methods that to a larger extent defines the need and role of private tech companies.

Edward Snowden (2019) in his autobiography "Permanent Record" gives full of surprises as how mass surveillance conducted by US government impacted privacy of individuals and he was

a part of it as system admin leading to what motivated him to try to bring it down. The book goes on to aware people of loss of privacy with even small uncalculated steps, he says that the techniques he exposed in 2014 still remain in place which ignited awareness among us that cell phones can track us even it is turned off and controls on microphones and cameras are not just with us alone. Snowden said how our searches in internet and footprints we leave behind becomes the metadata for future use. The book has managed to incite among internet users that if a democratic nation like USA can secretly spy on life of its own citizens then what about others.

1.7 Need and Importance of the Present Study:

The present study on cyberspace governance address the influence of increasing cyberization on international relations where nations are using cyberspace utilities to expand their outreach and influence global audiences, the internet enabled virtual network of cyberspace itself has several debates ranging from its functioning to governance where nations are increasingly trying to gain control to stay ahead over belligerent nations that has resulted in declaring cyberspace as the fifth domain of warfare after land air water and sea. Today when devices are getting connected to cyberspace for efficient functioning it stands threatened from cyber attackers that includes both non state and state backed criminals it is essentially required to address the cyberspace governance in order to ensure the domain is safe for innocent users and progress to positive development.

1.8 Objectives of study:

The study intends to cover following objectives:

1) To study the multi-stakeholder models of governance in cyberspace by analyzing role of international governing bodies (ITU, IANA, IRTF, W3C…) and private bodies like, (ICANN, IAB, IETF...).
2) To study the measures that can be taken for establishing a secured structure to growing interconnectivity of critical resources and civilian assets in cyberspace.
3) Geo political implications of cyber space.
4) To understand the public-private partnership in the cyberspace domain.
5) To examine the issues of disagreement on matters relating to cyber space governance
6) Study the diplomatic, IGO, NGO and CBMs undertaken by nations in cyberspace to

ease the tension of hostility in real world.

7) To study the approaches by nations related to multiple factors like- cyber penetration, cyber laws, cyber defensive and offensive capabilities are impacting road towards creation of a global cyber governance framework in cyberspace.
8) To analyze and present a suitable methodology for good governance in cyber-domain.

1.9 Hypothesis:

Hereby the following hypothesis has been framed in view of research proposal:

1. The rise in cyberspace activities has a direct bearing upon the national and international relations.
2. With increasing dependency on cyberspace there would be essential need of governance system which would prevent from colonizing cyberspace and securing civilian assets.
3. Existing cyber regulations are inappropriate to deal with emerging frontiers of cyber governance.
4. Cyber diplomacy can be a tool applied in cyber governance to deal with complex international relations in the virtual world

1.10 Scope & Limitations:

The study has been undertaken with the purpose of understanding the entire existing international Cyber Governance framework that is functional currently besides study will focus on the beneficiaries and bodies (stakeholders) associated with it directly and indirectly in order to provide a suitable model and methodology for governance that will help in creation of a framework for a uniform global cyber policy. The study will be limited to the analysis of existing data available online and books published for identification of issues and challenges in framing a suggestive global governance model in view of the limitations of field visits to major institutions during the current pandemic. Instead, online interviews have been conducted with experts from the domains and their views incorporated.

1.11 Research Methodology:

The main aim of the study is to understand the role of various actors and stakeholders associated with functioning of manmade virtual domain of cyberspace and how can a global cyberspace governance can be framed in consideration of preserving cordial international relations that will prevent cyberspace from getting militarized. The study has considered

advancement in technology particular in relation to cyberspace and their impact on national security and international relations for framing uniform global regulation.

The study has undertaken qualitative analysis of past and current events, to observe and identify the factors which hinder implementation of global cyber governance framework**.** Available public data has been analyzed, evaluated and interpreted alongside collecting first hand data (primary resources) by seeking opinion online from representatives of various stakeholders through unstructured interview by asking open-ended questions to seek deep insights on the understanding of the respondents.

Secondary data, collected through books, journal articles, research papers, research journal, websites, government data, non-profit agency reports, statistical data and information from media sources too has been included.

1.12 Scheme of Chapters

The chapters of this doctoral research are based on materials available in public sphere. This whole research is also supported by general experience in field of national security which includes cyberspace as a domain and engagement with additional peripherals of the domain. The terms like real world and civil society needs a clarification where real world is referred to the world where we live in whereas civil society is meant by different individuals and groups who have diverse opinions and suggestions related to cyberspace administration.

Chapter 1 – Introduction

This chapter discusses about the evolution of cyberspace and its governance as how the increasing digitalization and borderless nature has made not only nations to join the race for acquiring dominance and influence policy making but has led to creation of multiple actors who are becoming a factor in policy making. The chapter provides a broader outline of the thesis giving the objectives, hypothesis, scope and limitation, literature survey and methodological aspects.

Chapter 2 – Cyber Governance and International Relations –An overview

In the second chapter titled “Cyber Governance and International Relations” it discusses evolution of cyberspace to a domain of international relations and why cyber governance is essential at this world which is connected more by internet and less by landmass, alongside it

throws light on effectiveness of cyber governance institutions discussing on both multi stakeholder and multi lateral model of governance. The chapter also highlights as how scholars have viewed this domain and the impact it has on the management of the domain that is threatened with ongoing debates of "balkanization" and 'splinternet' between two giants USA and China and how ordinary users are being affected by it.

Chapter 3 – Role of stakeholders in cyberspace governance: Analysis of evolving global regimes.

In this chapter "Role of stakeholders in cyberspace governance: Analysis of evolving global regimes", it focuses on management of cyberspace and role of public and private entities in such issues and discus various diplomatic/IGO/NGO initiatives and CBM in cyberspace and their effectiveness in their goal towards framing a uniform cyberspace policy leading to peaceful coexistence of all in the domain and remove the threats arising from attempts of increasing militarization of it

Chapter 4 - Challenges before framing and regulating a global cyber policy.

This chapter "Challenges before framing and regulating a global cyber policy" deals with the challenges that comes to play when framing a global cyber policy, The chapter also discusses on advancement of technology and challenges coming alongside it besides how cyber criminals are gaining their advantage as nations are attempting to design their own internet by introducing sovereignty and dominate the governance of cyberspace including influencing policies.

Chapter 5 - Conclusion and recommendation

In the last chapter as Conclusion, the chapter will give concluding remarks with all findings put together and also recommend what can be the possible way by which cyber governance can be ensured in this digital world which is slowly getting converted into battlefield. The chapter will share models of the future cyberspace and ways to counter crimes including application of cyber sanctions.

Chapter – 2

Cyberspace Governance and International Relations

2.1 Cyberspace – New domain in IR

Cyberspace whose main component is internet was initially designed to cater the military is now the backbone to not only military but to civilian society as well. The limited user network is now a global area network which has no boundary or barrier where devices ranging from laptops, smart phones to IoT (Internet of Things) are getting connected thereby making people increase their dependency on it. Today no single agency or organization can claim supreme authority on the global cyberspace but can contribute to its development that has helped in creating a sense of global digital village that allows staying updated of all events happening across world and even participating despite being at a distance far from origin (Peng, 2018).

This increasing dependency on cyberspace is not limited to people alone but from government and other non state actors which resulted in not only been redefining politics and international security but has developed to become an element of diplomacy. This chapter will focus how cyberspace is impacting relations among nations in this digital era when

communications are now getting wired through internet and relayed by satellite or submarine cable with nations already initiating race to define borders and militarize the domain for both defence and offense creating in geopolitical tension in the world. The chapter further discusses about the various dimensions on which cyberspace is analysed like technical, security and governance, thus attempting to study the various factors that are responsible in creation of global cyber governance regime.

2.2 Cyberspace Governance

"I'm not sure what 'Cyber Governance' actually means!
We've conventionally used the term governance to describe relationship between citizens and the state, or more generally between a social group and its leaders… But I'm still somewhat challenged when I try to apply this *governance* concept to the vague and in-substantive digital environment. In the context of public telecommunication services or the cyber world, we could see the outcomes of a *governance* framework as a set of national legislated or regulated constraints that are applied to service operators. But even this definition is somewhat unsatisfactory. While many national regimes would like to think otherwise there is still a major set of activities that do not clearly sit within national frameworks." (Huston, 2020)

Geoff Huston
Chief Scientist at APNIC
(Asia Pacific Network Information Centre)

The debate over the writing of word "cyberspace" itself with some preferring it as "cyberspace" or "cyber space" i.e. with a space in between, while others use "cyber-space" might give us a glimpse to the complexities that revolves around cyberspace at large and governance of cyberspace in particular. The increasing digitalisation across world where 4.66 Billion people having access to internet till January 2021 (Johnson, 2021) and increasing everyday due to low cost internet plans being introduced in many countries has contributed in expansion of society where the hurdle of language is not a factor anymore owing to instant translating applications. Cyberspace is helping in achieving improved transportation, commerce and business giving power to anyone to obtain information and do trading bringing in competition helping user get more options and value for their money. The man

made domain is also leading to expansion of society by interacting with many stranger by eradicating the hurdle of language which often led to distrust and distance among people especially if they do not speak same language, eased now by real time translation services which at one side has made people to connect with people across globe at same time influenced changes in beliefs, ideas, political thinking and also holding potential to cause a rift with wrong translations resulting in unintentional hurting of sentiments. The relationships between people on cyberspace are sometimes found to be more intimate even from one whom physically living together and at same time this rapid growth in internet users who are not aware of the preventive measures gives rise to multiple threats like that of DDoS (Distributed Denial of Service), where skilled attackers might use those unprotected devices to create problems to their targets varying from corporate firms to nation further creating great challenges on regulations and policies that are in force for governance of this domain.

2.3 Cyber Governance: Origin and Evolution

The idea of cyberspace or network of connected devices that allows us to experience a virtual world is outcome of collective efforts by engineers, academicians, military and private entities that established the framework of cyberspace ARPANET by linking 4 computer nodes located at University of California, Los Angeles (UCLA), Stanford Research Institute (SRI), California, UC Santa Barbara (UCSB) and the University of Utah,Utah. This successful network of 4 computer nodes further drafted the new objective of expanding its outreach and during this phase it was only a side sided approach towards expansion and governance was not included for its management as it was only provided to selected user. It was in 1973 when ARPANET became successful in establishing connection to University College of London situated in England and Royal Radar Establishment in Norway stepping its outreach beyond United States (Cheng, 2016).

The development of a network from 4 nodes to a counting of 22 billion devices (till 2018) (Mercer, 2019) connected to cyberspace largely including computers, laptops and the internet powered IoT devices are an outcome of the principle of “Rough consensus and Running Code” which after initial birth of network was followed mostly by engineers and academicians who managed or governed the internet in a swift manner to pave way for today’s reality (Resnick, 2014). It all started in 1960 with MIT’s J.C.R. Licklider work (Licklider, 1960) “Man Computer Symbiosis” that gave concept of Galactic Network paving idea for making a network of

computers which will let all connected to share and access programs among them anywhere in world. Licklider's idea then pushed for creation of ARPA (Advanced Research Projects Agency) and appointing Licklider as head of research at IPTO (Information Processing Techniques Office) in 1962 while 4 years later US Department of Defence appointed Lawrence Roberts another MIT researcher who connected TX-2 MIT to a Q32 computer in California using a telephone cable which is known as world's first wide area network using packets and not circuit (Metz, 2012).

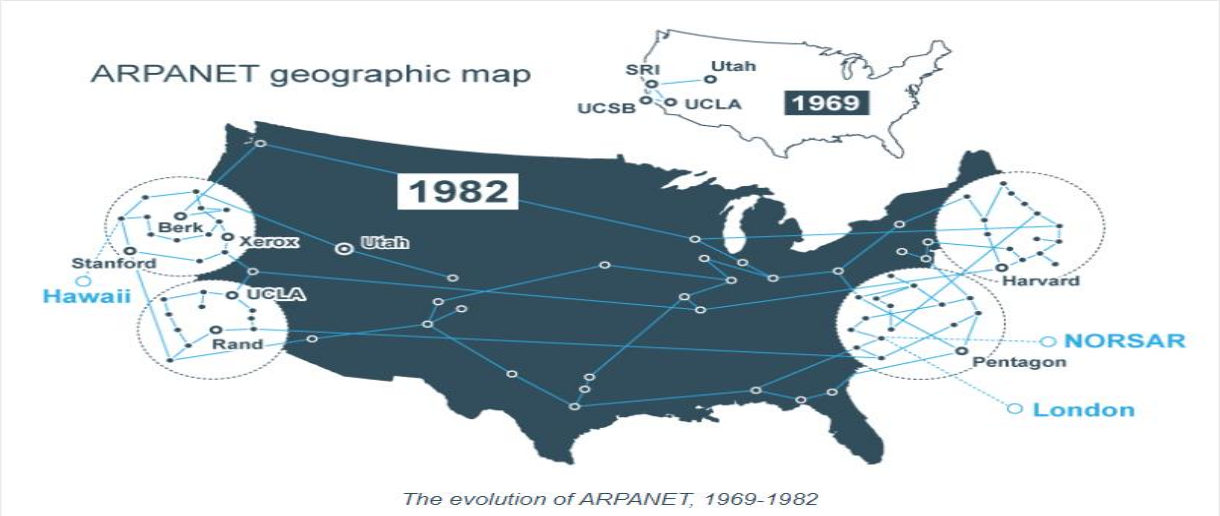


Fig.1. – The Early sketch of ARPANET (Source: The Daily Swig) (Leyden, 2019)

Some debate related to cyberspace governance which can be traced back to 1970s exist till date, regarding standardization where the rift continues with the architecture for governance of cyberspace is still not defined and efforts of IETF which can be considered as base for modern day experience also getting setback because of political conflicts within its body. Further increasing number of users and devices has brought in change of power related to decision making of internet governance where earlier USA had more number of devices connected to internet thereby pushing its authority as guardian over cyberspace, it got further strengthened when it established ICANN (internet Corporation for assigned names and numbers) primarily as nonprofit organization to look after the management of Domain Name System (DNS)[1]. The passage of time caused more complex scenario when number of user base increased in China and leading to formation of group along with other countries accusing USA of using its position in

[1] DNS is often referred as address book of internet where it works in handling names with corresponding unique numbers or IP address related to perspective domain names.

misusing non-profit body ICANN, US's influence in ICANN was made primary point of contention whenever debate for cyberspace governance came as it was accused to be influenced by US government and acting biased and not neutral since long (Hopkins, Easen & Young, 2000). Today when the race for dominating cyberspace comes it is between the two superpowers US and China who are employing various measures to control the governance of cyberspace that includes both technological development and influencing policymakers by giving incentives (Woo & Hinshaw, 2021) .

The debate between governments over governance of cyberspace has not given the other contributors equal opportunity to speak up until 2005, it was with initiative from World Summit on the Information Society (WSIS) led to decision of bringing joint partnership between governments and other stakeholders with establishment of Internet Governance Forum (IGF). This initiative included two of the main stakeholders the civil society and academia who are among the largest users in cyberspace and also addressed the rising voices from several nations of bringing ICANN under direct control of UN which was opposed by United States and its allies. IGF since then has been organizing annual meets to bring in a multi stakeholder approach where representatives from stakeholder can come together for suggesting ways in formulating plans for management of technical, security, governance and global dimensions of cyberspace governance (Ermert, 2015).

2.3.1 Technical Dimension

Cyberspace has given a notion in user's mind that the communication and other activities are happening in a vacuum or somewhere in cloud but in actual these clusters of user based networks are dependent on hardware devices that includes from a small semiconductor chips to large data houses storing all our data which are connected by long fiber optics cable laid underwater. The network established by all devices connecting to each other is based on practically three main areas which are Infrastructure, standardisation and the networking architecture that defines way of functioning of the infrastructures, this functioning of cyberspace owing to technical foundation has evolved over the years by contribution from technical community independently as well as backed by government which can be studied below:

a) Infrastructure:

The networking initiative of ARPANET (Advanced Research Projects Agency Network) to link multiple computers in a single network of 1969 has paved way for other agencies also to

design such networks in order to connect their peer computers for research. In 1981 National Science Foundation with its NSFNET (National Science Foundation Network) went to become backbone for establishment of academic research network across USA firstly by connecting all regional education networks established under CSNET (Computer Science Network) project, then to provide networking for computer scientists and later contributing in privatization of internet believing privatization would bring in new investment and progress to this technology for reaching to maximum audience. The NSF which handled key architecture is accused of involving other stakeholders like international organizations, private companies and nation states after it gave Network Solutions Inc subcontract to manage the internet's Domain Name System (DNS) (Salus, 1995).

Private companies were intimately part of consortium to give NSFNET the needed boost and it was led by Merit Network, IBM and MCI to re-engineer NSFNET resulting in connecting all research establishments in USA in a network (Goldstein, 2016). Since the transition from government to private it saw more development the first step happened in form of laying submarine cables for global communication which was based on telegraph model that was first laid in 1858 by Atlantic Telegraph Company (Lavallée, 2016). Today the internet is largely provided by private companies widely known as the Internet Service Providers (ISP) and categorised into a 3 tier model depending upon nature of service they provide. Tier 1 ISPs forms the most important who have invested in laying their own submarine cables and can provide internet without being dependant on government or other cables, the Tier 2 ISPs uses internet from Tier 1 ISPs to provide to their users via Tier 3 and if required the Tier 2 often peer with other Tier 2 ISP to provide internet and are mostly regional and national service providers. Tier 3 ISPs are dependent on others for getting internet and provide to end user which include households, local business etc. their services are confined to regions (Winther, 2006). The telecommunication standardization body of UN the ITU (International Telecommunication Union) suggested for adoption of a common approach for global internet architecture and contributed in establishment of International Cable Protection Committee (ICPC) in 1958 to look after billion dollar infrastructure that's responsible for looking after the submarine cable in ensuring the digital communication across globe which is believed to be only increasing with every passing days and the ongoing pandemic has made it rise further (Bannerman, 2020).

It is seen that technical requisites are essentially forming the element of geopolitical

contention with latest being the semiconductor chip that forms backbone of the circuits that power the utilities (Diwakar, 2021), presently when nations are increasingly trying to weaponise the cyberspace that includes the essential hardware components that makes resulting in manufacturing the products with snooping potentials (Robertson & Riley, 2018) it calls for wide research on the impact that other factors like electromagnetic waves and physical environment can cause in functioning of cyberspace. Research has found that even a part of a millionth Alpha particle present in packaging material can influence functioning of chips creating a soft error i.e. which does not leave back a trace for analysis (May & Woods, 1979) and also with another study finding impact of high altitude on electronic devices (Taranovich, 2018) needs to be now extensively researched to find that nations are not involved in direct war or confrontation over alleged sabotage caused by natural reasons.

b) Standardisation:

The formulation of a technical standard for implementing standard measure in internet came from the non government body, first from International Organization for Standardization (ISO) with its Open Systems Interconnection (OSI) standards around 1977, this was suggested by a group comprising computer industry representatives from UK, France and US who supported that a multilayered architecture can help in ensuring users across world to share and collaborate with each other and bring in more development to internet and world using internet (Zimmermann, 1980). OSI standard got support from companies producing computer and its accessories, national governments, academia and also US Department of Defense and was expected to be acknowledged as global standard by 1980s actually faded away by 1990s (Russell, 2013). The fading of multi layered OSI model can be credited to Paul Baran from USA and Donald Davies from England who invented the model of packet switching which worked on data to break into blocks or packets which can then be transported separately through various channels of a network where the recipient would combine them together resembling to its actual form. This method was believing to be more efficient than the earlier popular model of circuit switching where a separate channel was required for individual communication.

The modern day network remains rooted to launch of Sir Tim Berners Lee's World Wide Web in 1991 and Mosaic the first free web browser that gave user a graphic based interface in 1993 creating excitement among people and large thereby promoting to join this growing network, but the foundation happened in 1972 when International Network Working Group

(INWG) (Navarria, 2016) came to existence. INWG promoted the architecture of "datagram" which was planned on idea of connection less where there will be no relationship between sender and receiver which was completely a new architecture over the traditional circuit framework. The group met at frequent intervals and on 1975 applied for standardization to the International Telegraph and Telephone Consultative Committee (CCITT) who rejected terming as a model full of threats. Vint Cerf who was the Chairman of INWG left the organization to work at ARPA and later on design the architecture of modern day internet with Robert Kahn based on their "transmission control program" (Cerf & Kahn, 1974) module. Although there were support for OSI to be the standard but users started relying more on Transmission Control Protocol/Internet Protocol (TCP/IP) for connectivity, also ARPANET host protocol was stopped which meant that its affiliated users need to switch to TCP/IP for staying connected.

c) Networking:

During the initial developing stages, it was researchers that had control over governing bodies that governed internet protocols mainly being the ICCB (Internet Configuration Control Board) that later became the Internet Advisory Board (IAB) and IETF (Internet Engineering Task Force) which looked after the TCP/IP based networks. The governing bodies like IAB (formerly ICCB) and IETF primarily composed of technical scientists from various academic institutions, companies and government agencies; this indirectly removed the authoritarian control of ARPA over internet related decisions. IAB constituted various task forces and one being the IETF in which was responsible for creation of Internet Engineering Steering Group (IESG) as a body for standards (Leiner, 1997). The official need to bring in independence of state control came in when Internet Society was launched in 1992, with Vint Cerf as its President to bring in IAB an IETF under one body that would promote development of internet without much involvement of government and after the establishment of Border Gateway Protocol (BGP) in 1994 as advanced Exterior Gateway Protocol (EGP) for enhanced external routing using autonomous networks (AN) contributing to global expansion of internet without much focus on international agenda or considering government as a factor of developmental issue for global citizens (Leyes, 2015).

The increasing pace of population in virtual world on that period gave rise to the tension about the future as how to accommodate the new systems that will connect to internet as the address which are allotted to a system through Internet Protocol version 4 (IPv4) was found to be

insufficient in handling all devices in future. This led to the idea of Connection Less Network Protocol (CLNP) model which by then has also gathered some support in international community because of presence of government representatives in governing body of IAB, CLNP thus gave hope to solve the biggest upcoming problem related to issuing address to equipment as without address device won't be able to become part of this cyberspace (Katz & Ford, 1993) .

The IAB tried to prepare draft to convince then internet communicate about CLNP and their tireless efforts were misinterpreted by some section as an attempt of taking control over future of internet. Tension between IAB and IETF made end for CLNP and it was believed that TCP/IP and OSI will coexist for long time. In July 1992, IETF protested demanded newly framed Internet Society to support IETF and David Clark while speaking made a famous statement which is active even date "we reject: kings. Presidents and voting" we believe in: rough consensus and running code", thus making this meeting a hope for joy to all IETF engineers (Borsook, 1995).

By 1994, National Institute of Standards and Technology (NIST) halted GOSIP (US Government OSI Profile) and supported TCP/IP making OSI see a near end, whereas later on end to end architecture of the internet gave the new interactive platform World Wide Web. The competition between TCP/IP and OSI can be referred as foundation of internet and politics with David Clark's reference to kings, presidents and voting and modern day debate between two super powers (US and China) where both are trying to push for their version of technical architecture to ensure governance (Clarke, 2021). Since internet has its origin in American territory therefore a large part of important internet essentials was on United States and under their control through their private companies which included influence over cyberspace regulations and policies that largely remained a factor of global controversy. Recently Chinese government supported Huawei has come up with its New Internet Protocol which it believes can help to address the IP related issue (Sean, 2020) where the addition of new devices over passage of time is yet to address the increasing shortage for assigning IP (address) required for establishing communication, whereas many believes the protocol will be for implementing a state controlled system that will help to give China edge on global cyberspace with replacing TCP/IP internet protocol which is responsible for the flow of data between multiple networks standardized back in 1980s thus creating global debate for technical governance of cyberspace.

2.3.2 Security Dimension

The increasing human interaction with cyberspace has added essential elements like economy and security as a factor of concern since it is seen that data created by human in cyberspace is made use as commodity for revenue generation by companies and criminals. The digital society which is progressing regularly that has seen darker side like cyber fraud, crimes, terrorism which can be made equivalent to fact where internet is like a vehicle on the street (cyberspace) where terrorism and development are passengers in it, therefore to ensure that security measures are always applied to protect the presence of human and monetary means associated with it ranging from value of user generated data to digital currency. The security in cyberspace urges government to involve for bringing in adequate measures for ensuring that other insurgency like incident does not happen that can disrupt the aim of harmony in virtual world.

The aspects in defining security dimension does not remain confined to usage of tools and hardware but to use of digital economy as security of human and its data is often valued at digital currency as well at same time when we are keen in trying all newly available applications for getting more from cyberspace therefore the security of cyberspace and digital economy can be studied as follows:

a) Cyber Security

Since development in cyberspace comes largely from private players they hold more information than ever before where their interest in drafting of regulations for gaining control over infrastructure and other dimensions to have better control on cyberspace is a debate that needs proper attention for ensuring that security of ordinary users not stands compromised. The relatively late entry of government has made this virtual space witness urge of regulation due to entry of several non state actors that carry potential of causing widespread disruption on any nation's network. The government despite being a latecomer wants to take control on it to ensure safety whereas private players and other stakeholders are in opinion to include them in governance as they represent a large chunk on cyberspace both as contributor and user. Since cyberspace is officially now considered as fifth domain of warfare by many countries as many critical infrastructures of the developed nations relies on cyberspace, USA's digital infrastructure is already declared as its "strategic national asset" (Carr, 2016) thereby making it official that a full scale war or retaliation can be employed when its critical assets in cyberspace are attacked

similarly NATO declared cyberspace as one of its core task of collective defense and on 2016 NATO has recognized cyberspace as operational domain like air, land, sea thereby asking for enhanced cooperation across the alliance (Pomerleau, 2019). The increasing contention between nations brings in unwanted threats to private companies and users as nations often indulge in offensive attacks comprising data impacting privacy and race to dominate cyberspace can be seen in efforts to governance of institutions like ICANN nations as either part of power play or to ensure safety for their citizen which includes surveillance on their own citizen as well trying to gain control of its administration , this surveillance system is often compared with George Orwell' work "Nineteen Eighty-four" first published in 1949 talked about surveillance and policing system (Sharma, 2021).

Further there is no assurance that any genuinely purchased software or tools will not have backdoor access to state and other non state actors, ineffective regulations on espionage making cyberspace governance difficult even with efforts of IETF to review issues on surveillance, snooping and other privacy related matters. The need for surveillance as per states are generally a preemptive measure to thwart any large scale future attack, but for users its privacy which brings debate whether the security or privacy is to be acknowledged while governing cyberspace as US justifies its surveillance program as their effort to ensure that there is no repetition of events like 9/11 (Kurra, 2011). The cyber security rankings released by global and national level bodies also give us idea as how nations are increasingly implementing security measures to safeguard their digital assets.

UN's ITU publishes the Global Cybersecurity Index (GCI) a yearly assessment report upon conducting expert surveys to highlight the cyber security preparedness of nations and also contributing in increasing awareness among them. GCI was launched in 2007 and first survey was conducted in 2013 calculates cyber security awareness of 193 nations on 25 indicators which is based on its five pillars: legal, technical, organizational, capacity building and cooperation. GCI prepares question for each pillar and collects data through online survey then further consolation with its group of experts to frame the index. The report not only provides score or ratings it shows improvement and progressive status of the pillars of cyber security in the nations across all regions. The index also provides information on best practices performed by nations highlighting progressed achieved so that other nations can use ones which suits their

requirements resulting in global harmony in cyber security.

UN ITU' Global Cybersecurity Index GCI ranking 2017

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

Table 1 - UN ITU' Global Cybersecurity Index, (Source - https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf GCI 2017.)

UN ITU' Global Cybersecurity Index GCI 2018 ranking

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
United Kingdom	0.931	0.200	0.191	0.200	0.189	0.151
USA	0.926	0.200	0.184	0.200	0.191	0.151
France	0.918	0.200	0.193	0.200	0.186	0.139
Lithuania	0.908	0.200	0.168	0.200	0.185	0.155
Estonia	0.905	0.200	0.195	0.186	0.170	0.153
Singapore	0.898	0.200	0.186	0.192	0.195	0.125
Spain	0.896	0.200	0.180	0.200	0.168	0.148

Malaysia	0.893	0.179	0.196	0.200	0.198	0.120
Norway	0.892	0.191	0.196	0.177	0.185	0.143
Canada	0.892	0.195	0.189	0.200	0.172	0.137
Australia	0.890	0.200	0.174	0.200	0.176	0.139

Table 2 - UN ITU' Global Cybersecurity Index, (Source - https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf GCI 2018).

Similar type of cyber security ranking provided by Estonian government backed e-Governance Academy Foundation in their National Cyber Security Index (NCSI) ranking giving insight on the cyber security capacity of nations, highlighting best practices and areas for improvement. NCSI focus on providing constant progress which is not based on a yearly time period instead it is on an ongoing basis which includes evaluation of new evidence received about a nation and publishing within a month time. The NCSI follows a number of parameters for preparing index which involves network and data security, privacy and governance in nation besides many other aspects. NCSI also has website which gives overview of cyber security capacities of nations alongside a comparison feature to compare cyber security progress between two or multiple nations. The rankings are based on responses provided by respective countries therefore it cannot be considered as perfect way of analyzing cyber security strength further they do not consider digital economy as a measure while making the ranking.

National Cyber Security Index, Source - NCSI 2018.

	Country	**National Cyber Security Index**	Policy	Threat(s)	Education	Global	Digital	Essential	Eid & TS	Personal	CIRC	Crisis	Police	Military
1	**France**	**83.12**	86	80	89	50	80	83	89	100	67	60	100	100
2	**Germany**	**83.12**	100	100	100	33	100	100	89	100	67	20	100	67
3	**Estonia**	**81.82**	71	100	78	100	100	83	89	100	100	100	67	17
4	**Slovakia**	**80.52**	100	80	67	33	100	100	100	100	100	60	100	17
5	**Finland**	**79.22**	100	100	100	33	80	0	100	100	83	60	100	67
6	**Lithuania**	**77.92**	100	100	78	33	20	100	89	100	67	80	100	50
7	**Spain**	**77.92**	86	100	78	33	20	100	89	100	50	60	100	100

8	**United Kingdom**	**75.32**	71	100	100	100	0	67	89	100	50	40	67	100
9	**Switzerland**	**75.32**	57	100	100	83	20	67	78	100	50	20	100	100
10	**Czech Republic**	**74.03**	100	100	78	33	0	100	89	100	67	80	100	17

Table 3 - National Cyber Security Index , (Source - https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf NCSI 2018)

National Cyber Security Index, Source - NCSI 2019.

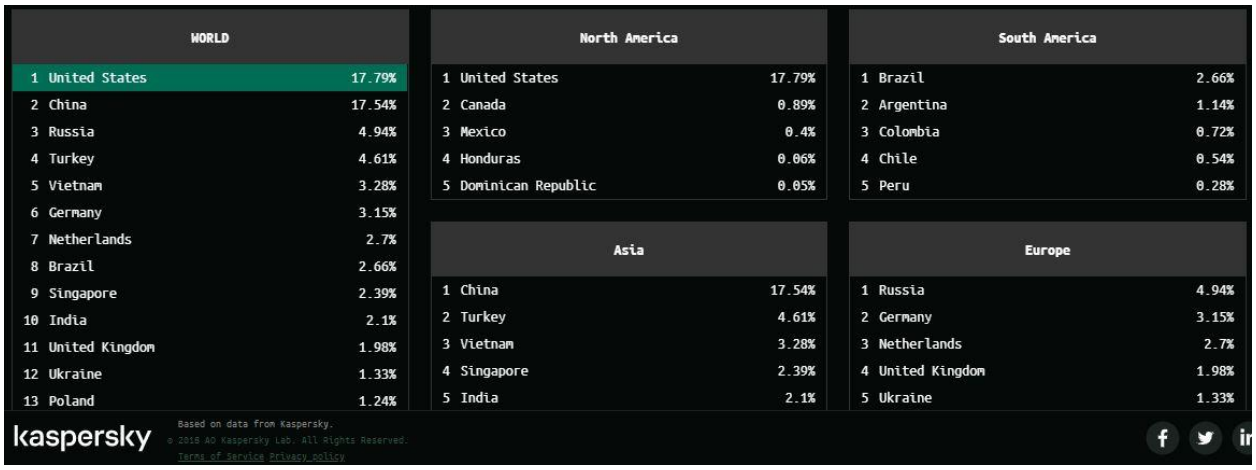
	Country	**National Cyber Security Index**	Policy	Threats	Education	Global	Digital	Essential	Eid & TS	Personal	CIRC	Crisis	Police	Military
1	**Greece**	**96.10**	100	80	100	100	100	100	89	100	100	80	100	100
2	**Czech Republic**	**92.21**	100	100	100	50	80	100	89	100	100	80	100	100
3	**Estonia**	**90.91**	86	100	78	100	100	83	89	100	100	100	67	100
4	**Lithuania**	**88.31**	100	100	100	33	100	100	89	100	83	100	100	50
5	**Spain**	**88.31**	86	100	100	50	100	83	100	100	67	60	100	100
6	**Poland**	**87.01**	100	100	78	33	100	50	89	100	100	100	100	100
7	**Belgium**	**85.71**	86	20	100	83	80	100	89	100	100	40	100	100
8	**Finland**	**85.71**	100	100	100	83	80	0	100	100	83	60	100	100
9	**Slovakia**	**83.12**	100	100	67	33	100	100	89	100	100	100	100	17
10	**Croatia**	**83.12**	100	100	33	33	100	83	89	100	100	80	100	100

Table 4 - National Cyber Security Index , (Source - https://ncsi.ega.ee NCSI 2019)

Private cyber security firm Kaspersky has its Cyberthreat Real Time Map that shows real time map on threats to nations that includes local infections, web threats, Network attack, vulnerabilities, spam, infected mail, on demand scan, botnet activity. The data is generated by Kaspersky antivirus which may be collected from its products installed at computer/laptops

which has large number of home and business users as its customers.

The site is updated monthly basis and mostly top 10 countries at any point of time includes, United states, china, Russia, India, United Kingdom besides other.



WORLD	
1 United States	17.79%
2 China	17.54%
3 Russia	4.94%
4 Turkey	4.61%
5 Vietnam	3.28%
6 Germany	3.15%
7 Netherlands	2.7%
8 Brazil	2.66%
9 Singapore	2.39%
10 India	2.1%
11 United Kingdom	1.98%
12 Ukraine	1.33%
13 Poland	1.24%

North America	
1 United States	17.79%
2 Canada	0.89%
3 Mexico	0.4%
4 Honduras	0.06%
5 Dominican Republic	0.05%

South America	
1 Brazil	2.66%
2 Argentina	1.14%
3 Colombia	0.72%
4 Chile	0.54%
5 Peru	0.28%

Asia	
1 China	17.54%
2 Turkey	4.61%
3 Vietnam	3.28%
4 Singapore	2.39%
5 India	2.1%

Europe	
1 Russia	4.94%
2 Germany	3.15%
3 Netherlands	2.7%
4 United Kingdom	1.98%
5 Ukraine	1.33%

Table 5 – Real time threat analysis (Source - https://cybermap.kaspersky.com/stats)

Other real time cyber threat monitoring sites includes

- Bitdefender Cyberthreat Real time
- Looking Glass Threat Map
- FOrtinet Threat Map
- Fireeye Cyber Threat Map
- Check Point Live Cyber Threat Map

The above and few other websites shows live map of cyber attacks which in most cases has USA, Russia, China, United Kingdom, India in their list of top 10 countries where they do shuffle in ranks among themselves with occasional exceptions, USA, China, Russia, France, UK, India are found to be on list regularly in DDOS threats.

b) Preventing digital manipulation to human life

Children who are more interested in science fiction thrills are recently found to be victim of cruel attempts made by games that are designed to risk their life, it is found that increasing amount of deaths are seen where there are challenges being circulated in social media which includes eating mouthful cinnamon, detergent. Social media has been found to be preying ground where children are persuaded to follow tasks that include turning on gas at midnight and in hope that they will become fire fairy next morning only to become victim of fire and burn their skin. Other online challenges include performing dangerous tasks which includes self-harm and draw

blue whale with knife in the arms and many more (Brooks, 2020).

Science fiction series gave rise to the concept of cyberspace and in recent past it has started to new concept of Cyborg combination of "cybernetics" and "organisms" which has been getting increased attention among internet users. Cyborg which was coined by Manfred Clynes and Nathan S. Kline (Madrigal, 2010) and is increasingly becoming popular as it is often depicted that using technology it is possible to make an ordinary human become extra ordinary powerful like superhero which might require just doing little engineering in brain or other related parts of body. Andy Clark's book *Natural-Born Cyborg* highlights the fact that it is not necessary to install hardware in human body even prolong dependency on technology might make all human as cyborg bringing in alteration in thinking as well as behavior (Clark, 2003).

The above actions when supported by belligerent nation can actually lead to loss of future leadership as weakening today's youth can ultimately weaken future of a nation and time when nations like China and France have already spoken about augmented soldiers to strengthen their power (Froelich, 2020). The word ethics and rule practically stands challenged in the race of supremacy where DARPA is already believed to be intensively involved in creating system to create brain machine interface that can create better human and computer interaction which will be effective in handling future threats at ease (Miranda et al., 2015).

c) Digital economy

The word coined by Don Tapscott in his best seller published in 1995 "The Digital Economy: Promise and Peril in the age of Networked Intelligence" which gave a glimpse how business will be revolutionized in virtual connected world. Today almost half population in online ranging from teens to their grandparents, virtual world has created a different world where user can make friendship with people across the planet where user created data are becoming more valuable thus disrupting old business models and giving rise to completely new. Companies like Apple, Microsoft, Facebook, Amazon, Baidu, Snapchat are constantly trying to secure online business from evil eyes and resulting them becoming main digital giants who have redefined way of business with their innovation and technical expertise. The cyberspace at large

facilitated opening up of markets like domain names, customized software this also challenged existing currency systems in place with digital currency like Bitcoins. Digital economy has joined with daily essentials like cab services, hospitality or delivery services making it a huge storage of user generated data which stands later as valuable remainder since it has much depth information about that person using that service. Survey by Bank for International Settlements (BIS) finds nearly 80% of world's banks are working in developing digital currency this has increased after Mark Carney the Governor of Bank of England has suggested that only digital currency can challenge Dollar's monopoly (Inman, 2019).

Tech giant Facebook announced of its ambitious project Libra in 2019 (Paul, 2019) to introduce its own digital currency that can be used by its users which now stands more than a quarter of world's population for paying against services from face book and its other subsidiaries / partner agencies or to another user. Facebook supports its move for introducing Libra digital currency for unbanked people and it intends to use as a floating currency like any other national currency but with a clear intention of not interfering or indulging in competition of any form with nation's currency system. The digital currency released in a global platform like Facebook has potential to disrupt global financial architecture as it can be used for money laundering and unintentional weakening of local currency where it will be used for instance, Facebook's Libra when sold in India by any outlet in Indian Rupees is exchanged for Libra need to be traded will be acceptable to Libra's reserve leaving impact in local currency. The increasing distrust on Facebook not only delayed the project but received setbacks from its initial plan of being used as a mainstream crypto currency that would have been used as legal tender for both online and offline with a much limited form which will be backed by dollar and not individual than planned before under a new team called Diem Association and currency will be called Diem from Libra (Ha, 2020).

The Chinese government has also started promoting use of its digital currency under Digital Currency Electronic Payment (DCEP) scheme which aims to implement digital Yuan as a substitute for US Dollars and China for that has been slowly taking steps since 2015 when Yuan got recognition of being considered as reserve currency across globe which now has 2.02% ahead than many other nations (Cheng, 2020). Using its ambitious Belt and Road Initiative (BRI) China has managed to push Yuan in several countries making it to be used by 7 African countries as its reserve. China's use of their Digital Yuan and being increasingly suggested to

join by other merchants including international to support the digital Yuan that China designed making it world's first digital wallet under a state-owned central bank which will work exactly like cash except it is on mobile phone with feature of NFC (Near Field Communication) allowing it to be used for offline payment as well and it is also believed to fuel the Sino-US digital war (Tang, 2020) . China went ahead to revolutionize the digital currency by announcing this will help government track transaction to counter challenges like money laundering and counterfeiting whereas world sees this as an addition to existing state surveillance methods. China has further managed to introduce it to American franchises such as that McDonald's, Starbucks and Subway to become tender joint station for digital Yuan's penetrating into global economy slowly making it a contention for cyberspace governance.

2.3.3 Governance Dimension

The approach of making a global standard is not strong as one international institution can adhere to one whereas other regional body can come up with their standard with aim of promoting their own regional business is a complexity in framing cyberspace governance.

Cyberspace initially was considered a matter of *low politics* which meant that cyberspace does not stand as factor for national interest, core institutions and decision making related to the state; the *high politics* (Cavelty, 2008) group included nationalism, political participation, conflict , violence and war but the impact of penetration cyberspace has done in life of every individual and nation by challenging the existing traditional power politics, national security, borders and boundaries has forced it to be considered as a factor of high politics in order to preserve national security and international relations. Today cyber attackers are sometime criminals attacking alone or groups having state sponsorship to wage a war on the other country's infrastructure and bring shame on the target state's cyber defense mechanisms, thus creating a situation nothing less than chaos in international politics with nations accusing each other of its alleged involvement.

The need of consideration or step for negotiation on infrastructure and regulations over usage of ICT tools stands a long standing unfulfilled agenda. The path towards governance was initiated by identifying the challenges and bringing concerned group or stake holder. The IETF (Internet Engineering Task Force) established in 1986 (Arkko, 2016) can be referred as first

initiative for cyberspace governance, since IETF required to meet and solve in challenges this created the Internet Society and IANA (Internet Assigned Numbers Authority) . The IANA was constituted as a standard organization which will look after IP address across world, which is now overlooked under ICANN that was formed under US department of commerce later making it a multi stakeholder run private entity. As expected the advancements did help in transforming business, education, healthcare and also e-governance system to help in citizens avail all government aids without any hassle but this increasing advancement has added to complications because of an absence of uniform cyberspace law and regulations which not only compromised user's privacy but nations often used at their advantage to wage attacks on belligerent nations which can be studied as follows:

2.4 The existing and proposed cyber governance models

2.4.1 Multi stakeholder model of governance

The multi stakeholder form of governance is an open ended form of governance architecture that supports open and inclusive process to address the interconnected network of devices across globe. Multi stakeholder format is considered as suitable way to address the issues that will arise due to increasing rise in users to cyberspace and also users are increasingly getting relied on it for economy and other daily activities urging it for a wider cooperation and participation from all stakeholders. The internet was initially developed in a collaborative multi stakeholder approach under efforts from government, private, academia and civil society initially in a limited network that now has expanded across borders which is still believed to require a transnational cooperation from all stakeholders in resolving all challenges in cyberspace.

Cyberspace has always been credited to be an open and borderless arena for everyone to explore its potential and now in today's time it has ventured into society so deep that this current generation is widely referred as digital age as now devices are connected to cyberspace for efficient functioning for making life easy and in that process often makes it prone to disruption if got compromised by cyber criminals or attackers. This rapid rise in the users and their devices are threats to society that comprises government, private companies, civil society and academia, which needs global attention and with passage of time it is seen that international organizations are also adopting multi stakeholder approach where ICANN did handover its control (Lee, 2016) and importantly the 2005 UNGA agreeing to proceed in multi stakeholder way for WSIS since

then other international organizations like Organisation for Economic Cooperation and Development (OECD) , Council of Europe (CoE) have also supported the multi stakeholder form of governance.

The aim of ensuring minimal digital gap will need more and more of the remaining people who do not have access to internet to be included in cyberspace and for that there will be several hurdles that will need inputs from all stakeholders for which multi stakeholders are considered to be applied for a longer time.

2.4.2Multi lateral model of governance (Also referred as the state controlled)

As internet was invented under the directives and initiatives from the US government they are believed to have influence over the domain owing to their status and also dominance of technology that are visible through their cyber operations like Stuxnet and largest surveillance mission PRISM. There are evidences of nations having offensive cyber weapons like flame and other malwares (malicious-softwares) which can be used as tool to penetrate into belligerent nation's network to obtain classified information as part of espionage or spread propaganda to disrupt peace in that nation.

Cyberspace today has potential to disrupt real life functioning as it can now go beyond just shutting down of computers but can now halt transportation, economy and critical resources that are connected to internet, therefore nations as a part of preventive measures have cyber warriors popularly known as APT or Advanced Persistent Threat groups whose work remains to defend nation's computer network and also retaliate in case of attack by other nations. Cyberspace is now in process of replacing paper currency with its digital currency and the first progress in this came from US based private company Facebook which was retailed with China's digital Yuan to prevent US from taking control of digital currency (Tang, 2020).

Cyberspace being transnational in nature the governments are constantly trying to keep up to challenges by ratifying its national policies and also forming alliance whenever necessary to address any threats, the opinion of leaders related to cyberspace on factors like politics, nationalism, religion etc. and its uses also decides the nature of approach towards cyberspace as United States having its critical infrastructures connected to internet focus on protecting it from adversaries whereas other developed nations like Russia, China focus on controlling the flow of information to prevent their people from demanding more democratic ruling. This difference in opinion creates different threat perception towards cyberspace making

nations to frame in different domestic policy and further reflecting similar in their foreign policy as well there by suggesting rules for cyberspace governance on same lines.

Interestingly, the nations who already have one of most censored internet like China, Russia, North Korea, Cuba, and other authoritarian nations support for multi lateral form of governance giving state the exclusive control of internet which is used to keep its people away from the liberal societies of the western world (Fidler, 2014). China and its allies have always been attributed in attacking critical infrastructures of US and to run propaganda campaign, which US and its allies have not been able to retaliate much as China employs a censored internet, the reason for China supporting multi lateral form of governance is to ensure that its citizens are not able to speak against government which in other democratic countries happen. Further United States's approach of liberalism or multi stakeholder is seen as failure by authoritarian states as private companies in US are powerful actors, who control large part of cyberspace and can influence public opinion which is not liked by authoritarian who wants to control the role of private players against holding monopoly ideal can be the 2021 China's fine on Alibaba group as part of anti monopoly rules (Wang, 2021).

2.4.3 The WGIG model of internet governance:

This models are outcome of the report published by WGIG the Working Group on Internet Governance (WGIG) widely referred as the WGIG model of internet governance comprising representatives from all stakeholders (de Bossey, 2005) and are as follows.

- **Model 1 -** The model suggested for establishing a Global Internet Council (GIC) which will be composed of equal representation of all regions and other stake holders. This model suggested for removal of governmental advisory committee of ICANN that can help in making the ICANN less influenced by any particular government. Further GIC can work in framing international internet public policy that will provide necessary guidelines related to management of internet resources which will include and not limited to root zone file, IP addresses thus making the technical bodies accountable to GIC. The GIC committee will also be responsible in ensuring coordination and cooperation for issues related to privacy, spam, crimes and breaches that can be made using cyberspace and other issues that are not addressed by any existing inter governmental organizations. The body will be made to act as facilitator for making in treaties, conventions and agreements related to internet dependant public policies besides providing guidance on

developmental issues which includes for ensuring every individual gets access to internet and promotion of multi lingual nature in internet.

- **Model 2 -** The second model which is based on ideas proposed by civil society participants suggests for enhancing power of ICANN's Governmental Advisory Committee (GAC) in order to address all concerns which are often raised by governments on particular issues. The model does not support idea of GIC like centralized body instead suggest for creating an IGF with participation from all stakeholders where all issues will be discussed and try for making solution. This model can be referred as one which by at large is being followed till date as we do not have any oversight mechanism and IGF has been place where all stakeholders discuss their problems and suggests for development.
- **Model 3 -** The third model proposes for establishing an International Internet Council (IIC), which can be of a multi stakeholder entity where governments would play a "leading role" on critical resources and policy matters after taking into account other stakeholders' advice. This model suggested for removing US government's stewardship roles leading to abolition of ICANN's Governmental Advisory Committee (GAC) and have broad global public policy decision-making authority.
- **Model 4 -** The fourth model suggested for a government-led Global Internet Policy Council (GIPC), with other stakeholders as observers that would replace the US government's influential role in internet governance and would have broad authority over global public policy matters. In addition, the model voiced for the creation of a World Internet Corporation for Assigned Names and Numbers (WICAN) which will be a private sector-led body bringing in a reformed and internationalized version of ICANN directly linked to the United Nations. The model also called for the creation of Global Internet Governance Forum (GIGF) which will have discussions comprising of all stakeholders.

Internet Governance Forum (IGF) was the preferred outcome from this initiative that was welcomed by all who believed that a coordinated effort is required from all stakeholders including government, academia, civil society and business to avoid cyber war and lead for enhancing partnerships and relations that can help in limiting politicization and militarization of cyberspace. IGF although left many actors specially authoritarians like China, Russia unhappy as they believe framing policies are work of government only. IGF first had meeting in 2006 and

since then happening every year that largely focus on creating in increased cooperation among stakeholders as per 2005 Tunis Agenda event for creating a new international decision making body but has not yet reached any consensus from all parties till date.

2.4.4 Lawrence Solum model of internet governance

Legal theorist Lawrence Solum expressed with his study (Solum, 2008) that hybrid models can govern the internet better than existing institutionalism methods using his five models of internet governance that are as follows:

- In his first model that is based on the central idea of independence supporting liberty where there will be no control of government in preventing data flow across their sovereignty and neither can regulate it. The model also says no single country's legal institution cannot make law for whole of cyberspace.
- The second model suggested by Solum is based upon nature of data flow which generally transcends national borders suggesting it to be managed by transnational quasi private co-operations or international organizations which will be operating under joint treaties and agreements between nations.
- The third model is based on concept of regulatory decisions that are based on communications protocols and software which often guides functioning of internet which can be found from Larry Lessig's work 'the code is Law' where internet's working is referred as the main factor that decides internet governance.
- The fourth model is based on regulations that can have government as authority where publications on online can be placed under laws of defamation and internet fraud can be brought under criminal sanctions.
- The fifth model can be based on economic drivers of digital market which will further decide about nature of internet.

The models by Lawrence Solum does discusses the technical infrastructure through established institutions like ICANN, IETF and calls in for strict regulations on issues like freedom of speech, child pornography and online gambling. Solum mentions as how institution that is trying to govern the internet is found running in itself a complex set of sub institutions, even though institutions like IETF, ICANN are at surface level but national governments of various cyber powered nations are trying to assert power for regulating the borderless domain.

Solum further suggests that cyberspace needs administration from a transnational quasi-private corporation created on the base of treaty and agreements considering cyberspace as an independent empire and not under control of any nation. Lawrence Solum argues that special institutions are always not necessary and administration of internet can be considered as a market for products and services where he feels market leaders who have reached top by providing better service at a lower rate have now gained power in market and national governments at their level can make necessary regulations to make policies and only if markets and national government fail then only institution can be created. Solum points that all issues in internet do not need regulation as making it challenges the basic liberties granted to all citizens instead focus on technological advancement to be given for developing the domain further and introducing any national or global regulatory framework can only weaken the progress of technological advancement. Through his model he further views that ideal model would be to incorporate all stakeholders and opinions making it hybrid that would be regulated by transnational institution that will support technological advancement and create in transparency in function making it an ideal market place.

2.4.5 Regulatory framework

The initiatives of regulations at national level and liberalization of telecommunication markets came after 1998s protocol of Fourth Protocol to the General Agreement on Trade in Service. While nations started working on their top level domains and ensuring regulations that can give them advantage the private companies in 1996 formed Global Internet Project (GIP) which focused on formulating governance mechanisms from the corporate benefit perspective (Lillington, 1999). When almost half of world's internet user were in US, the rest of world which whole accounted for remaining half of internet population eyed on ITU for regulations until the debate arose related to surveillance by states using internet leading a rising debate on multilateral v/s multi stakeholder form of governance which worsen after Post Snowden revelations, it is not unknown that US tried to control or regulate the internet age since beginning to ensure its global dominance as over the years it will be essential to stay connected with internet even if they have differences in opinion on other matter (Cavelty, 2008). Regional differentiations supported by ideological oppositions made it possible for only partial consensus to a uniform regulation from nations which led to formation of localized approaches on bringing in regulations to issues like cybercrime which was supported by corporate actors as they also were becoming target of cyber

crime attacks.

Many regional bodies and countries have made their own regulations even passing laws that can implement those rules. There are multiple regulatory framework and mechanisms in existence which is designed by actors who are more inclined in getting power to control cyberspace. Regulatory initiatives by various actors mostly states and international organizations can be traced back at the July 2002 ITU facilitated Intergovernmental Preparatory Committee (PrepCom) meeting which was attended by representatives from states and civil societies which discussed upon the need to frame a policy and regulatory framework to help in promotion of ICT for development (Outer, 2008). The passage of years and addition of more players to internet made way for different regulations and ICANN which was released from official control of US did progress bringing in new additions where domain names were allowed to be in other script as well (Yunker, 2011) under Domain Name System (DNS) making it a giant leap for users who speak other languages across globe thus giving hope that cyberspace is for all supporting idea of cyberspace for everyone and not just of only one language speakers (Jesdanun, 2010). After globalization of internet mostly after 1990s the saw rising of hybrid governance from both private and public spheres as policy makers not anticipating such overwhelming popularity at short span did not frame proper binding regulations giving space for private companies who were then leading it by making user connected to digital world. Initially internet was performing job of an advanced telecommunication systems by establishing fast exchange of information making countries to update their Communication Act or Telecommunication Act that also confined to US mostly as internet related development was mostly concentrated there.

2.5 Global Dimensions

Cyberspace is the newest member to the list of global commons after air, sea and space being only man made global common which is mostly under private payers that hosts range of assets including business /finance to nation's critical infrastructure urging nation to enhance their security (Raymond, 2012). A comparison of cyberspace can be drawn with air space where countries have adopted to norms of air management but have simultaneously made their own rules for declaring no-fly zones, no low flying zones, building infrastructure near airport etc (Dilipraj, 2018), only difference between them is cyberspace incorporates more global layers than domestic layers who are in form of internet providers, tech providers and service providers whom can as be regulated depending upon the country's interest or vision. Global regulation of

cyberspace is never a single time activity but an ongoing process which requires the government to stay updated with the technological advancements and formulate policies which can prevent any untoward to happen or give justice to any mishaps.

The global dimension of cyberspace also has to focus on decreasing the digital divide through initiatives like ICT4D that can help in creating a balance between the group of nations advancing with technology and others remaining behind, as the world is getting increasingly digitalised and also polarized where the virtual world of cyberspace is expected to be balkanized between USA and China led groups there is a need to promote ICT for development (ICT4D) for reducing the digital gap and ensure the basic human right of all in cyberspace.

2.5.1 Digital divide

The United Nations has pushed for safeguarding fundamental human rights of every individual of all its member nations in both offline and online where we are now heading. Many individuals do push in to include accept to internet as basic human rights which should be granted to individuals for utilizing the vast resources in cyberspace In reality it is found that access to internet ranges from one section of population having high speed connectivity and few do not have where many are in middle of the both who have limited access. This difference in term of access to internet is understood as digital divide and gap is known as digital gap which can be due to multiple factors like socio-economic or geographic factor.

The global digital divide if studied across country it can be found that in terms of access to internet as per statistics Africa has less than 40% internet connectivity where the rest of world has closer to 63% (Faria, 2020). Similar when seen in terms of speed and accessibility African region remains at lowest.

To obvious the digital divide there are factors that are:

Economy – to make internet available and with highest speed needs infrastructure which needs money either by government or by private companies can invests to do business but need to be countries as global power invests in digital assets to have control of nation as world is most becoming digital

Geography – geography plays crucial factor in everything even when it comes to internet as laying of cables depends upon geography. The larger the country more is infrastructure needed and lesser the size of country means less infrastructure.

Unlike landlocked country that is connected by underground cables the Island country depends on underwater submarine cable and if any of its cable gets damaged the impact is felt for long.

Terrain of land- the terrain of land if plain and accessible is quite easy to access and install infrastructure than if is covered with mountains or rocky prominent example being Nepal which is a land locked country but its mountain region makes it difficult to establish infrastructure hence Nepal still receives relatively slow internet than its neighbours.

Government restriction – due to security reasons government initiated shutdown in order to install stability and law and order in a particular region but that impacts those who are innocent tech enthusiasts as well. At same time there are authoritarian states like North Korea, Iran, China Saudi Arabia.

Internet kill switch – nations are progressing to develop their own version of internet as an alternate to protect their cyber assets and continue their own internet in case of foreign cyber attack. Russia's RuNet serving as example in this case.

While digital divide on the basis of national policy and censorship cannot be addressed cannot be addressed by any global regulation as the state's role must be respected when addressing ideological, legal and security issues in cyberspace but when it comes to bridge the gap between people who are not getting access to internet for connecting to cyberspace definitely needs global attention

2.5.2 ICT for Development (ICT4D)

The term Information and Communication Technology (ICT) is referred to use of technology for processing information and communication using technology like computer network, internet, satellite and other media. Access to internet started getting felt as an index for human development calculation upon understanding ICTs role as capability booster where it provided enormous support to humans in domains like healthcare, livelihood and education. ITU in 1982 established an Independent Commission for World Wide Telecommunications Development where they acknowledged the importance of ICT for development of society (Ellinghaus & Forrester, 1985). Development of ICT over years when social media started to bring people closer and also bring new means of business and communication then WSIS in 2003 and 2005 started to include in ICT for development convened by United Nations it was actually 20 years after ITU acknowledge the need. ICT4D mainly relies on using digital tools for bringing in development among people which at large helps that has helped in overcoming the

digital gap that did got created due to uneven access to technologies, one such example was installing mobile internet connectivity in developing regions to include them in fast evolving cyber world. ICT today has impact on political, economic, social, cultural and daily life of large chunk of population in developed nations who are dependent on internet for their daily activities. The increased initiatives by handful nations in developing often arming cyberspace as competition to its belligerent is again depriving the remaining world making it necessary to share the ICT for global development. Nations have come up claiming about their focus on using ICT technology as their tool for diplomacy, on 2018 at the International Seminar on Digital Diplomacy organized by Indonesian Ministry of Foreign Affairs in association with Pulse Lab Jakarta and DiploFoundation witnessed the keynote address by Indonesian Foreign Affairs Minister Retno Marsudi where she expressed that Indonesia now focusing on using digital strength in transforming their economy and empower people (Vacarelu, 2018).

2.5.3 Civil liberty and Human rights

Internet's potential was unleashed only after contributions from its users and not from a single authority whereas with passage of time and continuous addition of users there came in powerful bodies who tried to act as central authority to bring in administration in cyberspace. Now it is mostly few giant companies who have dominance on this borderless world which was believed to be a place for freedom for all. Tech giants like Google and Facebook have continued to dominate digital advertising networks for it almost becoming essentials to track user's movements giving them power to censor and carry surveillance as there is lack of competition and if any start up comes with potential as future competitor these giants acquire them by large amounts leaving users with no choice besides them for using social media and other platforms for daily works. This dominance by large giants also results in suppressing human rights activists who often share adulterated events in social media platforms and being top players they have power to customize the results for a query according to user and region they targeting.

United Nations General Assembly (UNGA)'s adoption of resolution 68/167 affirming that rights of individuals in offline must be protected online suggesting all states to review their existing regulations related to online mechanisms so that it does not resort to massive surveillance, collection of personal data and other actions that can causes violation of individuals' human rights (Joyce, 2015). Nations which are already divided in their opinions related to privacy and data protection where one group comprising Russia ,China ,Saudi Arabia

and other authoritarian countries continue suggesting that state control over internet is essential whereas other group led by US , UK and other democratic nations suggests for multi stakeholder form of governance in case of authoritarian the control over of data leads to large scale surveillance and depriving humans of their fundamental rights related to privacy.

2.6 International Relations Theories and Cyberspace

Although the impact of technology on international relations was experienced initially during 16th -18th century when countries especially European nations went for expansion and made colonies worldwide. Then in 19th century the telegraph system connecting the colonial rulers that ensured uninterrupted communication to aero plane, radio, TV all has started getting transforming IR, but the invention of internet in 1960s and rapid expansion of it started giving indication that by the end of 20th century it is all about cyberspace. The 21st century is now where all previously discovered technologies are connected to cyberspace for creating an interlinked virtual world that is influencing the global politics and relations between nations thereby urging the scholars to apply theories in analysing the role of IR theories in understanding cyberspace.

International Relations or as popularly known as IR theories helps individuals and scholars for understanding things through various dimensions making complex puzzles appear simple. The relevance of theories in understanding process was understood with Thomas Kuhn's The Structure of Scientific Revolution (1962) (Kuhn, 1970), which also highlights the evolution or arising of new theories when existing theories seems irrelevant or needs a polish to shine for fitting in the new brightness. Increasing complexities in global scenario have also paved ways for new theories from the two primary theories Liberalism and realism to understand the role that IR plays in analyzing the world which may vary from personal opinion and time depicting one theory to be more relevant that other.

2.6.1 Liberalism

Notable liberalist Immanuel Kant through his work of Perpetual Peace (Kant, 1983) gave opinion that to prevent war more nations across world should follow path of liberalism which suggests the states to be governed by citizens and they should find harmony to be better alternative than war contrary to the kings and others who hold power often try to fulfill their desires and wish of conquering more land leading to war. This idea of staying peaceful hold

strong for long and even till date which was even found in US President Woodrow Wilson's last point in his "Fourteen Points" (Fried, 2018) which he presented before US Congress during final year of world war suggesting for establishment of a group with like minded nations which lead to formation of the League of Nations in 1920 but the studies of liberal scholars like Kant and Wilson fail thereby calling upon scholars to add the unavoidable element of war in existing theory thus leading to rise of realism.

Applying the idea of liberalism in cyberspace has led to the creation of a multi stakeholder governance institution for management of cyberspace that recognizes efforts of all contributors and similarly the neoliberal idea can also be applied to ensure the security factor in cyberspace can be handled with creation of a global institution to oversee harmony in this contested human made domain. The multi stakeholder model which is supported by many including large section of civil society is outcome of liberal approach.

2.6.2 Realism

Realism theory which is based on opinion that it has no central authority to compel others to follow rule which reflects that only war and threat of war can make another state to follow orders of other thereby supporting their theory of war as more common and unavoidable than a prolong peace. The model for multi stakeholder model is often criticized by digital realists by suggesting that military, arms race and espionage can never be controlled by initiating cyber governance architecture. The digital realist scholar Judge Frank Easterbrook claims that there is no need of any special law and comparing it as "Isn't this just the law of the horse?" suggesting that any new law created is set to be outdated in a matter of five years if not immediately in couple of months. The realists suggest to implement law of real world in cyberspace only after law in real world is able to map all clauses in real world to make it applicable in cyberspace (Easterbrook,1996).

The balance of power theory (BOP) coined by Stephen M. Malt in his article "Alliance formation and the balance of power" (Walt, 1985) is one of the fundamental theory of international relations from realist view. The BOP system is a form of realist approach in which the power possessed and exerted by states within the system is checked and balanced by the power of others. Whenever a nation rises to the height of becoming a threat to others, the equilibrium is brought by the combined efforts of two or more actors of equal strength who are with same notion of the threat and are eager to safeguard their stand in the international politics

even if needed can go for war. The balance of power defined by Hans Morgenthau as "the aspiration for power on the part of several nations, each trying either to maintain or overthrow the status quo leads of necessity, to a configuration that is called the balance of power and to policies that aim at preserving it" is often , the balance of power over the time and transitions in international politics has undergone changes in its application with emergence of super powers who focused in spreading their presence and persuade them to join their power block across the world (Han & Paul, 2020).

There is a visible balance of power observed in the borderless cyberspace where all the digital devices are getting interconnected to each other and have been national asset too as many countries have their critical infrastructure like power, water connected to it thereby increasing its need of domination on it. That's why over the years internet is being used by nations as both for display of soft and hard power undertaking covert operations for collecting intelligence for commercial gain as well as to weaken the belligerent party by proving dominance. The race between United States and China is creating a splinternet (Flew, 2017) type of situation where US and its allies are supporting the multi stakeholder form of governance and China and its allies are pushing for multi lateral form of governance to push for their dominance in cyberspace.

As it is clear that balance of power is more of an accommodation and adjustment as it cannot satisfy every actor in the system, it suits perfect for preventing the irked entities in toppling the international order, and it does not bring solution in bringing peace completely therefore in cyberspace also we see rise of other non state actors who are often disruptive to that of nation states.

2.6.3 Constructivism

The other theory which is perceived to be in between two extremes being liberalism and realism is theory of constructivism. Theory of constructivism focus more on relation of individuals over entities like nations and states and notable scholar Alexander Wendt in his work Anarchy is what States Make of it: The Social Construction of Power Politics (Wendt, 1992), 1992 highlighted that relations between individuals and bodies like states are decided by diplomats, ministers and envoys representing it also he pointed how nation have different planning for individual nations considering one to be friend over other where example of US with Canada and Cuba is made similarly with that of US and its relations with UK and former

Soviet Union where both UK and Soviet Union having near equal military potential is treated differently.

Constructivist scholars argue over the human consciousness and their role in shaping international relations. Scholars focus on impact which is created by all actors to understand increasing governance architecture that is happening due to interaction of multiple state and non state actors at global level. Constructivist takes reference of internet groups like Anonymous, legion which is a group comprised of people from varied location but joining to form groups like anonymous aiming attacks on government and other entities which is believed to taking away freedom from online users. Famous attacks include 2010 Australian government sites takedown on protest to censorship proposal followed by efforts to support WikiLeaks where they mirrored latter's site so that it cannot be removed from internet easily (Somaiya, 2010) besides protecting servers where data is hosted. The displaying of potential to disrupt nation by above has made a fact that non state actors cannot be left behind when defining international relations and it is difficult to handle digital non state actors who do not have any official hierarchy or office located in real world to be handled with proper understanding of ideology and not merely over conventional methods. Notable scholars suggest constructivism for understanding digital threats with "symbolic politics as highly relevant for studying digital age security" (Eriksson & Giacomello, 2006)

2.6.4 Critical Theories

The challenges posed to established primary theories of liberalism and realism are provided by critical theorists who support idea of designing new methods to understand this world.

a) Marxian theory

Marxian theory finds internet development is similar to industrial revolution where internet is created by government using tax payer's money and now big companies like Amazon, Google and Facebook are making money from it. The development of social media and other initiatives which offered profits to get more financial aid for it does not offer anything to ordinary users who are making the companies or capitalists earn and giants like Google and Facebook become richer. Christian Fuchs describes in internet and class struggle that users are

similar to peasants or digital workers who are producing data which is then being sold by advertising companies for their profit by either sharing the producers pr peasants a small share or often nothing (Fuchs, 2014) . The online users who are either viewing posts, videos create traffic for websites and same way generating other user generated content for those platforms. Marxian idea of unpaid labor can be referred to nonpayment of any payment to users whose videos fails to reach the minimum view criteria which varies from 1000 views to 50000 views as per websites.

b) Feminism

The other section of society who claims to be left behind in international relations is women who suggest feminism theory which questions primary theories of liberalism and realism. Feminists point to fact that only few women are seen in decision making thus accusing IR to be more of masculine centric, urging need to focus on gender in promotion of international relation. Feminists focus on studying gender equality using different methods like case studies, quantitative and interviews.

Feminist scholars work for supporting women and queer persons irrespective of any difference for experiencing life full of harmony which they equally hope for them when accessing virtual world. A feminist version of internet is referred as place which will challenge existing hegemony of powers and apply alternate forms of model which will avail them to use power of cyberspace to address challenges that are faced by women and queer users online varying from bullying and other forms of harassments. The Association for Progressive Communications (APC) has already shared 17 feminist principle of the internet for ensuring rights of women and queer persons which using internet (Fascendini, 2015).

2.6.5 Regime theories

Cyberspace which was initially designed as an arena devoid of regulation has now invited for serious governance due to the increasing threats to the advancements of cyberspace. Joseph Nye Jr in his work (The regime complex for managing global cyber activities, 2014) (Nye, 2014) has tried to map the exercise of cyber governance using regime theories where he describes cyber power as a unique hybrid regime of physical and virtual properties. Physical properties include infrastructure, resources where virtual properties include the network created using physical resources. Cyber power is referred as collection of tools that aids in achieving desired outcomes with use of electronic and computer based information network systems. He further

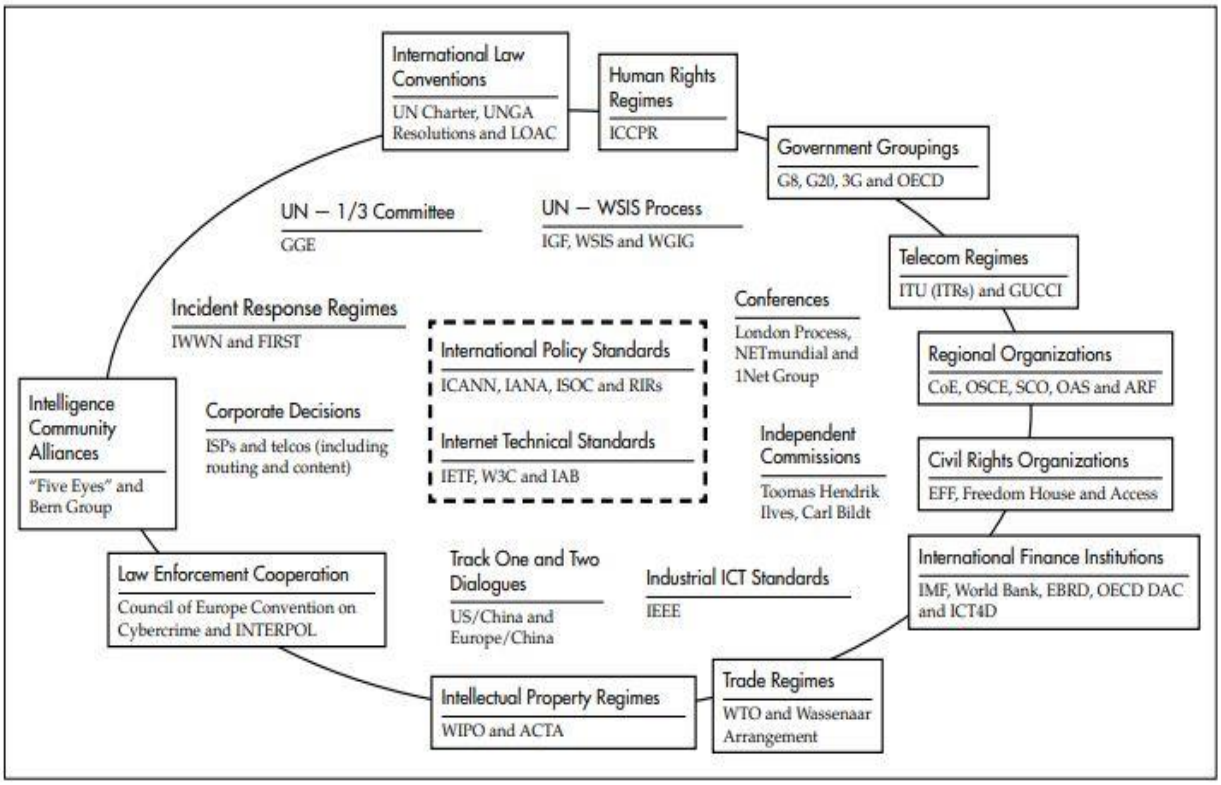
argues over the proclamation made by ideological libertarians that internet will bring end to government's control over citizens to its contrary internet right from the invention has active involvement of government.

Nye further points that in this complex arena of cyberspace governments and non state actors often cooperate for the race of cyber power which can be further implemented in attaining desired results in virtual world and also to influence outcomes in domains outside cyberspace which includes real world as well. He refers to the critical structure of cyber governance by highlighting the layers involved in it where the subset internet governance is designed by all stakeholders like governments, civil societies, private companies, academia and technical groups to frame rules and norms and other initiatives like naming and numbering activities primarily done by regional Internet registry (RIR)s and ICANN are merely a small part of the subset internet governance. The greater efforts in managing cyberspace comes from government within their national frameworks and their respective Computer Emergency Response Team CERT or computer security incident response team (CSIRT) bodies when threats arise to disrupt the internet of a nation. As ensuring security to an essential resource has mostly been a state subject to avoid unnecessary threat the same is supposed to be witnessed in cyberspace with increase in threats. Conflict over cyberspace today is not confined to defence and offensive actions it also includes as how a nation can convince or influence the way of governance of cyberspace.

The IR scholars having considered above attempts made by actors have tried in to apply role of regime complex for better understanding of the scenario. Regimes are like the accepted principles, norms and rules which stand as accepted rules and procedures that govern issues arising in areas of international affairs, whereas regime complex is a set of regimes linked together. Cyber governance does not have a single regime for its management, it is instead functioning with norms and guidelines framed by institutions ranging from small to large which can be understood by pic below, The picture below covers crucial elements of technology that helps in functioning and development of internet along with other issues like DNS and ICANN that are often referred as crucial are much inferior to actual complexities that impacts functioning of cyberspace, making us understand regime complex theory does not map all governance activities but it helps in understanding internet governance as a subset of cyber governance thus further helping in accessing existence of all the actors and their activities that ranges from varied

groups in initiating cyber governance.

The Regime Complex for Managing Global Cyber Activities Source - Joseph Nye Jr in his work The regime complex for managing global cyber activities, 2014)



ACTA	Anti-Counterfeiting Trade Agreement	GUCCI	Global Undersea Communications Cable Infrastructure	ITRs	International Telecommunication Regulations
ARF	Association of Southeast Asian Nations Regional Forum	IAB	Internet Architecture Board	IWWN	International Watch and Warning Network
CoE	Council of Europe	IANA	Internet Assigned Numbers Authority	OAS	Organization of American States
DAC	Development Assistance Committee (OECD)	ICCPR	International Covenant on Civil and Political Rights	OECD	Organisation for Economic Co-operation and Development
EBRD	European Bank for Reconstruction and Development	ICT	information and communications technology	OSCE	Organization for Security and Co-operation in Europe
EFF	Electronic Frontier Foundation	ICT4D	Information and Communication Technologies for Development	RIRs	regional Internet registries
FIRST	Forum for Incident Response and Security Teams	IEEE	Institute of Electrical and Electronics Engineers	SCO	Shanghai Cooperation Organisation
"Five Eyes"	Alliance of Australia, Canada, New Zealand, the United Kingdom and the United States	IETF	Internet Engineering Task Force	telcos	telecommunications company
G8	Group of Eight	IGF	Internet Governance Forum	UNGA	United Nations General Assembly
G20	Group of Twenty	IMF	International Monetary Fund	WSIS	World Summit on the Information Society
GGE	Group of Governmental Experts (UN)	ISOC	Internet Society		

Fig 2 - The Regime Complex for Managing Global Cyber Activities Source - Joseph Nye Jr in his work The regime complex for managing global cyber activities, 2014)

The complex issues that revolves around cyberspace includes response of nations that differ from real world where nations that protest against western states are not complete authoritarians but are on their path towards development and are concerned of their sovereignty. When it comes to democratic nations there are also distinguishable differences observed when it comes to privacy with surveillance as a factor. The involvement of regime complex might help in removing few challenges by bringing in a sense of cooperation or unity among nations who differs in few other aspects for example China and United States which differ with each other on human rights and censorship over internet data can join together for matters related to economic cooperation and on similar ground nations that differ or oppose each other on conduct of espionage or rules of warfare can cooperate on cyber crime and other issues like child porn. The mapping done by Jospeh Nye Jr. on regime complex indicates the crucial bonds that the cyber complex regime still being in early stage of formation has supported opinions on different IR schools which regime theory scholars believe can have better approaches that define and pave way for future of cyber regime complex which are as follows:

Realists as this set of idea is creation of powerful nations and only they can sustain it as they will be ones who will be befitted from supporting such initiatives of providing public assets and ultimately as their power will shift it will lead to difficulty in management like how the internet is starting to get divided after US has started losing its grip on it (Craig & Valeriano, 2018).

The liberal approach to cyber regime complex highlights interest of states for merging with others to bring in solutions to their problems which can further lead in reducing their expenses in solving a complicated scenario and difficulties. This approach defines why issues like DNS have received regime support and not on espionage (Netanel, 2000).

The constructivists approach which identifies how states act in their national interest and how they will be implemented as in the relatively new domain of cyberspace it is getting still difficult for nations to understand their interest and act accordingly. Once nations are able to make them self reliant in cyberspace they will act accordingly to their need which can call in for

joining or creation of groups as per their requirement (Stadnik, 2017).

Progress in international platforms do emit positive that regime complex can be future of cyberspace governance as Europe's Convention on Cybercrime or Budapest Convention has started getting in more supporters and INTERPOL or the International Criminal Police Organization has established functional centre in Singapore to look after threats arising in Asia Pacific. Nations like USA and Russia have paved in way for including cyber affairs in military hotline between two nations which is gradually being thought by other nations as well to limit the mutual loss incurred in a state backed cyber attacks. The suggestion of Joseph Nye Jr. includes that instead of a global agreements on cyber governance which is distantly difficult as international bodies ranging from small to large are yet to come on a decision about the model for governing the cyberspace where their opinions not only diverges from each other but contradict too which varies from integration to disintegration and also state and non state actors are both agreeing and disagreeing over topics bringing in mixed reactions in cyberspace over their clash of interest.

Bodies like ICANN remained under state control until 2016 and is accused to be influenced even now, the important factor like standards are finalized by non governmental institutions / non state actors but is believed governments still influences the proceedings, thus with larger differences at opinion and ideology yet at same time nations who share same opinion on certain topics like cyber crime and piracy where states can come together to deescalate tension as future of cyberspace governance seems difficult to predict and also a single regime overseeing cyber governance is not possible in near time due to increasing complexities. The above can help in paving way for regime complex might be an ideal solution as for immediate near future in preventing cyberspace into a battlefield and place for granted by internet users and policy makers due to prolong nature of a poorly unregulated place.

2.7 Cyberspace and International Politics

The transformation in international politics because of cyberspace is clearly visible and with addition of new sovereign states, international institutions, private players besides powerful non state actors the arena is getting more crowded and being a free space it is giving opportunity to rise of collisions or tensions. The increasing advancement has also led to rise in vulnerabilities

leading to more security challenges and more than government it is from unregulated private cyber actors who are dominating thus creating complexity in managing the cyberspace. Topics like cyber espionage, cyber attacks, hacktivism and internet censorship now has consistent presence as caption on first page of newspaper with increase in political involvement than merely technical concern as its mostly about dealing the political and geopolitical motivations that actually initiates the cyber war thereby it indicates that the end of era where cyberspace was referred being an exclusive IT specialists domain is no more as politics has a far important role in it.

The cyberspace being already a field of contention where countries are trying to develop and upgrade both defensive and offensive cyber capabilities to stay dominant, this competition has raised the formation of groups in the domain to form forces and often indulge in offensive exploration. The international relations are yet to address the rise of conflict and competition among different actors and stakeholders in the virtual domain where only academicians and civil society has mostly supported cyberspace to be a non militarized theatre to be used for peaceful purpose. The policymakers and defense community on contrary to academic and civil society perceive cyberspace as an extending ground of battlefield with focus on establishment of Cyber commands and prepare their respect cyber strategy first initiated by US (Lynch, 2018), this strategy allows cyber security policy formulation that initiates their control over their sovereign cyberspace territory when cyberspace gets demarcated till it will be applied to ensure that citizens are not intending disruptive actions by carrying out effective surveillance.

Cyberspace increasingly becoming complex with a space for political action where threats and progress are working together where systems being connected to interconnected network for obtaining information simultaneously preparing own air gapped network to prevent data from getting compromised (Nohe, 2018) . The low cost in waging offensive measures in cyberspace make it a preference for state and non state actors which calls in cyberspace to be reviewed by nation for its plan of classification while administering it. The cyberspace can be considered as smart power as it has elements of both hard, soft and economic added to it differing among states according to its need. How the bombarding and destruction of bunker and terrorist ammunition dump has not been able to wipe terrorist similarly spending huge amount in creating offensive tools or cyber weapons like Stuxnet will find it difficult to stop the cyber arms

race (Cheong, 2017). The cyberspace has become part of individual's daily life and states following path of espionage need to continue with their routine tasks in cyberspace it urges state to perceive cyberspace as an element of smart power which will help government to secure its citizen and also implement diplomacy laws and multilateralism. Today's complex virtual world needs both hard powers and soft power as implementing a single type cannot assure stability because hard power cannot control and soft power often gets suppressed.

The cyberspace is set to witness bipolar world even if undesired where China is set to provide equipments to developing and under developed nations with free or complimentary maintenance that adds up to its surveillance capability and United States which earlier had surveillance mechanisms over globe will find it difficult as Chinese gadgets will be coded in encryption hard to decode and if economy is considered then Chinese products being highly economical compared to low value when compared to USD (United States dollar) which comes with cheap manpower whereas in US payments end up in multiple times than its Chinese counterpart. The option where China will be seen in back foot is restarting of initiates like relief fund which helped nations to stabilize their nation designed on ground of technology where US will provide gadgets like China and also creating in IT parks across world which will have one consequence that USD might come down in value with these initiatives.

The ongoing situation where dependency has increased over each other taking examples where China needs USA to buy its product and USA needs China to lend money as the economy and stability areas tied together. Noah explains excessive defence spending will make US less competitive economically, worse it will encourage China to become aggressive itself, leading to an arms race and also allowing other nations to join the race for power supremacy once economy of these giant nation declines similar to Noah Feldman's idea in his work "Cool War: The United States, China and the Future of Global Competition" as how cool war is evolving in the world (Brauchli, 2013).

2.7.1 Cyber Diplomacy

The term *diplomacy* first coined in 1960s by Edmund Gullion, a former US diplomat, has been in use to portray the foreign policy in general to establish relation with other nations which has the ultimate aim of securing the national interest. Diplomacy which has multiple meaning and reference is referred to skills which help in managing international relations in different dictionaries (McGlinchey, 2017), interestingly have received addition of words to it for defining

its association to the environment like the word “cyber space” which has been added with suffix like cyber-crime, cyber-security, cyber-terrorism etc for defining the phenomenon attached to it, the word “diplomacy” has received prefix like para-diplomacy, NGO diplomacy, business diplomacy ,cyber diplomacy etc. Barrinha and Renard in their paper “Cyber diplomacy: the making of an international society in the digital age” has discussed the unfolding of cyber-diplomacy from an English School perspective in which the paper analyses the works of other IR scholars like Sending O.J, Pouliot V and Neumann IB, (Hurd, 2015) where diplomacy has been referred to as mere “constant” , which is more eager in studying the inception of power politics or the evolution of warfare. The Neumann I in his work says “diplomacy should be studied concretely, as a specific practice which is carried out by human beings acting inside a web of historically emergent norms and organization. Inasmuch as these norms and organizations seems to be changing, so does diplomacy” (Neumann, 2002).

Cyberspace has also brought in change in the language of diplomacy, earlier French language was referred to be the language of diplomacy when the language of romanticism became the language of diplomatic affairs between nations where diplomats stared learning French which later on initiated a competition between Eenglish and French in a race to establish themselves as the language of diplomacy (Crossette, 2001). Now cyberspace diplomacy has made the transition from sending pile of paper as letters to electronic mail (e-mail) and highly short and summarized tweet of less than or equal to 280 character, this shift in method of communication by foreign ministry officials of a nation have forced them tin using abbreviations to convey more response as part of diplomacy and send strong response besides obliging to the restrictions of social media platform Twitter which initially started with 140 character, now has 280 character limit. This increasing involvement of social media on traditional life has brought in changes like introduction of new words like netizens and giving new meaning to existing words like block, troll, surf which is getting updated in major dictionaries proving cyberspace influence over the language (Nordquist, 2020).

Diplomacy in social media particularly at Twitter is seen to be more effective as it has more accessibility where it is visible to global users which if undertaken using traditional methods like press conference would not have gone to users who are more active on social media than watching TV or next day newspaper or reading political updates. Twitter and other social

media platforms like Facebook now becomes factors in international relations because of common citizens increasing their reliance on cyberspace as a replacement of their traditional activities making it a “cyberization” of international relations (Below et al., 2014)

Cyberspace has been able to reflect the threats of real world in digital world with threats often having consequences on life, real world threats have been able to bring in a lot of change in international relations and law where use of nuclear bomb on any country followed by banning use of it and nations supporting it. It took more decades to come together to decide on signing on international treaty that will prevent further use of nuclear weapon on any country on 1963 when US, USSR and Great Britain signed the Limited Nuclear Test Ban Treaty, similarly other arenas than land like seabed and outer space that have direct impact on environment and lives has been added to the list where nations would not indulge in offensive activity. The 2010 Google attack has been able to change US government’s perception of threat arising from economic espionage and attacks on critical infrastructure has already shown impact that cyber attack can have on humans (Markoff, 2010). Thereby arising the call that asks is this the time to start treaty that bans using offense on such areas associated which are linked to cyberspace e.g. healthcare system and other critical infrastructures. The ministry of foreign affairs of every country now have started to put in effort to the cyberspace issues and constantly update itself in order to the be able to gear up to address the transforming nature of diplomacy in this internet age.

China has expected to supplement its Made in China 2025 program with China Standards 2035 which is aimed in spearheading global standards for next generation of technologies using its global influence on ICT related advancements (Kharpal, 2020). The existing bodies for standards are often doubted by China to be western nation backed groups and since there is already a competition in internet where China wants to ensure that other nations can start using Chinese made products, Chinese products often gets denied under western based regulatory bodies denying it citing threat factors. Chinese products till date stands as one of the most affordable in the world will be able to bypass all regulations after introducing standards like Chinese Standards 2035 which will definitely be backed by other friendly nations of China enabling it to give a stiff competition to other regulatory bodies established in same sector. China thus sees this technology as new weapon to colonize the world and rule it virtually and make developing nations weaker and their slaves as they have done in real world. A study undertaken by Australian Strategic Policy Institute (ASPI) International Cyber Policy Centre (Cave, Ryan &

Xiuzhong Xu, 2019) on China and its technological expansion across globe gives us deep insight on China's potential role in making global surveillance through its use of soft power. China's technological diplomacy has already been witnessed where they are providing high end devices including surveillance cameras to its friends across world and they would also be communicating to servers that might have access to China either on pretext of maintenance or with its hacking capabilities.

An example of diplomacy using cyberspace can be found in Make in India initiative of government of India that has brought in big companies to open manufacturing unit which will result in creating jobs and boost economy. Mobile device giant Apple announced opening manufacturing hub at India and it saw 3 Taiwan companies Foxconn, Wistron, Pegatron joining to invest in $900 million (Gaurav, 2020). This comes at point when the relation between China and US is undergoing tension and Taiwan is trying to get attention, participating in Make in India is definitely help in global attention and support specially from world's largest democracy when China is adopting aggressive role in acquiring land from India by claiming as its own. This type of increasing contentions between nations brings in element of diplomacy to avoid war as it happens in real world, similarly in cyberspace to curb tension which when arises the element of cyber diplomacy is seen active and Estonia already appointed their first cyber diplomat and set up first ever data embassy in Luxembourg indicating soon the world is set to witness a virtual sovereignty.

2.7.2 Cyberspace and Election manipulation

Looked by the policymaker's eye balancing giants and cushioning emptiness are not considered as equilibrium since the balancing will involve political risks and support for race to supremacy bringing in military, it is also true that state cannot sit back and relax in anticipation waiting for their agenda getting fulfilled, as it is the theory of the basic survival states that it is survival of the fittest (Lack, 1983) which refers that nation must prepare and be ready for war to preserve the balance and also preserve its own position in world politics.

After Russia was alleged to be involved in the US presidential election campaign where it was involved in hacking networks and running propaganda campaign, one such being leaking of classified documents that first reported of candidate Hilary Clinton of violating government rules

by having private server while still being the secretary of state. The emails leaked were from account of John Podesta's, chairman of campaign for Hillary Clinton. Hackers published those mails at WikiLeaks an international non-profit organization which publishes news leaks and classified information, the emails released contained information on Clinton family business by misusing government position (Stein, 2016). The involvement of Russian government involvement was proved when Department of Justice convicted Russian intelligence officers behind the hack of presidential election (Riotta, 2020). It was then found as how cyberspace can influence election process across world where machines where all voting machines are not connected to cyberspace.

A study conducted by freedom house finds more than 25 nations has experienced influence of cyberspace in their election campaign that eventually affected their election outcomes as well (Hern, 2017), the tactics used in such campaign ranged from using misinformation to paid commentators who sitting on a foreign nation portrayed being local and influence the minds of people. The Cambridge analytica scandal that used in personal data of Facebook users for mostly influencing election and politics without user's consent showed us how cyberspace can be used to manipulate election and another notable being the misinformation that was found during 2016 elections from the North Macedonian town of Veles, that created websites to spread in fake news related to 2016 elections in support of Trump (Synovitz & Mitevska, 2020). The use of cyberspace in manipulating elections cannot be restricted to only the above misinformation but if coordinated attacks are waged on networks in cyberspace can ensure to refrained people from voting which can be as denying people from casting vote

On most occasion information related to place and location of voting are spread using internet, if hackers can manage in to either change in the polling lists creating chaos among voters. This can be supplemented with high jacking traffic management system on roads or a fake weather report on the date of election. On early morning of Election Day, the critical infrastructure like water supply and electricity can be halted to prevent users from carrying their daily chores can add it to the benefit of the political party where it sees chance of votes to go against it.

Involvement of cyberspace in election process is not new where efforts were made by hackers to halt Nelson Mandela's win in 1994 as claimed by Peter Harris in his book Birth The conspiracy to stop the '94 elections in 2010 which involved hacking into networks of election

commission to get in details and also create chaos as it was the first time when black people got their right to vote (Plaut, 2010). It happened at time when not every user were connected to cyberspace now looking at today when people got connected using internet saw more involvement by cyber criminals in form of spreading disinformation campaigns and manipulation of voter's data. Russia is considered to be proactive for their involvement in election hacking where Russia is found to be involved in multiple regions like US, EU and Africa through its state supported agency Internet Research Agency that run disinformation campaign , in Africa in runs its propaganda from bases like Sudan, Madagascar and in EU Russia was found targeting voters from Britain, France, Germany, Italy and Poland whereas its involvement in 2016 US election is not unknown anymore (Satariano, 2019).

Fake news and misinformation had a great role in 2016 election after that world got cautious over using of social media and cyberspace as whole for manipulating election outcomes. This time in 2020 US presidential election the Washington post posted against Donald Trump before election which mentioned number of false or misleading claims the President has made. Though attempts were made this time also to swing the citizen which was seen through hashtags #mailfraud, #stopthesteal and gained momentum but was not allowed by social media to disrupt the democracy this time (Collins & Zadrozny, 2020).

It all started in May 2016 when Twitter started to add in blue level that placed disclaimer on its authenticity which received backfire from president trump with a threat of stopping twitter and accusing it of interfering in US election. Twitter further disabled the option of like and share from his posts. The relation between cyberspace and US election gained more complexities as there were questions raised on online voting as United States have option for online voting where applications like OmniBallot, Voatz are used in huge numbers even though researchers from MIT and Michigan University have voiced for possible chances of getting it tampered as in one application OmniBallot there was issues found with end-to-end verifiability (E2E) , that ensures secure voting and upon research it was further found that this particular application uses services from third parties that includes Google Analytics, reCAPTCHA and others (Miller, 2020). Even if the process cannot be hacked but the election remains vulnerable to cyberspace influence as misinformation on process getting hacked can spread over social media creating in chaos which needs to be addressed

2.8 Geopolitics and cyberspace

The word Geopolitics which studies on influence of geography on determining the politics and relations of nations with others was first used by Swedish political Rudolf Kjellen. The expansion of internet itself has included actors from different region who are now increasingly trying to influence the control of internet by making it an object of power rivalry between its stakeholders and occasionally turning to a theater of confrontation as well as a tool of geopolitical conflicts. The extension of traditional geopolitical rivalry in cyberspace is more a multi scalar approach which is by at large due to increasing digitalization. The issues and threats are no longer a topic of discussion for a small group of security council of nation but the whole country at large as unlike other domain where nations military are in picture to secure here in fifth domain of warfare all citizens and public critical infrastructures are exposed and prone to digital attack from enemy nation.

Our ever increasing reliance on cyberspace for social and economic activity is making it necessary for government to ensure security in domain as non state actors are harnessing this to develop their own capacities and challenge state actors. Elected representation of government and even criminals has started harnessing cyberspace for its profits. The delay in formulation of a global consensus and standard global legal framework stands unaddressed as advancement of technology is faster than accessed where existing international rules seems to be unsuitable for this domain. Additionally, lack of trust between stakeholders slows down these efforts instead raises tension in globe.

Communication in cyberspace mostly takes place over private owned submarine fiber optic cables which initial undersea cable carried only Victorian telegraph message now they carry virtually everything of digital communication that almost accounts for over 90% of data including all sensitive that contains diplomatic cable, military orders, data from government offices, swift details and other sensitive information. Any disruption of undersea submarine cables would not only affect ordinary citizens but also government, commerce including financial truncation. The interest over finding vulnerability and tapping the cables dates back to USA's operation "IVY Bells" which was also on preemptive measure as even US DoD's net centric warfare and global information grid relies on undersea submarine cables therefore it

becomes easy to understand why US wants to have dominance on regions through which its cables passes (Blitz, 2017) .

In real geopolitics the enemy's enemy is considered a friend but in cyberspace there is a least possibility of it as the evidence of surveillance found that even US had spied on its allies probably to ensure that they remain allies. On June 2015, US then President Barack Obama described relations with Germany as "inseparable allies" and months later Wikileaks published reports claiming US' NSA has been spying on German citizens including the Chancellor Angela Merkel and her staff (Tapper, 2015).

2.8.1 Defining borders in cyberspace

The era of Westphalian model of cyberspace or Cyber Westphalian where each state can have its jurisdiction over its territory is yet to be seen and between that many nations are increasing their control to on this borderless domain with their power resulting in class among nations (Manjikian, 2019). The creation of an international cyber law is already taking years to be framed and before it actually gets framed the transition time from situation of no law to a well-defined law will witness cyber aggression by states to project their power and dominance on the theatre to ensure their legal structures are more absorbed in global law. The unstopped increasing crime rates both by state backed and non state actors will lead towards an international cyber law, the law is expected to regulate the domain by creating at least two different categories of nation where one will be highly secured after fortifying their virtual border in the virtual world and other category will be one who failed to follow the call for initiating action. The secured or well positioned nation will try to influence coming cyber backed global system.

The idea of introducing sovereignty over cyberspace was introduced in 1990s when Van Alstyne and Brynjolfsson referred to *cyberbalkanization* (Alstyne & Brynjolfsson, 1997) which will be creating smaller groups in cyberspace who share similar interest among them. The world is already witnessing different types of administration where nations are restricting use of social media and other forms of censorship over its citizens which includes China's Great Firewall and

Russia's RuNet and events like Arab Spring and other which has contributed to political turmoil has brought in idea of Splinternet becoming active (Malcomson, 2016). Both authoritarian governments who are denying citizens freedom and companies who are not preventing their platform to be used for promoting hatred has created problem for the very main aim of cyberspace which is to keep everyone united under a global umbrella by applying censorship. Splinter or Cyberbalkanization in particular brings in a question to software firms that help in bypassing the censorship and tunnel through different networks to participate in free movement. It is further believed that nations who are strengthening their boundaries are in a better position to address threats if initiated against them in larger level over nations which supports undivided boundaries. Boundary line raise the question that whether boundary will be drawn in dark web or it will be continuing as the ungoverned space.

The first known act of state sponsored cyber war was by US and Israel indicated that cyber arms race had begun in order to stop Iran from developing nuclear weapon and years later Estonia received large scale DDoS cyber attack on 2007 allegedly by Russia which came as retaliation for removing of a statue that praised the former soviet government. Russia having technical expertise and also a political reason to attack on Estonia denied of its involvement, similar incident a year later on Georgia resulted in countries announcing cyber strategies for their offensive actions with France (Delerue, Desforges & Géry, 2019) and Great Britain (Scroxton, 2019) announcing their initiative towards developing offensive capabilities and increasing control on cyberspace. Recognition of large scale cyber attack as an act of war started getting more acceptances where nations reserve option to respond by any means. Russia while denouncing increasing militarization of cyberspace has been able to conduct large scale cyber attacks. There is no official guarantee or confirmation that a conflict that originated in cyberspace can be confined there; taking India and Pakistan where a surgical strike on terrorist camps inside Pakistani territory that was functioning with support by Pakistani army saw large scale digital retaliation with cyber hacking at Indian websites and same was then responded by Indian cyber warriors (Katoch, n.d.).

In a joint framework of collective security when it comes for cyber security it is actually showing strength and weakness and in digital space no one is friend of other making it worse to think for cooperation. Further disparities in capabilities are very wide making each other often go for a pact with other feeling insecurity as the technological dependency of many countries on

USA for data as many internet goes are either HQ at US and on China which procured cheap equipment. Understanding geopolitical threats to cyber assets the city of Los Angeles made contract with Google and Microsoft cloud that their data will remain in contagious 48 states making it immune to ocean cable interference from other nations (Williams, 2010).

The connectivity of real world geography with physical nature of internet is supported by scholars of geography over a decade now it is further argued that whatever cyber utopians claimed about cyberspace that people would be able to relieve from this stress of real world but in reality it is not a different place than real world which never offers escape from reality. It is shared that words such as wireless and clouds are used to hide the long wires that make this whole communication a reality (Starosielski, 2015) this effort helps to deter the debate on sovereignty over the cables or charges to be levied on them. Benjamin Bratton argues that existing computing systems can be defined better as the 6 layered model of a stack which are Earth, cloud, city, address, interface and user where he supported his claim by pointing to challenges Taiwan, China, Hong Kong faced when typhoon disrupted underwater submarine cable. Bratton thus defining the layer of cloud from stack as vast server archipelagos that provide computational services while remaining behind the scenes further arguing that presence of states and trying to apply legal sovereignty in cloud platforms as a whole has complicated the functioning (Bratton, 2016).

A non state actor that managed to gain real land using cyberspace is ISIS (Islamic State of Iraq and Syria) at their peak managed to grab area of the size of Great Britain and this all by utilizing power of social media, instant messaging applications, dark web even jihad themed games (Atwan,2015). ISIS first started as releasing videos of be-headings and sharing it as propaganda on social media like Facebook, Twitter, YouTube, even though Facebook twitter tried to stop them but failed to prevent them using social media for recruitment and training purpose (Corera, 2020).

2.8.2 Cyberspace and Militarization

The cyberspace has seen many battles for showing dominance or gaining supremacy is often referred as cyber war was expected to be a supportive military action during a physical war as with increasing dependency in technology it was deemed to be crucial and strategic for

fortifying one's own critical information and also penetrate into enemy's digital information network, but the extensive development and progress in the cyberspace has made it the primary choice for waging an offensive action which can bring down enemy's digital architecture including telecommunication, transportation and financial stability.

The ability of staying incognito in cyberspace has made it a preferred choice and a new normal for expressing anger or taking grudge which often comes in form of propaganda, crimes and espionage which might not be considered as cyber war, cyber war is considered only when nation state penetrates into network of other nation's network for causing damage (Buchanan, 2020). The actions like hacking for stealing money, spreading propaganda and espionage into Research and Development (R&D) centers for taking away the research is not considered cyber war as they didn't attack the nation's critical infrastructure like power and telecommunication but it did make the nation loss of financial gain and peace , if the action can be linked to the teaching of Kautilya then it can be compared to the theory of Kotayuddha (concealed war or guerrilla warfare) which suggests for using of alternate paths to weaken enemy (Haaster, Gevers & Sprengers, 2016). Cyber weapons being comparatively economical to regular military arsenals like tanks, missiles or aircraft it needs humans in form of cyber soldier who knows computer networking can initiate the war and leaders who can motivate them in waging the attack, cyber war being affordable it can be conducted by all nations including under developed.

There are countries where military has always been strong and dominant (Ratner, 2018), the dictator run nation can employ various methods which they seem to be on top and seen as supreme leader of world someday (Freeman, n.d.) is feared the most as the can be exploited by belligerent nations in waging war over an enemy or any common enemy, few instance being North Korea's involvement in hacking of several US and South Korea servers notably being July4, 2009 Denial of Service attacks to Sony Pictures hack in 2014 , an elite North Korean defector who taught computer science at Hamheung Computer Technology University shared how the regime is spending its military budget on cyber operations which includes provoking other countries to display its supremacy of their leader in cyberspace (Lee & Kwek, 2015). It is worth mentioning then cyberspace of any nation might be another testing ground for cyber atomic bombs similar to its efforts made in nuclear weapon production. The dictator or military junta creates more threat to this domain as the leaders refrain from taking opinions from their

cabinet and being comparatively affordable cyber attacks can be arranged with a team of close aide can help to wage war either for leader's inner satisfaction or for the junta.

Increasing complexity in cyberspace often opens door for bitter international relations like during July 2009 attack on USA was initially traced back to China and only later it was calculated that attacks are less sophisticated and codes have similarities to North Korea thereby preventing another Sino-US tussle, North Korea allows its citizen to browse internet in form of internet known as *Kwangmyong* (Williams, 2015) which has the basic necessities like books, videos etc. Internet Security providing Antivirus firm Trend Micro (Kropotov, Lin, Hacquebord & Yarochkin, 2017) has found in their study that North Korea has involvement of nations like Russia and China in their daily internet operations catering to government and elites.

The cyberspace has been able to refine the intelligence war craft where earlier methods has been redesigned to fit in this digital age even human intelligence or HUMINT uses memory card for storage and online gaming involving multi player which usually may be the handlers to the agent. This inclusion of cyberspace into statecraft needs a vigil or observance in order to limit it from being converted into a battlefield or place of contention.

2.8.3 Censorship of cyberspace

Governments, private companies, schools /institutions, Internet Service Providers (ISP), and work places use means to filter the internet to regulate the flow of data in their network which includes installing software to prevent users from accessing certain websites and services while that remains available when using non restricted internet media which widely known as Internet filtering or blocking is a form of censorship. This censorship or filtering can be in different forms which can range from blocking entire websites, hosting providers, or keywords based.

It can be agreed that censorship and surveillance are two sides of a single coin only where blocking or disrupting the process of data flow process not only impact one region specific but globally as censorship often leads to adoption of various bypassing tools which further leads in breach of privacy of users and compressing network security. Primary reason for implementing filtering is given for identifying "unsuitable" activities itself is surveillance at first which is

applied by government and corporate at their level to implement their opinion on cyber governance which are as follows:

a) By Government

As days are passing the dependency on internet for daily activities are increasing for global population which is still a place of anonymity with no uniform governance system implemented making it a choice for criminals to cause harm to innocent users and also this domain is used by belligerent nations do mapping of the nation's crucial networks identifying the vulnerabilities and penetrate inside economy and defence architecture even during peacetime. Cyberspace remains highly contested even on peacetime where powerful nations have been using their influence in drafting global norms for cyberspace governance to be according to their desires which includes placing restrictions and censorship at their own level that are based mostly on political reasons that helps to ensure dominance of government and surveillance for monitoring anti-government activities.

Nations like China and North Korea are often designated as masters of implementing censorship whereas other top leaders across globe are found to use their stature to shutdown internet in their country. The first internet shutdown was witnessed during Egypt's Arab Spring in year of 2011 where it was seen that governments holds the capability to shutdown internet of their nation to make it complete disconnect from cyberspace which then has been followed by many other nations in imposing it over a particular region or over country as a whole; few of which continue being shut till date. According to reports published by Accessnow titled KeepItOn publishes in its latest report that world's largest democracy India for ensuring peace and as precautionary measure from inciting violence in a particular region of Kashmir which is being fueled by neighbouring nation for terrorism has made longest duration of shutdown (Duggal, 2021) .

These censoring or blocking are done at the choke points which are the places that act as gateway to outer world and it is here where nations carryout their censorship or shutdown complete internet by denying data to pass choke points. The choke points or autonomous systems being data packet carrier it can read message as it is required to transfer to next autonomous system for sending it to destination or dropping to destination but are not aware of starting point

as it might not be only autonomous system who has accessed the data. It can therefore be said that key theatre of battle in cyberspace for controlling internet is autonomous system (AS), country like China maintains relatively low lesser number of AS than rest of world to have better control within its network.

Various methods for blocking or censoring internet are as follows (Xu, 2016):

- IP and Protocol-based blocking - Considering information (data) as a letter then IP or Internet Protocol can be compared as the address which is issued to every building in a network this can be compared to the computer/laptop to which the letter (data) has to be delivered, in IP based blocking the network administrator can make a list of such IP and block them to censor their access to data.
- Deep Packet Inspection-based blocking - Deep Packet Inspection refereed as DPI mainly does through check of the packet that is getting inside network based on the rules that are set by administrators can include keyworrd based censoring, it also helps in taking real time actions on this packets if required that is why this is largely used for Intrusion Detection System (IDS).
- Uniform Resource Locator (URL) -based blocking - This type of blocking is very widely used where the filtering is based on the websites and not any applications, here in the URL blocking the censorship is imposed on the website attempted to connect and if matches with the list of blocked URL then connection is terminated else allowed to pass.
- Platform-based blocking (especially search engines) - Platform based censoring is carried in association with platforms like Google or Yahoo where government regulates the flow of information in their geographic area where the results to any query by user is filtered and reverted with a different answer based on the query if deemed to be objectionable by the government.
- DNS-based blocking - DNS stands for Domain Name System which is like the phone book of the mobile where only typing the name gives the related contact number and similar in websites when the address generally alphabets are typed it converts using DNS resolvers generally from the ISP, the ISP can modify its DNS resolver to share wrong information.

b) By Private

The private institute or company often frames regime which is often not highlighted or discussed in majority of events where institutions can block access to internet and private company enjoys their dominance to delete or take down any content that they deem it unsuitable, this debate is not new since social media is often accused to deny basic human rights of freedom of expression. The right to equality is not mostly followed as almost all ISPs manage their bandwidth and money by throttling which involves setting limit of speed for group of users or to for selective websites (McCue, 2019). They often follow this step to justify their effort of serving more users but in actual they do save in money. Especially when internet providers especially in India after launch of Jio has made internet so cheap (Ghosh, 2019) and a populated nation like India streaming video continuously nonstop on it makes throttling a needful tool to serve more users at low price.

Social media companies have their own terms and conditions for usage of their platform which not always need to match the legal bindings of the country where the user is browsing and selective handling of these social media companies vis a vis users of different countries also becomes a concern where in some countries the approach remains as to give notice to unsuitable content and then taken down whereas for Canada it is to inform and then taken as matter for adjudication. The process of censoring by private is not new where major forms of censorship remains unnoticed globally owing to difference in thinking of users as for US users the censoring of political speeches is more debated than other forms of content and with other nations like in Middle East the content like movie and advertisement hurting culture might be debated for censorship over political. These selective approaches question the transparency of social media and their companies at large where they are showing different behavior to different user on basis of country of data origin.

Various methods for blocking or censoring internet by non government entities are as follows:

- Blocking or filtering devices.
- Filtering local network.
- Throttling
- Delaying posts of anti government in social media citing reason of fact checking

- Blocking or filtering by Internet Service Providers (ISPs)
- IP address blocking.
- DNS blocking.
- Keyword filtering.
- Website filtering.
- Port blocking.
- Network shutdown.

2.8.4 Cyberspace as tool of geopolitics

The nations which maintain a military base on a foreign land when studied can be found are in race for trying to secure landing ground for their submarine cable before other nations gain control. As the world is getting divided on US and China groups both powers are increasing their race for overseas deployment is feeling tension felt across world where cyberspace has also been used as a tool which includes from online campaigning to laying of underwater cables to show solidarity. There are three cable chokepoints that are important to ensure global connection which are: Luzon strait, Suez Canal-Mandeb Strait and Strait of Malacca which are always under contention and that is reason why nations are increasingly trying to get in their own route to avoid such choke points and once their dependency is reduced on these nations can be on offensive mode as at this situation they all rely on an action could be a collateral damage.

Threats to submarine cables (Source - Author).

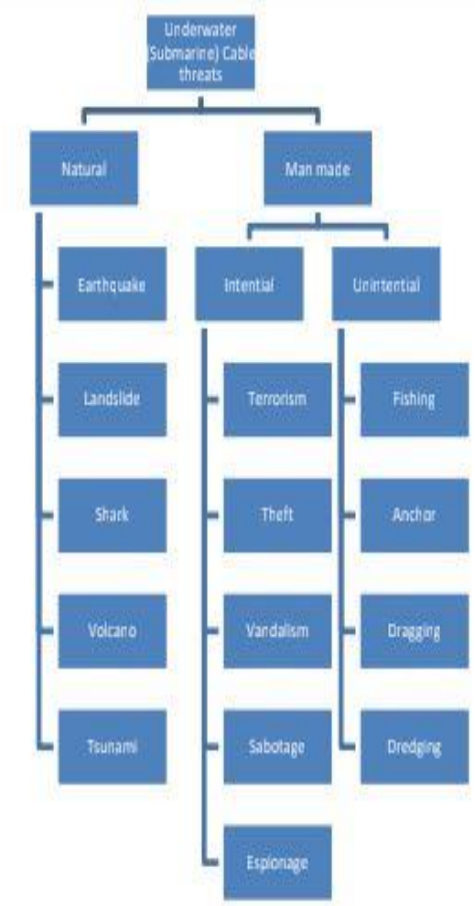


Fig 3 – Threats to submarine cables (Source - Author).

The impact from submarine cable was felt on 2015 when the Governor of CNMI (Commonwealth of the Northern Mariana Islands) declared state of significant emergency when the region lost connectivity with cyberspace for couple of days after the undersea cable carrying data got cut, the impact was felt in all sectors creating huge loss of revenue as banking, retail sectors were unable to function and even few airlines were grounded (Daleno, 2015). This incident fairly gives an idea of potential of cyberspace which is why on July 2012, Jim Clapper Then Director of Intelligence even stated that cyber threats will surpass threats for terrorists (Ryan, 2012), later it was found that US itself was carrying large scale surveillance. Therefore, it can be attributed that having ability to cut the submarine cable itself using dual use Un-Manned Underwater Vehicles (UUV) with both defensive and offensive capabilities are sufficient to weaken the enemy enabling it to play significant role in managing geopolitics.

a) Race in Oceania

China off late has started increasing its presence in Oceania region with opening its embassy in small island of Kiribati after it recognized Beijing over Taiwan as main true China, the island nation Kiribati was one of the few remaining nations that recognized Taiwan. The island nation Kiribati is a place of high geopolitical conflict because of its geographical location which made it a friend to US and its allies until recently when it shifted towards Beijing after receiving its donation and heavy investment in all major sector that includes internet infrastructure in Oceania region initiating competition with US, EU and their allies on controlling global data traffic. The recognition of Beijing over Taiwan now leaves Palau as one out of only 4 nations that recognizes Taiwan and now Palau is seen as a nation for conquest by super powers as Palau which was earlier dependent on satellite internet sees new cable landing station which is a huge support as it will be connecting them to fast internet and creation of another market where global powers will come to donate aid for ensuring control of Palau's digital network as this can serve as alternate route to divert traffic to Beijing over other available (Lyons, 2018).

Australia the key member of intelligence group Five Eyes (FVEY) has been gearing to prevent Chinese expansion in the region after China's Huawei signed deal in 2016 to lay submarine cables in Solomon Island. The region has started late in 2014 when Vanuatu linked Fiji with its first submarine cable since after that nations started to experience better connectivity and it provided opportunity for China to enter in the region. Australia managed to cancel many deals with neighboring nations as it being the giant has even initiated to take lead in laying the cable prominent being 2017 Solomon island, Papua New Guinea (PNG) and Australia with $67 million project. Australia has also stopped Vanuatu and PNG project from going to China and recently Australia is able to bring back Pacific Island nation Nauru to agree in allowing Australia for laying cables and connect them with other pacific nations like Solomon Islands and Papua New Guinea. (Barrett, 2021)

Even though pacific remains a place for several submarine cables but the nations were not connected to it leaving region remain on higher risk of experiencing blackout as they have less cables with poor backup, one such country in Tonga which experienced black out in 2019

for 12 days. Tonga' state owned Tonga Cable's director exerted the involvement of powerful actor behind it which found in its investigation that sabotage was caused by European flagged vessel to at that of incident at that location, the incident till date has left impression in minds of people for being an act of sabotage (Pullman,2021).

China has supported creating domestic internet cable system in PNG, e-goverenment system in Vanuatu and in Fiji China has contributed with e-governance system in association with France whereas US in its move has initiated network to connect Fiji, Samoa, Kiribati. China' Tan Suo 1 deep sea research mission has succeeded in live streaming video which can help china collected data for its submarine fleet (Stashwick, 2018) near Mariana land and Guam. Sydney landing point is crucial link between US and its allies at Oceania and its administered land Mariana Islands which if it is severed the consequences besides communication will be of economic and military as well.

b) Race in Africa

US and China opened new front in Africa with a race to gain control over internet network that are located undersea. US did started campaign against Huawei about potential threat that the Chinese backed Huawei brings to people's privacy (Roy, Volz & Purnell, 2019) forgetting it ran largest surveillance program in world. Since the cables not only support economy but also national security every powerful nations trying to secure their dSLOC or digital Sea Lines of Communication which carries more than 90% of global communication against vulnerabilities and attacks.

Huawei Marine Network Company a Chinese state backed global telecom supplier has established 6000 km undersea submarine cable network between Fortaleza in Brazil and Kribi in Cameroon in association with the South Atlantic Inter Link or SAIL (Hardy, 2018). This network joined Africa and Latin America which will meet the demands of data traffic flow from users of Africa and North America with Europe and South America making it a point of strategic importance. Another Chinese state supported company the China Telecom Global announced another submarine cable deployment partnership this time with Angola Cables for connecting BRICS nations together by establishing cable from Asia to Latin America using the South Atlantic Cable System (SACS) (Tredger, 2020). Huawei started entering North Africa in 2010

with a small contract of establishing collaborating with UK based Global Marine systems a 177 km cable connecting Libyan cities of Tobruk and Emasaed (Pisch, 2011).

c) Race in Asia

USA made PRISM surveillance project, Five Eyes (FVEY) to spy on Asia also with its allies maintained presence in Asian region at Hong Kong, Philippines, Malaysia, Indonesia that extended to Pacific from its base at Guam. USA maintains cables to Palau extending connectivity to Australia, New Zealand more appropriately to ANZUS (Australia-New Zealand-US) partner. Now China plans to counter with PEACE (Pakistan and East Africa Connecting Europe) project that is being executed by Huawei Marine which will connect China from Pakistan to Djibouti, Egypt, Kenya, South Africa, France, Seychelles creating tension in Europe already (Fouquet, 2021), further the Silk Road from Pakistan to China is already in full motion and now digital Silk Road is also in swing.

India's Reliance communications owned submarine cables were snooped on by British intelligence agencies besides other cables which is considered to be part of operation "PFENNING ALPHA" jointly executed by US' NSA and GCHQ (Datta, 2014). Reliance submarine cables carried large amount of data from Asia to Europe named FLAG cable and from Europe to American continent cable called FLAG Atlantic 1 (FA1), The cables also carried data from other internet service providers as it had landing stations in Egypt, Arabian Peninsula, India, Malaysia, Thailand, Hong Kong, China, Taiwan and Japan which were of high interest for British agencies and their US allies NSA. India now holds more potential as its largest private player Reliance has started deploying own submarine cables which will almost eliminate dependency on international sources (Basu, 2021), this project once completed will enable India in rising as leader of digital NAM (Non Aligned Movement) which will provide internet to countries are not willing to join any power blocks of splinternet cyberspace particularly economically weaker nations.

d) Race in Arctic path

When environmentalists and common peoples are fearing over global warming and melting of polar ice caps many nations are seeing this as an opportunity to open up another

upcoming area of contention that is seen as strategic shipping lane full of unexplored natural resources and Arctic is not bound by any treaty which unlike Antarctica that is governed under the treaty of Antarctica 1959 dedicated the region for scientific research and denied military aggression (Hirji, 2015).

As the region of Arctic was becoming increasingly accessible more nations have shown interest in entering the region and interestingly the region which until 1991 had military presence shifted towards making cordial relations after Union of Soviet Socialist Republics (USSR)'s disintegration in 1991 when Russia and other seven Arctic states Norway, Sweden, Finland, Russia, US, Canada, Denmark and Ireland got together to sign the Arctic Environment Protection Strategy for protecting the environment and after 5 years later paved the way for Arctic Council for keeping the region secured (Oude Elferink, 1992). The Arctic council is increasingly getting requests for joining it as observers, presently observer status is granted to European and East Asian countries with Britain claiming itself as nearest neighbor of the region and China going a step ahead claiming it as a near arctic state even though it is well distanced at above 900 miles from the last tip of arctic to its northern point. China also called the Russia-China cooperation on Northern Sea as Silk Road on ice (Mammadov, 2020), which it again mentioned on its 2018 white paper as polar Silk Road.

On 2017 August, Russia made headline by making new northern sea route navigable for its purpose by declaring it has been able to reach South Korea from Norway in just 19 days by taking new northern sea route from about 30 days if travelled by traditional route (Barkham, 2017). Same year on November Arctic council at a meeting in US decided to ban unregulated fishing for next 16 years to ensure proper study of underwater biota but at same time have initiated developing underwater naval capabilities with fleets of ice breaking ships in Arctic with Russia standing largest including its Yantar class vessels capable of disrupting submarine cables followed by Finland, Canada, Sweden, China and America (Peter, 2018).

This increasing shift towards the Arctic route can be a signal that nations are trying to harness that new pathway and to ensure they have dominance in the region that will help to deploy new submarine cables that can help remove dependency on other existing cables and in turn can rise can create their own network or a separate cyberspace comprising like minded

nations.

2.9 Conclusion

Cyberspace today in general understood as a mean of communication for government and for personal usage that enables the publication, exchange and storage of information that travels faster over traditional methods. The man made domain of cyberspace was initially reserved for military purpose before it making it available for civilian use and now has billions of people using it for their daily activities, this dependency of citizens for easy access options and availability of free large data storage facility creates in valuable information which is perceived as a necessary tool by nations towards achieving dominance thereby applying military strategies.

Today's generation is widely referred as digital age where all useful devices are equipped with inbuilt technical configurations to make them "smart" allowing them to be part of cyberspace easily but this rapid growth in such devices with their users who are not aware of the security gives rise to multiple threats like that of DDoS (Distributed Denial of Service) where skilled attackers including state sponsored groups use those connected devices to create problems to their targets varying from corporate firms to nation creates great challenge on regulations and policies that are in force for administration.

The governments are constantly upgrading their national policies and also making alliances according to similarities in opinion for tackling any transnational threat, whereas the differences in opinion related to functioning of cyberspace has given arise to balkanization of cyberspace where concept like "splinter net" are gaining popularity and cyberspace is predicted to get divided into multiple factions with factors like politics, nationalism, religion etc. might lead to division like that of geographical and commercial boundaries. Latest development indicates that internet might be divided into a bipolar world with one led by USA and other by China, where US supporting open internet and China pushing its allies pushing for a censored version, the division might not be directly but based on users using facilities like one who is using USA based apps and others using China backed apps

The increasing dependency on cyberspace and difference in threat perception from cyberspace has made nations to frame in different domestic policy and same is further

reflected in their foreign policy as well there by suggesting rules for cyberspace governance on same lines. The race for supremacy in cyberspace has now included satellite and optical cables that carries data traffic now has potential of influencing geopolitics and private companies who since beginning holds ownership of the cables find them as important player in framing of cyber governance. Further the unexplored region like Arctic can be an arena where China in particular with its allies can lead to creation of separate internet network by connecting them with submarine cables.

The former NSA consultant Edward Snowden has already revealed that United States and its allies have been monitoring submarine cable data China has gone a step ahead by planning its own digital Silk Road with its state controlled Huawei company taking lead role. The constant tension has brought in a sense of competition resulting in deployment of defensive and retaliatory mechanism to ensure safe passage of data that need to travel vast distance using cables placed underwater or often via satellites at low earth orbit both which are part of other domains like underwater and space respectively. This clearly indicates that there is a need to involve the concerned domain representatives which is underwater and space respectively to ensure that Un-Manned Undersea Vehicles (UUV) and other anti satellite weapons are observed as they can have dual potential of being a peace time observer and during wartime they may unleash lethal force.

Chapter 3

Role of stakeholders in cyberspace governance: Analysis of evolving global regimes

Administration of cyberspace or the new global common has now become important as it can be compared with other inventions which were designed for peaceful and have later been used for creating large scale loss to humans. For instance, invention of aircraft which was used for joyride purpose and never designed to drop any bomb during its trial run. Similarly, cyberspace was designed for connecting computers for establishing communication by military but is now used by cyber criminals with or without government support targeting mostly civilians population and resources than its primary aim for military use.

This chapter will discuss the initiatives cyberspace has seen from its major stakeholders

like government, corporate firms, Inter Governmental Organizations (IGOs), civil society, academia and Non Governmental Organization (NGOs) either separately or often collaborated with each other to suggest a global regime towards either a multi stakeholder or multi lateral architecture for safeguarding the cyberspace which although is virtual but relies on heavy infrastructures. Further the chapter discusses the

3.1. Cyber governance regime

Nations are joining together to work in the new global common cyberspace where the debate between multi stakeholder and multi lateral form of governance is being debated. Multi-stakeholder form of approach is for global challenges like climate change, conflict prevention, peace building etc. are being implemented to address the rising difficulty and policy framing issues to come up with a dependable and practicable solution for peaceful coexistence in this digital world. The study in the area of cyberspace governance is getting more diverse with passage of time due to involvement of multidisciplinary topics that includes politics, psychology, and economics besides role of nation states which did not have presence in main frame of internet which had foundation of only technology. The stakeholders of internet are wide ranging which includes government, academia, civil society, intergovernmental/international organizations, technical community and private sector which exists with every member states of UN with credibility of each stakeholders varying within individual countries. The push towards accepting of multi stakeholder model of governance to govern the complex domain that calls in all state holding including state and non state actors have resulted in for a new institution like Internet Governance Forum (IGF) to help in giving a right direction to progress in cyberspace and help to harness its richness. The image (fig-4) below defines the internet ecosystem that has to be balanced in the process for a global cyber governance

The complexities in cyberspace ecosystem

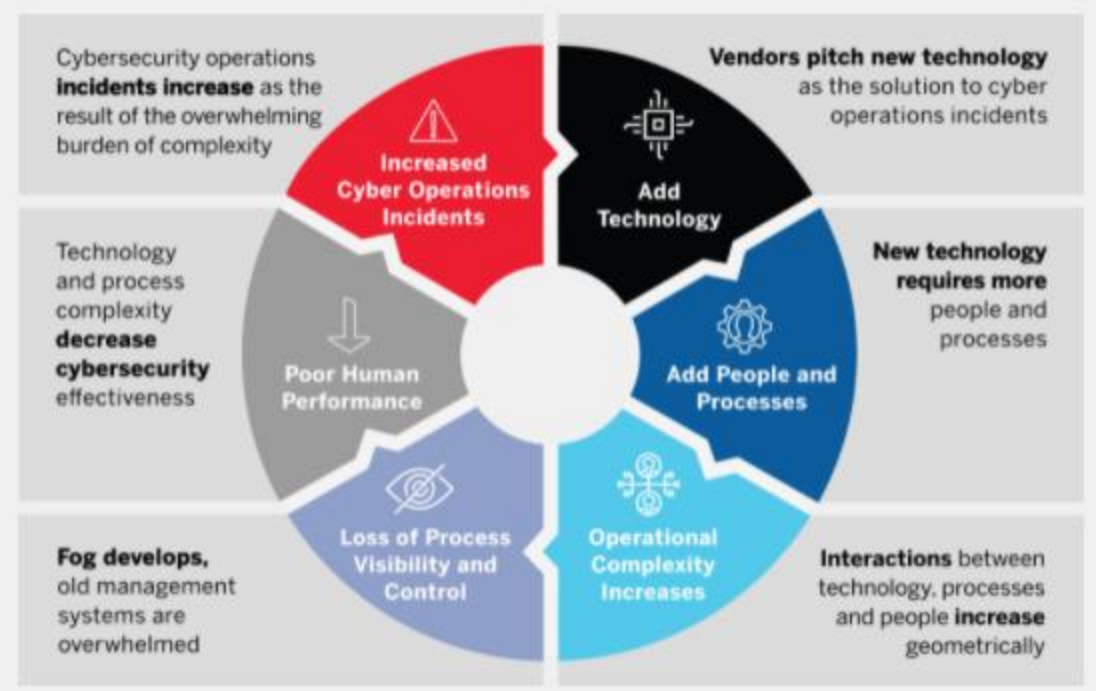


Fig 4- Complexities in internet governance (Source- Wilson, Hamilton & Stallbaum, 2020)

The potential of virtual environment which is created with cyberspace is based on data often considered as new oil (Arthur, 2013) for its increasing value in today's environment and stakeholders are working to either protect or secure it. The initiatives taken by stakeholders are mostly confined to country, region or associated groups as there is no global consensus on governance of cyberspace on how it's essential per-requisites like infrastructure, security, legal, regulations etc. will work for securing individual's human rights and grant justice to deprived users in cyberspace (Mihr, 2017)

Effective international co-operation in cyberspace is essentially required as the cost of offense is less than defence of it has undertaken series of treaties and agreements at regional and global level which includes prohibition against military usage under United Nations General Assembly resolutions 31/72 of 10 December 1976 and 1977 Convention on the prohibition of Military and other hostile use of environmental modification techniques, resolution for ensuring prevention against crimes related to cyberspace UNGA 55/63 of 4 December 2000 and 56/121 of 19 December 2001 (Nitu, 2011). Similarly, the 2001 Council of Europe Convention on Cybercrime (Budapest Convention) and for creating a culture of cyber security globally with UN

resolution UNGA 57/239 dated 20 December 2002 (Wamala, 2011), but with emerging technologies like IoT, AI distributed unevenly with more in possession in hands of developed countries there is need to ensure equal distribution as well. Further international organization comprising nation state representative do see involvement from non state actors in governance through business community and civil society, which becomes a key player in regional for either on business or other factors that not yet received consensus globally and the reach of non state actors like NGO is often found at grassroots level which make them a direct point of contact between government initiatives and beneficiaries.

Scholars like Joseph Nye Jr have suggested for application of regime complex theory to initiate the framework of uniting nations to collaborate against mutual threats leading a path for nations to frame a mutually acceptable norm. The hindrance that come in framing a uniform cyber regime includes increasing cyberskeptics who stands firm that the threats from cyberspace are not much and it is not capable of causing physical harm to anyone it is just a trick to divert form real world challenges (Rid, 2013). The presence of cyberskeptics are found among decision making groups which over time brings in idea that cyberspace does not need a specific law and attention it can be handled in a normal way as it is going resulting in opposing comments from both sides accusing one section to be in a hurry and other accusing to be too slow.

The absence of a uniform definition of cyberspace and cyber security as discussed in previous chapters are one of prime factors that has led to this slow process of framing an international cyberspace regime. Debate among the parties or stakeholder relevant to building an international regime can be divided into two groups one which supports multi stakeholder model which includes equal participation from government, business, civil society and other group that contributing in development and functioning of internet whereas other group supports the sovereignty based architecture where government can have complete control over cyberspace and associated architectures. Security which stands supreme and common to both parties often diverge in its meaning where from one side it can be referred to protection of physical infrastructures that includes wire, cables, equipment, servers and other utilities associated and on other way it asks for the safety of the information that passes through those physical infrastructures.

3.1.1 Existing regimes

The following collaborations that already exist can be considered as foundation when framing any new international regimes on cyberspace, as these existing collaborations are made on the basis of mutual need of the members therefore updating them can be helpful:

- The five eye intelligence community which included United States, United Kingdom, Canada, New Zealand and Australia where they shared intelligence among them which started long back and has been working actively according to revelation made by NSA whistle blower Edward Snowden **(**Gallagher, 2018).
- Sharing of information between governments and private bodies need a reformation like in case of government to government existing mechanism of Memorandum of Understanding (MOU) and a vulnerability disclosure agreement between individual and companies can now be extended to bring in both private and government so that a threat can be quickly addressed.
- Establishing cyber hotline or adding cyberspace as a topic for hotline resolution in order to deescalate tension in cyberspace that might arise due to any offensive actions between belligerent nations.
- Existing measures like the Wassenaar Arrangement established in 1996 with 42 member nations to ensure transparency in sharing of arms and dual use technologies for ensuring security can now include cyberspace utilities as well, since many mobile applications are now being exploited with their dual use nature particularly with the advancements in artificial intelligence (AI), Big Data etc (Cross, 2018).
- As regional alliances are being maintained by nations to ensure their national interest, threats like child abuse and cyber attack on civilian resources can be added to make it more effective as regional alliances are an existing framework.

- Tallinn Manual (Tallinn 2.0) which was established after cyber attacks on Estonia in year of 2017 after discussion among scholars and practitioners as in what context international law can be applied on cyber warfare and conflicts happening in cyberspace. The application of law of arm conflict (LOAC) failed to draw in required support internationally making it difficult to mark the limit of threshold point beyond which the victim nation can initiate in a full scale war as relation to armed cyber attack (Adams, 2019).

3.1.2 Confidence Building Measures (CBM) and International Humanitarian Law (IHL) in cyberspace

International regime in cyberspace might not be a tool for ensuring global harmony but can definitely bring in peace in cyberspace if a fair policy is followed. As the global digital village connecting people to each other across the world has brought threats from state and non state actors it often includes complicated threats like a state backed non state actors making threats highly diversified in nature (Verton,2003). Therefore the complex threats brings in a sort of compulsion for nations to join for collective alliance safeguarding them against such threats further cyberspace being a highly contested space and highly affordable for nations in waging attack on enemy's economy is widely considered as preferred option over traditional forms of attacking, cyber operations are not myth anymore its lethal capabilities has been witnessed already that is now raising concerns about the security of innocent or civilian life which once suggested by IHL (International Humanitarian Law) (Greppi, 2018) .

The International Humanitarian Law or IHL which does not support any forms of warfare including cyber warfare where a nation state uses its forces to wage attack affecting belligerent nation's innocent civilian population is much concerned on cyber warfare and suggests limitation of cyber operations during armed conflicts. International Committee of Red Cross (ICRC) which is focused on impact of innocent civilians by cyber operations conducted by nation states as more than military it is civilian population that are connected to cyberspace (Rodenhäuser & Mačák, 2021). ICRC supports for implementing IHL measures during cyber aggression by nations as the threshold to which an attack is considered as complete armed attack is not defined under any international guidelines making it difficult for decision makers in responding to threats, with nations accepting it as a domain of warfare and pledged to retaliate it full force makes it more complex since different nations will make their own threshold point and can initiate total war on potential accused as it is difficult to identify an attacker in cyberspace. Existing principles that applies on cyber operations under IHL are as follows (Biggio, 2019):

- Offensive cyber attacking developments that holds potentials to be utilised as weapon for destruction;
- Direct cyber attacks on utilities used for civilian including their assets are barred;
-Provocative actions using cyberspace that promotes spreading terror or hatred among unarmed civilian population are completely prohibited;

- Disproportionate attacks through cyber space that can result in loss of civilian life and assets as a retaliatory action often leading to involving direct military action.
-Ensuring to avoid damage civilian and their assets during military operations conducted through cyber means, usage of cyber weapons only after confirming target as military;
- Life saving resources like medical services must be left unharmed during cyber operations conducted while being at armed conflicts.

The above rules related to cyber attacks by nations on nations are focused in saving civilian life and their assets both during peace time and when at armed conflict. The IHL is not accepted and followed by all nations as there are instances when attacks like Ukrainian power plant (Park, Summers & Walstrom, 2017) have happened which has denied innocent civilians of electricity for hours. It further brings to notice that an urgent need has arrived to ensure and fortify the bonds of friendship between states and society over the use of this borderless domain. There is a need to build confidence among the power blocks and other members of the cyberspace to ensure prosperity prevails in the domain which can be achieved by initiating more CBMs (Confidence Building Measures) which are considered a trusted tool of international politics which can prevent any conflict or international crisis, it helps to redevelop trust and improve relation between nations. As it is important to undertake efforts to resolve all related topics that make cyberspace a contested place like espionage as nations are increasingly relying on cyberspace for their espionage activities, since there is no proper treaty on espionage it makes it difficult to limit such offense (Buchanan, 2020).

The factor that who is decision maker or decision making body and who holds control over implementing decisions plays crucial role in framing regime as that will lead in forming a closely possible structure that is acceptable to all as exiting debate between Multi stakeholder led by US and multilateral led by Russia and China brings in a totally opposite roadmap ahead and often allowing the rise of a third framework of privatized cyberspace management where bodies similar to ICANN above it can be made to oversee the debated space. As DNS and TCP/IP has been running till now because of private players and they stand as a potential contender to ask for granting equal opportunity in showing potential to design model of governance.

3.2 Role of stakeholders in cyberspace governance

The stakeholders who are presenting their credentials for seeking the control of cyberspace are advised to represent them through respective RIR (Regional Internet Registry) for

participating in discussion and participation in cyber governance dialogues or conference to plan for road map for multi stakeholder form of governance. The five RIRs are managed under Number Resource Organization (NRO) which was established in 2003 to act as coordinator to all RIRs in sharing internet number resources in their regions. First RIR was established in 1992 and is maintaining transparent multi stakeholder decision making process where is allocates internet number resources (IPv4, IPv6 and Autonomous System Numbers-ASNs) and services to ISPs in respective geographical regions. Due to lack of effective coordination between stakeholders it was found that there was increasing digital gap where the allocated IP addresses on one side was getting exhausted at rapid rate while on the other side particularly in Africa there was surplus comparing with the required numbers leading to widening of digital gap (Tamon, 2015).

There are 5 RIR in world which manages the internet registry system and responsible for keeping record of data on allocated internet resources to ensure un-interrupted services, five RIR are as follows:

RIR	**Region**
African Network Coordination Centre (AFRINIC)	Africa
Asia Pacific Network Coordination Centre (APNIC)	Asia- Pacific
American Registry for Internet Numbers (ARIN)	USA, Canada, few Caribbean nations and North Atlantic islands
Latin America and Caribbean Network Information Centre (LACNIC)	Latin America and remaining Carr abeam nations excluded from ARIN RIR
Réseaux IP Européens Network Coordination Centre (RIPE NCC)	Europe, the Middle East and parts of Central Asia

Table 6 - The RIRs managing the global internet registry system Source (The Number Resource

Organization - NRO)

3.2.1Attempts by Government

To understand the role and necessity of government in cyberspace we can refer to a comparison of commercial passenger modern aircraft Boeing 787 against just a relatively small Rafael fighter jet which can carry two pilots only for aerial defence, in this scenario passenger aircraft cannot provide deterrence to fighter jet and for offensive purpose it is only Rafael that can attack. Even though commercial aircraft can be used for reconnaissance purpose but not to attack therefore in similar way corporate firm single handedly cannot secure cyberspace assets against foreign government attacks they can only gather data and other information of nation's belligerent countries.

The internet or modern day cyber world has its origin because of initiative funded and raised by United States government with its ARPANET project that not only designed internet by connecting devices via cables but it paved way for networking via satellite and land based mobile networks. United States have managed to steer the wheels of internet for long as it is accused of using influence in ICANN (Internet Corporation of Assigned Names and Numbers) that acts as a nodal point or a directory which helps in processing DNS or domain name service that identifies websites by words instead of complex IP addresses. The revelation by Edward Snowden in 2013 that pushed in regional organizations and developing nations became more enthusiast in taking effort related to cyber governance making it to hand over the control of the database holding all domain names the IANA (Internet Assigned Numbers Authority) making US end its authority over ICANN in 2016 (Lee, 2016) .

Edward Snowden revealed of global surveillance on citizens and political leaders allegedly by US and its allies reigniting the debate of governance architecture model of cyberspace. The debate which is often focused on contribution that individual stakeholders have on development of enhancing experience of cyberspace is questioned by fact that national governments mostly focus on employing strict online policies depending upon the degree of freedom it wants to grant to its citizen which ranges from banning online gambling to blocking content. The censorship of online includes initiatives like removal of search result from indexing, taking down of websites and technical blocking of websites to ensure citizens are able to view only what is fit according to leaders. The complexity arises when multinational companies who operates in both extremes like country which supports freedom of speech and one which denies

making nations to abide rules of the nation where it is operating for doing business calls in for self-censorship (Corr, 2019) to avoid loss of business making private companies to act as police and when required by government to share details of users which is happening most in order to curb cyber crime but at same time this act of state asking details of users is seen as a violation of human rights.

Government often takes control of internet by shutting down completely even world's largest democratic country India has done it on several instance in order to prevent violence from spreading using internet as there is no effective mechanisms to prevent misusing of internet by criminals backed by belligerent state actor (Rampal, 2019). Increasing threats from cyber criminals has led government adopting higher security to safeguard its citizen's data irrespective of their view on administration of cyberspace to be managed by either multi stakeholder or multilateral such being Netherlands, Slovenia who support the net neutrality that is where every communication is treated equal without processing it influence of any organization, destination or source of address and application used have higher security and countries like China, Russia , Saudi Arabia who follows an authoritarian regime yet implements higher amount of security and filter on cyberspace checked at BGP (border gateway protocol) the main entry point of nation for data flow (Saakashvili, 2021).

European Union's introduction of General Data Protection Regulation (GDPR) which is adopted by governments across European Union to protect data of its citizens stands as foundation of government's effort in ensuring data privacy while at same time assuring citizens of its security as state takes responsibility of it with their strict law in place for violators to the law (De Groot, 2020). After GDPR many nations have acknowledged the importance of data protection and have brought in law like Brazil's Lei Geral de Protecao de Dados (LGPD) (Browning, 2020) and Thailand's Personal Data Protection Act (Suwanprateep, 2020). Nations have made their CERT or computer emergency response team as a immediate responder to any cyber attacks often joining with allies for effective retaliation in case of large scale transnational cyber attacks besides strategic partnerships or MoUs that commits of mutual non interference in cyber offence on each other like UK and Singapore MoU (Barker, 2018).

As discussed in previous chapter (second) there is a sharp contrasting approach by nations like USA and China who are joined with their own allies in some way is leading us in

getting a bipolar version of it with arise of “splinternet”, therefore US and China are playing in crucial role to frame an international norm due to their prolong disagreement on topics like open v/s censored makes the later outcomes differed as they both then follow different roads and frame in their own alliances and policies further trying to push in for global acceptance of it. The approaches by these countries if studied can be found to be diverging from an idea of establishment of a uniform global cyber regime agreeable to all nations. Approach by US includes International Strategy for Cyberspace that would guide all agencies of US government to collaborate and coordinate for their roles in cyberspace, further joining in for public private partnership besides keeping it available for other states if they are keen to join in for promoting open, secured and harmony in cyberspace (Nakashima, 2011). International Strategy for Cyberspace will also support norm that promotes freedom of fundamental rights and harmony with security by including other stakeholders if required. The approach by China includes its rigidity on issues like data control and sovereignty, China is a strong believer of constructing a replica of great wall of china in cyberspace which can be a identification for other states to not trespass into territory of china as it has a belief of non interference and each nation must be allowed to design their own rules for internet.

The idea to include all stakeholders for forming the cyber governance model receives constant resistance by prominent nations that are members of elite groups like Shanghai Cooperation Organization (SCO) led by China , Russia besides disagreements over application of international law on cyberspace where US suggests that existing norms and laws can be directly applied to cyberspace and China on other hand differs supporting a separate regime for cyberspace which can include sovereignty as a subject (Margolin, 2016).

Nations have started modifying existing infrastructures to tighten security and aim to establish a digital sovereignty which indirectly has impact on global cyberspace governance which can ultimately lead to fragmentation of internet. China has made it compulsory for using real name when getting a top level domain under .cn category. As discussed in earlier chapter 2, nations have started appointing cyber diplomats and created dedicated agencies to handle cyberspace related issues of international politics. The government after AI evolution has started to focus more on it as Russia’s President Putin has already claimed nation who will lead in AI will become ruler of the world (Vincent, 2017).

Government taking measures of censoring on applications and websites due to threat on

national security where belligerent nations use it to gain advantage like China tried on India when the world was forced to accept the culture of work from home digitally due to global pandemic COVID 19 leading to more digital usage and during this time on June 2020 India banned Chinese backed applications like TikTok and 59 others due to threats of India's national security and again banned another 43 applications on November 2020 (Bhargava, 2020) this came in after increasing Chinese threats from cyberspace and also aftermath of Chinese aggression on India's land boundary claiming Indian territory as theirs, this move was welcomed by US and other nations citing threats from China's Huawei 5G and more nations came together to block in the company as this led the fight against China who is believed to behind this pandemic by not informing world on time to take precautions.

China stands among one of the top leaders in AI based facial recognition technology has managed to bring in discipline among its use where it has highlighted of getting success in preventing crime and ensuring safety to common citizens has used it for other purpose like waging large scale surveillance and also sharing it with other nations like Uzbekistan, Laos, Saudi Arabia, United Arab Emirates, Kazakhstan, Kyrgyzstan, Uzbekistan etc who are implementing it stating benefits of preventing crimes and others are found to be involved in violation of Human Rights (Tsz Yan, 2019). China stands as one of top contributors to UN wants to implement its influence its opinion globally has often used technology as tool to help ruling regimes suppress opposition like what found in Uganda and Zambia (Woodhams, 2019) besides that China through trade and investment has managed to convert African nations as its trial grounds for spying gadgets so that it can later sell to world. China is not alone in race to suppress oppositions and critique, Israel has also designed software called Pegasus that is widely used to identify and track human rights activists, journalists and other academicians who spoke against regime (Priest, Timberg & Mekhennet, 2021).

Following India's path to make all citizens record digital through Aadhar, China also plans to introduce a digital identity card project where Alibaba and WeChat are competing for it (Elias Dec, 2017). To harness the power of AI nations are working tirelessly and China in its July 2017 launch Next Generation Artificial Intelligence Development Plan which says that it aims to be become world's primary AI innovation centre by 2030 needless to say AI has huge potential in cyber security and military which can be used for offensive as well (Richard, 2020).

Government also ensures that foreign corporate firms who are doing business in country do not hamper privacy of citizens like Facebook on 2017 prompted new Indian users to give name as per Aadhar card and on similar case Amazon asked users to share details of Aadhar card for cases related to return and refund of product. Government is also acknowledged for initiating public private partnership to protect critical assets in cyberspace and collaborating with other nations for alliance and present shared opinion or create collective defence against mutual threat that often includes cyber exercise like " Multi-Lateral Cyber Defence Exercise 20" at Germany where Israel military trained the German and cyber troops from Austria and Switzerland (Monroy, 2020), these outcomes further suggest government with effective policies and framework and trade tariff negotiations that can be possible only with coordination with other government.

Bilateral and Multilateral Treaty regimes on Cyber space

Treaty	Goal	Signed	Parties
Shanghai Cooperation Organisation	To assist in promoting awareness and uniting all stakeholders working for cyber security	2015	SCO members
Bilateral Treaties	To improve position in cyberspace and provide mutual security.	2017 2015 2015 2015 2015 2011	US-India China- EU China –Russia China –US US- Russia China- Japan- Korea
Unilateral Initiative by countries	International Strategy of cooperation on Cyberspace	2017	China

	International Cyber Strategy	2017	Netherlands
	International Cyber Engagement Strategy	2017	Australia
	International Strategy for Cyberspace	2011	United States

Table 7 - Initiatives by governments including bilateral and multilateral initiatives (Sources-Google)

3.2.2 Attempts by private players

United States which founded internet understood the skills that private players have in promoting the technology worldwide by Clinton administration in 1997 suggesting for non-regulated approach to promote e-commerce, although keeping 9 areas under regulations including customs and taxation, electronic payment, intellectual property rights (IPRs), privacy, security and technical standard, this initiative was further supported by 1998 general agreement on trade in services (Thierer, 2012).

The world's most valuable firm related to information technology does not hold complete United States monopoly it is being well challenged by Chinese and Indian companies further compete among each other in their own nation to conquer all emerging markets and most importantly the new users who are joining the cyberspace, while aiming for above they try to harness potential of involving all existing and upcoming technologies in order to ensure they are able to reach to remote corner where their potential user can be and to convince them in voluntarily share their data which is main source of profit for these companies. The content we view in search engine as a result to our query is due to algorithm and other techniques employed by private entities projecting their potential in content mediation. Government and IGOs mostly requests private entities for details and activities of citizens for tracking or surveillance purpose as majority of services to users is provided by them and not government making private players as first responder during any upheavals, prominent example of it can be 2010 Wikileaks case where online financial contributions were stopped to the whistle blowing site by platforms like Paypal, Mastercard and others including bringing down server to cooperate with government (Greenberg, 2010). After initial questioning by US authorities Amazon stopped hosting the sites

thereby reducing presence of Wikileaks which therefore raises a query about the power it holds vis-a-vis government being gatekeeper. Further the debates between governments and IGOs on global cyberspace governance has made them stand in crossroad yet putting in best effort to manage harmony at local, regional and global level.

Since advent of computers and expansion of internet private companies have contributed much to its development and concepts like cloud computing, AI are all from private companies and research funded by private companies leading are Amazon, Alibaba, and Microsoft who have eased people's worry of carrying large quantities of data with their cloud computing innovations available at affordable prices. Private companies have tried to stay away from government influence as they are often accused of influencing geopolitics by influencing people's opinion specially in cyberspace where companies have data of individuals ranging from financial details to behavior courtesy the applications which user are increasingly getting dependant on and belligerent government can use it for their surveillance and other purpose to weaken enemy nation's social harmony at large.

It is worth mentioning that a key step towards cyber governance was initiated by private companies where Global Internet Project (GIP) a consortium of 13 leading private companies who took up with initiative to make sustainability related to financing of forthcoming non-profit entity for managing domain name system (DNS), GIP suggested for equal contribution and set a benchmark for $50,000 so that no company can try to show power over others (Lillington, 1999), GIP included top brands that time like IBM ,MCI, AT&T,GTE etc. GIP which consisted the chief executive officer (CEO)s of top the then tech companies were aware that future progress will be highly dependent on cyberspace and it needs to be neutral otherwise there will be imbalance in resource sharing had there been similar initiative by government then there would not have been any gap in digital outreach of cyberspace and today if seen then it can be experienced that the access for internet is a must for staying updated and still many especially in developing countries are either having limited connectivity or no connectivity to the digital world at all. Africa the land of rich heritage in particular has been behind in joining the cyber world where its large population still has limited access. Private companies have taken initiative to provide internet connection where government has not been able to provide yet few of the initiates are as follows:

- Internet.org

A Facebook initiative by name Free Basics was launched in 2013 where they collaborated with local mobile network providers to provide free mobile internet for essential contents like news, health, local information and their own social network Facebook for free, the initiative claimed to connect 100 million people to cyber world even though there was criticism related to net neutrality rules but on a positive note it managed to connect people to internet (Morris & Kehl, 2014). Facebook also has an application called Discovery that allows users to visit any website and browse the text only which is capped at 10MB per user in Peru (Zeevi, 2020).

- Google's Project Loon

Google tried to create a network that will help in connecting rural and remote locations all over world using stratospheric balloons which will be solar powered which will be connected using antenna from stations at ground to directly reaching user's phone (Prinsloo, 2018). This initiative was designed keeping in mind for natural disaster and it proved to be successful after Hurricane Maria created havoc in Puerto Rico back in 2017 where Google's Project Loon managed to provide connectivity at that emergency situation to more than 200000 people on that island while the repair works were going for damaged mobile networks (Iscrupe, 2020). Google has recently discontinued providing free WiFi to all major railway stations in India which started in 2015 (Sheth, 2020). Google's free internet to Africa is seen as support to Goal 9 of Sustainable Development Goals (SDG) which aims in increasing digital connectivity to all parts of world.

- Laying Submarine cables

The most effective means of sharing of data for intercontinental communication is through submarine cable due to being cheap in nature and more efficient than satellite, in this domain also it is private sector that has invested till date and tech giants like Microsoft, Facebook , Google even date continue to lay submarine cables for improving connectivity for which they have several dedicated initiative like Microsoft and Facebook's joint MAREA cable which connects US to Southern Europe and Google's FASTER that joins US with Japan and Taiwan (Bennett,

2021).

- Deploying Satellites

Satellites are best possible way to communicate where geographical barrier exists and in this area private firms are racing against each other to expand their reach with companies Amazon, Facebook's Athena and SpaceX in particular with its Starlink project have started launching thousands of Low Earth Orbit (LEO) satellites that will help in not only providing internet to remote villages but also decrease the travel of data which is usually larger when transmitted to traditional satellites that are placed much higher altitude above earth surface (Shieber, 2019).

- Free Internet without business

US based company Jana has taken initialed to provide free internet and unlike Facebook's initiative of Free Basics which was claimed as controversial due to net neutrality, Jana users has no limit to internet usage (Peters, 2017).

When the global pandemic made work from home a new normal, it was private internet firms that first came out with extended or free data support to its users to cope up with work from home and study from home for students. The private companies with their internet projects have managed to bring more people connected to internet than government has managed to bring piped water to their houses finds a study in 2016 and counts are increasing for internet users from region (Parke, 2016). Many non IT corporate firms have initiated collaborations with IT firms to support initiative for providing internet like Coca Cola joining with BT Global Services (Sharma, 2014).

Technology firms do come together to protect the democracy after once Russia was able to manipulate in 2016 elections where even tech giants like Facebook failed to analyze the alleged attempts to manipulate voters (Winck, 2020). Later it is seen during 2020 election social media stepped ahead to ensure voters are kept away from misleading posts by marking them with warning sign and with passage of time analyzing threats they have started marking posts as "Manipulated video" which was first seen to be marked on a post in Twitter by senior party leaders and head of IT cell of BJP the ruling party of world's largest democracy (Balakumar,

2020).

Social media has stepped up its effort but not complete yet where the Twitter war between China and Australia has seen too much of spread like wildfire where national leaders of both nations are openly taking talking against each other's conduct, since war nowadays is mostly initiated at social media therefore platforms are increasingly seeing them as mediator and peacemaker (Ward, 2020). It is now a responsibility to be ensured by the social media platforms that so called "Twitter war" or debates in social media is not being exploited for spreading unrest in forms of trolling and verbal abuse of ordinary citizens and companies at large, as other non state and state backed groups might seize the opportunity to fuel the ongoing debate on social media platform for degrading relation between those two nations.

Private companies like Uber and Airbnb has managed to use internet in redefining user experience where Uber provided its customers with vehicles without actually owing one, similarly Airbnb being one of largest real estate chain actually does not have any property of its own and Alibaba the world's largest valuable retailer utilises software to manage flow of goods from factory to customer instead of storing them in their own inventory (Goodwin, 2015). Cyberspace has created scope and enthusiasm for youngsters and tech savvy guys in particular to become independent in creating opportunity for themselves without being dependent on government instead extending their contribution to government in form of tax and designing innovations to help law enforcement agencies.

The new upcoming innovations from startups are coming with more innovative ways in saving people from falling prey to fake news by using AI or algorithms which if not done can be a source for huge violence in real world. Post Snowden revelations when data breaches were being reported regularly that included personal information including hacks on medical facilities that disrupted healthcare systems in United Kingdom (Manos, 2013) the call was initiated to restore trust in internet and digital world first by technical bodies and then by international organizations. By 2015 the companies took efforts to collaborate with government in finding solution to threats where companies went on to step for a Digital Geneva Convention (Guay & Rudnick, 2017). Time when AI started to be used to redefine human machine interaction private firms understanding double edge potential of AI in 2017 urged UN to make regulation regarding law on development of AI weapons and ban of Lethal Autonomous Weapon Systems (LAWS) like killer robot (Saad & Gosal, 2019).

Microsoft in 2017 approached against stockpiling of cyber weapons to protect innocent civilians at times of cyber war when it's President and Chief Legal Officer Brad Smith in his keynote speech at Geneva mentioned about learning from each other community to address all challenges even went to highlight how US is increasingly loading its cyber arsenals for offense (Lamm, 2017). Microsoft led the six of world's largest technology companies Apple, Amazon, DeepMind, Google, Facebook, IBM, technological companies in 2017 to form industrial consortium represented by researchers known as Partnership on AI (PAI), which conducts researches and creates educational materials that further aids in advances in understanding AI technologies as AI is increasingly becoming part of daily lives. The consortium later included six non for profit board members making it a multi stakeholder organization which founding member feels will help in better outreach of AI for public good (Johnson, 2019). Next following year in 2018 Microsoft initiated an effort to ensure protection of users from malicious attacks form criminals and from state backed through an accord which had Microsoft and 34 top IT companies united for a common goal of secure cyberspace with "Cybersecurity Tech Accord" which pledges for a strong collective defence against cyber attacks and initiate joint development of cyberspace with other stakeholders which has now got more than 144 global IT companies and counting (Smith, 2018).

The Hague Centre for Strategic Studies (HCSS) and the EastWest Institute (EWI) for promoting awareness and uniting all stakeholders working for cyber security published in 2019 report titled "The Global Commission on the Stability of Cyberspace (GCSC)" to prevent cyberspace from becoming militarized and promote a sense of unity by bringing in all cyberspace actors to work together for cyber security and international harmony by contributing in policy reformation that can help in building global cyber security and cooperation (Kundaliya, 2020). Antivirus firm Kaspersky in its effort for bringing in improved transparence for effort of providing quality security solutions to users initiated "The Global Transparency Initiative" on October 2017 which is widely considered as a step towards its commitment of assuring integrity and dedication in its products. Kaspersky seeks to involve other stakeholders in authenticating its product codes so that trust on its product besides being available to any collaborations in effort of making cyberspace secure (Wong, 2018).

There are occasions when private companies have initiated process for global security and governments have joined like that of Siemens along with eight partners which initiated "The

Charter of Trust" for enhancing cyber security by framing regulations and standards to pave way for secure digital tomorrow. The charter focuses on protecting privacy, critical infrastructure and more transparency by joint initiatives with other stakeholders to bring in collective effort for safer digital world. The charter initiated by corporate(s) or Multi National Companies (MNC) is now joined by government agencies like the German Federal Office for Information Security and the National Cryptologic Center of Spain making it a multi stake holder model of governance in cyberspace (Buntz, 2019).

Private led initiatives in ensuring governance in cyber space

Treaty	Goal	Signed	Parties
Global Commission on the Stability of Cyberspace	To assist in promoting awareness and uniting all stakeholders working for cyber security	2019	The Hague Centre for Strategic Studies (HCSS) and the EastWest Institute (EWI)
Global Transparency Initiative	To improve transparence in effort of providing quality security solutions to users.	October 2017	Kaspersky
Cybersecurity Tech Accord	The accord pledges strong collective defence against cyber attacks and initiate joint development of cyberspace with other stakeholders	April 2018	Microsoft and 8 other companies initiated and now has 144 global IT companies still counting
Charter of Trust	It was initiated for enhancing cyber security by framing regulations and standards to pave way for secure digital tomorrow.	2018	Siemens and eight partners
Digital Security & Due Process: Modernizing Cross Border Government	To help countries particualrly the law enforcement agencies in obtaining required information or evidences required to	2017	Google

Access Standards for the Cloud Era	investigate legitimate cases saving precious time.		
International Cyberattack Attribution Organization	The utilise the expertise of private sector in a non-political way to analyse the evidence in establishing linkage of a state-backed cyber attack.	2017	Microsoft ,RAND

Table 8 - Initiatives by private companies for helping government and civil society in ensuring cyber governance (Source- Google)

3.2.3 Attempts by IGO

The governance of internet and cyberspace as whole is referred as regime where management of resources initiated political involvement due to rising conflicts with other existing international regime (Mathiason, 2009), regimes as discussed in last chapter is a set of principles or norms that help in maintaining global international relations has been formed to be centered on the nation state concept and not much an organization. Political scientists suggested institution of complex over regimes complex can help in solving challenges in complex domain as institutions are created after they have reconciled with other existing institutions (Aggarwal,1998), it is therefore considered that established international organisations can be utilised to frame the initial global governance architecture. United Nations generally referred as UN is an international inter governmental organization formed in 1945 to increase international relations and cooperation among its member nations through its agencies like ITU and UNESCO at global level are drafting the role for their contribution is process of global cyberspace governance and similar initiatives are being carried out at regional level by Council of Europe (CoE), OECD, AU etc which are defined as follows:

a) United Nations led initiatives

Global organizations are created to resolve conflicts and other issue whenever threatened but has not been able to effective as desired (Hallaert, 2020), it is often seen for a same issue two or three difficult coordination committee are set up leading to contradicting suggestions of each other not letting for a globally accepted solution considering UN whose members include almost all nations except few like North Cyprus , Somaliland who are not recognized by majority

international community and counties like Taiwan and Kosovo are also excluded as one or more powerful member nations feel their presence is not necessary as their independence is deemed unnecessary and void. UN formed two groups to find in much needed solution for cyberspace governance and report to its General Assembly one being the UN Group of Governmental Experts also known as GGE (2019-2021) and other UN Open-ended Working Group referred as OEWG (2019-2020) in response to rising threats of cyberspace being increasingly militarized by nations whose working can be found below.

UN led working groups on cyberspace for developing rules on behavior of state in cyberspace.

UN Group of Governmental Experts	**UN Open-Ended Working Group**
(2019-2021)	(2019-2020)
25 selected Member Seats	All interested UN Member States
Chair Brazil	Chair Switzerland
Consultations	
6 with Regional Organizations (AU,EU,OAS,OSCE, ARF, ASEAN Regional Forum)	Inter-sessional meetings with interested stakeholders (business, NGO, and academia)
2 with all Member States	
To address	
Norms, rules, and principles	(Further develop, or change) Norms, rules, and principles listed in A/RES/73/27 (par. 1)
Confidence building measures (CBMs) and capacity building	Confidence building measures (CBMs) and capacity building
How international law applies to cyberspace	How international law applies to cyberspace
UN GA A/RES/73/266	Existing and potential threats
	Establishing regular institutional open-ended dialogue within UN
	Relevant international concepts for securing global IT systems
	UN GA A/RES/73/27
Reporting to	
76th GA Session (2021), incl. annex with national contributions on how international law applies to cyberspace	75th GA Session (2020), on consensus basis
Timeline	
17-30 September 2019: 74th GA	3-4 June 2019: Organizational meeting
5-6 December 2019: Informal consultation for non-members	9-13 September 2019: 1st session
9-13 December 2019: 1st session	17-30 September 2019: 74th GA
24-28 February 2020: 2nd session	2-4 December 2019: Multistakeholder informal consultation

17-21 August 2020: 3rd session	10-14 February 2020: 2nd session
20-21 May 2021: Informal consultations	6-10 July 2020: 3rd final session
24-28 May 2021: 4th final session	15-30 September 2020: 75th GA-OEWG Report
14-30 September 2021: 76th GA-GGE Report	

Table 9 - The UN led two working groups (OEWG and GGE) on cyberspace (Source https://www.unidir.org/sites/default/files/conferences/pdfs/overview-of-the-group-of-governmental-experts-and-open-ended-working-group-processes-eng-0-786.pdf)

The OEWG and GGE mandates came to end this year in the month of March 2021 and May 2021 respectively, where two resolutions were approved by the UN First Committee one sponsored by USA and other by Russian Federation, the USA supported mentioned of deciding further plan of action upon considering outcomes from both OEWG and GGE whereas the second suggested the timeline for next OEWG from 2021-2025 (Gold, 2021).

Besides OEWG and GGE existing mechanisms under UN for finding solution to cyber governance includes World Summit on the Information Society (WSIS) that was outcome of UNGA resolution 56/183 adopted in 2002 an effort by UN-ITU along with other UN bodies and international organizations. WSIS was suggested for working in identifying the necessity to create strong cooperation among all international organizations and civil society at all levels of both regional and global to promote development in IT and allied technologies. WSIS was held in two phases first being in Geneva from 10-12 December 2003 and second one being held at Tunis from 16 to 18 November 2005 (Leuthard, 2018). The first phase raised for support to Geneva Declaration of Principles and Geneva Plan of Action which is based on principle for building the information society where as the second phase was to implement action plan of first phase the Geneva Plan of Action besides planning for a global internet governance, the second phases is also known as Tunis Agenda to be information as it suggested for multi-stakeholder governance model for governing the internet.

The same WSIS (World Summit on the Information Society) as defined in the Tunis Agenda is praised for leading to creation of IGF (Internet Governance Forum) as a successful outcome of the meeting, which assures to bring in global multi stakeholders and examine role and impact of ICT on the UNSDGs to ensure the betterment of the world at large has received kudos across globe for allowing all stakeholders to get equal opportunity for getting to express their view on framing global policy on cyberspace. The IGF is seen as a forum of no outcome as there is a lack of authority to implement the suggested or decided points to the global internet

usage but only functioning as a discussion platform encouraging all stakeholders to share opinion as its prime drawback lie in being a non decision making body. IGF first started on 2006 with theme of development has moved online due to COVID 19 in its latest yearly discussion which yet again concluded without solution to the complex challenges.

Internet Governance Forum themes over the years

Year	Place	Topic/Theme
2006	Athens	Internet Governance for Development
2007	Rio de Janeiro	Internet Governance for Development
2008	Hyderabad	'Internet for All'
2009	Sharm El Sheikh	Internet Governance – Creating Opportunities for All'
2010	Vilnius	Developing the future together
2011	Nairobi	Internet as a catalyst for change: access, development, freedoms and innovation'
2012	Baku	Internet Governance for Sustainable Human, Economic and Social Development'
2013	Bali	Building Bridges – Enhancing Multi-stakeholder Cooperation for Growth and Sustainable Development
2014	Istanbul	Connecting Continents for Enhanced Multi stakeholder Internet Governance"
2015	João Pessoa	Evolution of Internet Governance: Empowering Sustainable Development
2016	Jalisco	Enabling Inclusive and Sustainable Growth'
2017	Geneva	Shape Your Digital Future!
2018	Paris	'Internet of Trust'
2019	Berlin	One World. One Net. One Vision
2020	Online	Internet for human resilience and solidarity

Table 10 - Themes of IGF (Source - https://www.intgovforum.org/multilingual/ IGF)

Other offices of United Nations that has taken part in effort to ensure peace in cyberspace includes United Nations Office for Disarmament Affairs (UNODA) a specialized body of UN formed in 2007 which helps in achieving disarmament had earlier included weapon of mass destruction as threat but recently has added cyberspace to the list. The Agenda for Disarmament was launched in 2018 where the Secretary General has suggested two action points for disarmament in cyberspace first being the good office of secretary general will be used for preventing such unlawful activities. Second being the bringing in more unity and cooperation in cyberspace which will include in obeying of regulations and norms designed to keep account on member nations about their cyberspace behavior in order to ensure human rights is not violated of any ordinary citizens for which the Office of the High commissioner for Human Rights

(OHCHR), has acknowledged that progress in the ICT helped people to raise their voice against abuse and torture being done on them and others which are directly contribution to the goal for ensuring human rights protection for all which included. The United Nations Commission on Science and Technology for Development/CSTD set up in 1992 as a subsidiary of Economic and Social Council (ECOSOC) addresses the challenges that come as byproduct of the technological advancement where on the twenty second session in a path breaking resolution on the role of frontier technologies in fulfilling SDG which that included new technologies like Artificial Intelligence (AI), cyberspace, biotechnology as tools to achieve the Sustainable Development Goals (SDG) 2030 (Vinuesa et al., 2020).

The global development efforts by UN by United Nations Development Programme (UNDP) that was established by general Assembly of the United Nations in 1965 has included Information and Communication Technology (ICT) for development in it for achieving the goal of sustainable development running a number of programs at global, national and regional level including several pioneering task force like the Digital Opportunity Task Force (DOT Force) co-hosted by World Bank (WB) and UNDP created under the G8 (Ó Siochrú, 2007). UNDP also played key role in UN ICT Task Force which was launched in 2001 and later joined with CISCO systems and UN Volunteers to set up training academies for least develop countries. UNDP being core support body to UN system is responsible for providing digital support to it and under UNDP Digital Strategy 2019-21 it plans to harness technology to yield better results for all UNDP network (Opp, 2021).

The United Nations Office on Drugs and Crime (UNODC) came into existence in 1997 after merging of United Nations Centre for International Crime Prevention (UNCIC) and United Nations International Drug Control Programme (UNIDP) supporting and assisting the General Assembly resolution 65/230 and Commission on Crime Prevention and Criminal Justice resolutions 22/7,22/8 has been conducting extensive study of challenges and response of member states in handling cybercrime by its Open-ended inter-governmental expert group. The group has also initiated several programs like Global Programme on Cyber crime (GLOX76) aimed at helping countries to fight cybercrime and project Cyber CRYPTO which focus on handling illegal crypto currency usage in Association of Southeast Asian Nations (ASEAN) member region (Walker, 2019). The effort by UNODC comes at time when cyberspace is being increasingly used for selling and procurement of illegal contraband drugs through dark net and

other illegal online markets. The dark net threats have called United Nations Education, Scientific and Cultural Organisation (UNESCO) that was established in 1945 for promoting knowledge has acknowledged the need to include cyberspace in its list of areas for cooperation and it partnered with Dublin City University (DCU) to establish a dedicated centre for addressing online cyber bulling and other harassment in cyberspace (O'Higgins Norman, 2020). Other efforts by UNESCO includes organizing conference and including popular celebrities to join the cause and produce more effective results in their fight for countering threats available in cyber world especially in Dark Net which acts as epicenter for issues like child pornography and radicalization.

In another effort related to elimination of discrimination by UN under United Nations Convention on the Elimination of all forms of Discrimination Against Women (UN CEDAW) defined measures to prevent discrimination against women has recognized cyberspace as an emerging theatre of threat for discrimination against women and same is recognized vide General Recommendation No. 26(2017) which suggests in taking actions to help in fighting the cyber bullying, blackmailing ,exploit, threaten or revenge needs immediate response at national level or international level as most criminals are based across border (Arimatsu, 2019).

The increasing threat to lucrative aviation industry which owing to its potential of holding user data has also been on the list of cyber attack besides the aviation sector is also a direct contributor to nation's economy and one successful casualty can lead to severe loss of life and national reputation. The threat actors to aviation ranges from state sponsored to cyber criminals as compromising airport can allow belligerent states to create backdoor for hijacking control system whenever they want and other intentions might include hacktivism and financial related crimes where the airport WiFi can be compromised to install malicious code in the users phone for getting in emails and other bank related details which can be sold in dark net for money. All above threats have called the UN's International Civil Aviation Organization (ICAO) established in 1944 as a specialized agency of United Nations which works in regulating governing of civil aviation in coordination with 193 member states to jointly come to agreement on topics related to safety and other civil aviation rules and established the Secretariat Study Group on Cyber security (SSGC) to design a framework on challenges the domain faces from cyberspace and how to address them.

Since the time cyberspace started gaining momentum it was predicted to be important

tool for most future business and transactions calling in for global monitoring, as there is increasing use of personal data and loss of money through financial crime involving transnational elements where threats from cyberspace is seen increasing on financial sector. The World Bank (WB) founded in 1944 which is an international organization and source of financial and technological support to developing countries across globe has initiated various programs and infinitives exclusively designed for developing countries to address cybercrime which includes sharing best practices, self-assessment tools , and a virtual library which helps the nations to develop better capability in handling issues to Information and Communication Technology (ICTs) (Tunji, 2021). World Bank (WB) is also part of the Financial Inclusion Global Initiative (FIGI) a three-year program designed to support and help in achieving the global Universal Financial Access 2020 goal. The WBG as part of the Security, Infrastructure and Trust (SIT) Working Group has led initiative of the FIGI Cyber security for Financial Market Infrastructure Work stream, which focuses on finding best practices on cyber security for financial architectures. The group has also published two reports being the Financial Sector's Cyber security Regulatory Digest, which analyses existing regulations including cyber laws related to financial sector and second being a paper on Financial Sector's Cyber security Regulation and Supervision which identifies the nuances needed when sharing of regulatory or supervisory power in relation to financial sector and state other agencies come as dependency on ICT technologies has increased involving multiple stakeholders.

The other notable organization can be expected for bringing in global cyberspace governance is ITU (International Telecommunications Union) a part of UN which deals with information and communication technologies (ICTs) responsible for granting radio spectrum and satellite orbits besides framing global technical standards. Being an UN body it works with all member nations it manages to reach nations including under developed and nations with lowest number of ICT users, yet this organization cannot be vouched for a multi stake holder governance unit as it involves only the respective state's government to send in representative and take the decision to frame policies. The International Telecommunication Union/ITU is a specialized agency on Information and Communication Technologies (ICT) of United Nations founded in 1865 as International Telegraph Union and on 1932 it got its current name finally joining UN on 1947. ITU' main responsibility stands to add security in ICT as per the guidance of World Summit on the Information Society (WSIS) and ITU plenipotentiary conference where

it is undertaking initiatives like cyber drills at regional and national level to gauge the readiness of nations and also bringing in unity by bringing in several member nations take part in such drills and also provides hands-on exercises for national cyber response teams like Computer Incident Response Team (CIRTs) or Computer Security Incident Response team (CSIRTs).

Although WSIS initiative has been acknowledged as foundation for management of cyberspace and since then it is observed that Intergovernmental bodies at regional level adding the element of cyberspace in their agenda for focusing on collaboration on cyber issues are as follows:

b) Europe

The European Union (EU) was formed in 1993 which aimed in overcoming barriers which will help all citizens from its member nations in achieving peace, freedom, and other rights to live in the region as regional citizen and not merely of its own country alone. The member of EU has collectively acted against all threats arising or coming towards region, recently the union has identified cyberspace as a domain of threat to its digital market and harmony which paved way for Cyber Security Act 2017, the digital threats are managed by ENISA (European Union Agency for Network and Information Security) which acts as nodal agency for threats arising in region (Markopoulou, Papakonstantinou & de Hert, 2019). The EU is also working for a establishing a single cyber security market and a secure election procedure besides a united cyber defense mechanism to counter any offensive threats arising from anywhere in virtual world (Perez Grandi, Sarri & Paggio, 2021).

Europe also has the Council of Europe (CoE) formed in 1949 is another international organization which is not part of UN but a regional organization and joined WSIS, better known by one who enforced landmark Convention on Cybercrime widely referred as Budapest Convention stands as first of a kind multilateral international treaty that gave foundation for nation states to work together in uniting against cyber related crimes (Gillespie, 2019) The convention which was opened for signature on 2001 and came to force in 2004 acts as reference for many developing nations who have not framed their cyber policies taking into concern the human rights issues across society like xenophobia and racism on digital platform as it has added cyberspace as domain for collaboration and adopted the Convention on Cybercrime and its Protocol on Xenophobia and Racism, the Cybercrime Convention Committee (T-CY) and the

technical cooperation programmes on cybercrime to ensure security in cyberspace across globe (Nettey, 2019). CoE's leadership in initiating first European Dialogue on Internet Governance (EuroDIG) which is also referred as regional IGF is widely acknowledged to bring in awareness related to management of cyberspace at regional level that was followed by other regions as well (Taylor & Hoffmann, 2019). Besides the Budapest Convention on Cybercrime (2001) other initiatives to address issues related to cybercrime includes the convention of the Prevention of Terrorism (2005) prevents using internet for influencing and promotion of terrorism, the Lanzarote Convention (2007) for protection of child against exploitation, the Modernization of Data Protection Convention "Convention 108" to address new threats to privacy (Dashab, 2018). The Budapest Convention is opened to both members and non member nations of Council of Europe where the convention is accorded as one of first concrete guidelines for dealing with cyber crimes which also includes breaches like intellectual property, copyright and network security. The conventions also suggest for a unified approach for fighting common goals that can increase coordinated efforts internationally.

Europe has been on forefront when it comes for promoting regional security and it has the Organisation for Security and Co-operation in Europe (OSCE) which formally came to existence on 1994 after getting its name changed from the Organization for Security and Co-operation in Europe (OSCE). The body has added ICT and cyberspace as a domain for cooperation and increased mutual security by adding more members from other regions for enabling better cooperation and decreasing tension among member nations over usage of ICT and handling threats arising from cyber criminals or other non state actors (Abdullin, Davletgildeev & Kostin, 2020).

UN also has its representation in the Europe region for supporting the working of United Nations as facilitator in implementing outcomes of global United Nations conference summit in the region and also acts as nodal point in binding rules and regulations to promote international cooperation within and outside region, it has one of the five regional organizations United Nations Economic Commission for Europe (UNECE) established in 1947 by ECOSOC to create economic integration among its member countries and promote SDG through dialogue and technical cooperation. UNECE has also taken initiated like constituting task force as a subgroup to the Informal Working Group on intelligent transport system/automated driving to address cyber security threats in transportation system in the region (Burns, 2005). Europe also has multi

stakeholder initiative comprising states, organization and companies established in November 2018 the Paris Call for Trust and Security in Cyberspace that invites all stakeholders to work together for fighting threats to citizens and infrastructure that has contributed to Europe being one of leader in matter of cyber security across world (Lété, 2021).

c) Africa

International cyber regime which is aimed to highlight the areas of coordination and cooperation must also find in areas where there is no joint action in order to ensure no options left for misinterpretation or promoting distrust. Till now there have been multiple efforts to establish cyber regime by multiple organizations but could not get the global success as most of the proposed regime talks on importance that are more bounded by regional, cultural and other norms. Taking example of Africa which is believed to be origin of human civilization has their own regional organization the African Union (AU) that launched a Convention on Cyber Security and Personal Data Protection focusing in addressing rising challenges to internet users from cyberspace over issues like data protection and privacy (Ball, 2017). This convention talks in ensuring that every member nations makes necessary amendments or addition to respective state cyber law in order to ensure security in cyberspace, where it mentions for establishing Data Protection Authority (DPA) institute at national level for processing of data which will be under strict guidance of convention in order to protect privacy of individuals urging in create unified regulations and response mechanism for addressing rising privacy and security threats from cyberspace to citizens of African Union.

The region of Africa has acknowledged the growing need to address the rising concerns of cybercrime in region and keeping in mind that its crucial in the digital age to incorporate technologies like ICT in African's progressive goals and also ensue that these technologies are used for benefit of African citizens, institution and nation-states by ensuring data protection and online security. The African Union drafted the "African Union Convention on Cyber Security and Personal Data Protection" in 2011 which targeted in introducing a framework for cyber security in Africa focusing on electronic transaction, personal data protection and cyber security and cyber crime , the treaty was adopted in June 2014 after postponing it on several occasions and is yet to be ratified by all member nations (von Solms, 2015).

The African Union (AU) is a representation of a united vision for building a united and healthy pan-Africa, steered by its citizen in the global arena which came to existence in 2002 by

replacing the Organisation of African Unity (OAU) comprising 55 African nations has further sub regional groups which have their initiative and opinion on cyberspace like the East African Community (EAC) Member nations on 7 May 2010 signed Framework for Cyberlaws ("Framework") to initiate reformation in national laws for protecting rights of users and improve relations among members (Okuttah, 2010). The framework suggests a series of modification which can be implemented in existing national laws to make citizen's use of internet safer and also develop better relationship among member states to stand as example for best practices worldwide. The Economic Community of Central African States (ECCAS) on December 2016 adopted Declaration of Brazzaville (adoption of Model Laws in ICT and Cyber security) to support the sub region in achieving success in digital transformation (Seewoosurrun, 2016). The framework guides sub region for initiating development of ICT related activities under regulation in order to boost citizen's morale and also protecting their online security besides developing for digital economy in the region. The Economic Community of West African States (ECOWAS) signed agreement Directive on Fighting Cyber Crime within the region on 2011 with all member of ECOWAS that aims to identify critical areas of cyber related crime and implement regulations for violations (Tamarkin, 2015). The Directive identifies critical areas of cyber related crime which includes manipulation, interference to computer network, fraud committed using computer and others including child porn. Another group formed by 21 member nation the Common Market for Eastern and Southern Africa (COMESA) adopted Cyber crime Model Bill on October 2011 to provide a framework for countering threats of cybercrime which aims in drafting a framework for member nations in addressing crimes and issues related to cyberspace, the bill also suggests on working together at national level for ensuring effective legal bindings on cybercrime besides ensuring users of getting full access of cyberspace and explore diverse resources safely. On similar line the Southern African Development Community (SADC) on November 2013 adopted Model Laws on Cyber Security; Cybercrime, Data Protection and Electronic Transactions to frame a unified cyber law for the region to provide citizens better security from transnational cyber threats, providing guidance on regulation of cyberspace by member states to address increasing regional cyber related crimes besides focusing in building better global ties to promote information security (Hove, 2017).

These different organizations are unable to work to make the region support for a uniform law making. Some countries like South Africa (Mzekandaba, 2019) and Nigeria turn to be a

favorite for cyber criminals due to poor regulations. The crucial part being cyber security dilemma where centrally located Cameroon was in a dilemma whether the training imparted to youths and professional for creating cyber security team should not be misused for conducting cyber crime only in the country or on other nations (Chimtom, 2016). Further looking at countries which have their own individual security architecture like Kenya which adopted its data protection act on 2019 on similar grounds to Europe's sees that country will not be able to make gain from cross border data flow and besides that other members in AU has not made similar changes in their framework where the debate between data protection and anonymity is still discussed that at large is still causing hindrance to attacks originating as well as targeting AU nations (Issaias, 2019).

d) Asia and Asia pacific region

At Asia pacific region the 21 member states Asia Pacific Economic Cooperation (APEC) forum for promoting regional economic progress established in 1989 has added Information and Communication Technology (ICT) as one of the areas of cooperation for bringing effective measures on the domain. The region being a key strategic location it receives proposals of cooperation from powers like China, Russia and US to initiate join ventures for ensuring their connectivity in key affairs supporting the trade (Stronski & Ng, 2018) .The region's tech giant Singapore has established a five year project in 2019 called the ASEAN - Singapore Cybersecurity Centre of Excellence which will enable in boosting cyber security capabilities in the region (Gan, 2021). The region even receives support from private companies where recently in 2021 Microsoft launched the first Asia Pacific Public Sector Cyber Security Executive Council which is targeted in establishing a discussion forum comprising representatives from multi stakeholder including government agencies to strength the region's cyber capabilities (Smith, 2021).

Asia Pacific also has regional establishment like the UN ESCAP or Economic and Social Commission for Asia and the Pacific of UN for supporting and promoting cooperation among regional member nations which will led in achieving the SDG 2030, UNESCAP (United Nations Economic and Social Commission for Asia and the Pacific) has published working paper series Asia Pacific Information Highway (AP-15) Enhancing Cyber security for Industry 4.0 in Asia and the Pacific which provides critical analysis for challenges that are needed to overcome in establishing the Asia-Pacific Information Superhighway (AP-IS) which ensures to make internet

available to population in region which is becoming as basic need of human in this digital age (Garrity, 2020).

Understanding the need for internet by citizens is acknowledged if not denied by almost all nations but the degree of involvement including censorship varies from countries to countries and Asia holds powerful actors like Russia and China who are in support for asserting state control over internet which they claim as nation and through their groups like Shanghai Cooperation Organisation (SCO) came to function in 2003 comprising 8 countries. On 16 June 2009 signed an agreement on Cooperation in the Field of International Information Security to create cooperation among member nations for prevention against use of internet for terrorism and other disruptive activities (de Alcântara, 2018). SCO brings member nations together in identifying on collective measures for promoting and observing information security globally. The member nations must be ready for addressing threats arising from use of ICTs for disruption purpose where it also urges amendments in state legislation if required for promoting global information security using ICT. The group has also initiated International Code of Conduct in Information Security often referred as "Code" as a collective effort by members to suggest norms for global approach in cyberspace initially submitted to UN in 2011 and later a revised form in 2015 with support for establishment of an international norm (McKune, 2015). Members of SCO highlighted the need for an international order to address information security as there have been events of cyber attack in gaining access to critical resources and information concerning states. "Code" takes into consideration of efforts taken by UN GGE on field of information and telecommunications in context of International Security. Another Russia led consortium the Commonwealth of Independent States (CIS) where other members like Ukraine, Belarus and Kazakhstan on 1 June 2001 established agreement on Cooperation in Combating Offences related to Computer Information to progress for cooperation in fighting crimes using computer and digital network and bring effective re-addressing mechanism for enforcing legal actions on it (Maroz, 2019).

The dominance of powerful and bigger actor China in the region has often challenged the existence of other smaller nations especially with their sovereignty at south china sea and impact of which can be felt at cyberspace as well which led to creation of a southeast regional intergovernmental body the Association of South East Asian Nations (ASEAN) of 10 members which was established to boost economic among its member nations. ASEAN has realized

importance of cyber security and added in its area of cooperation in its annual summit of 2019 (Haworth, 2019) and have planned to release a future plan in coming time as how to establish a digital regional cyberspace governance architecture. As the world is moving to digital economy the threats to region is being analyzed to prevent any attack on regional economy as the region has been target of several large scale cyber attack over members like Indonesia and Singapore adds more worries. The ASEAN Regional Forum (ARF) consisting of 27 member promoting regional security has acknowledged Cyber Security as one of the domain for regional cooperation and now cyber security has been considered as arena of critical importance with increased effort for initiaing colelctive mechanism to prvent cyberciem in the era of digitla economy (Farzan, 2021).

e) American continent

America continent both North and South combined can be referred as economic power house especially North American region comprising US, Canada and Mexico which holds a large chunk of global GDP. The region also has multilateral agreements for undertaking secret cyber operations like the UKUSA agreement widely known as 'Five Eyes' comprising USA, Canada, UK, Australia and New Zealand which came to limelight after NSA contractor Edward Snowden revealed of the their activities. United States has long maintained controlled over ICANN the first body managing the global internet directory and wishes to do so through means of such secret cyber alliances that do not even leave the ally leaders from surveillance whereas on the front it has supported for free speech extending cooperation to nations in development (Beens, 2020).

In terms of inter governmental body one of region's oldest bodies the Organization of American States (OAS) established 1948 has included cyberspace in as one of newest area for collaboration to fight challenges arising due to increasing dependency on it. OAS through its General Assembly has agreed to work on cyber security on priority through its special Secretariat CICTE or Inter-American Committee against Terrorism suggesting in establishing of Computer Security Incident Response Team (CSIRTs) known as Computer Security Incident Response Teams (CSIRTs) for every member nation who in turn will share data for mutual support and handling crimes committed in cyberspace under special portal with Inter-American Telecommunication Commission or (CITEL) is one such a special initiative which has worked on cyber security development in the region (OAS, 2012).

The region has common forum known as Caribbean Community (CARICOM) comprising 15 Caribbean states but lack a comprehensive cyber security architecture makes other powers to involve like the Early Warning Cybersecurity System was implemented with support from OAS to boost the Jamaica' Cyber Incidence Response Team JaCIRT (Mcintosh,2021). The UN' Economic Commission for Latin America and the Caribbean (ECLAC) continuously working in analysing the cyber security preparedness and highlighting the areas where improvements are required, besides ECLAC is also involved in promoting use of ICT towards achieving the sustainable development goal (SDG) in the region (McCartney, 2020).

Even with multiple organizations at place in same region there are still cyber attacks observed in past that took down government websites and the region being a place where money flows in regularly from overseas is expected to be under cyber criminals target and absence of any stronger actor makes it obvious to involve US or any European nations to their infrastructure which itself is compromising the regional integrity (Jackson, 2021).

f) Pacific island region

In the Pacific region the Pacific Islands Forum Secretariat which got the name on 2000 earlier referred as South Pacific Forum compositing 18 member nations is premier regulatory body which region jointly decided to add cyber security as one of elements for regional security declaration was necessary and accordingly Boe Declaration 2018 was framed which focused on protecting Pacific people from digital threats (McNeill, 2021). As Oceania remains a key interest of all major global powers as discussed in last chapter due to its geo-political positioning and also due to higher concentration of submarine cables which holds large chunk of global data generated across world , it has seen involvement of other bodies like ITU and regional power Australia which is also an ally of United States in creating Cyber Cooperation Program that includes other stakeholders from pacific to work in ensuring security to cyber assets (Rudolph, Creese & Sharma, 2020).

g) Organizations based on non-regional/ multilateral grounds

The G8 or Group of Eight is a initiative by 8 leading nations for addressing global challenges, which covers all international topics that helps in shaping a better international relations not only among member nations abut with others. The forum at its G8 meeting of Justice and Interior ministers on December 1997 has agreed to work together in adopting law for cooperation in cyberspace among all member nations and preventing cybercrime by creating a

network for supporting each other in identifying cyber criminals operating across border (Hart, 2005). The forum has established joint network to fight against high tech cross border crime at their 24/7 Cybercrime Network (Ott, 2018).

Even at the level of global trade , World Trade Organization/WTO renamed on January 1, 1995 as successor to General Agreement on Tariff and Trade (GATT) which was established in 1948 to regulate trade regulations has implications on cyberspace. In this digital age when cyberspace has become a key trade component, member states have raised queries on issues related to high end technological products as amount of issues are increasing from this products ranging from espionage, data breach to data theft (Meltzer & Kerry, 2019). The nations have accused each other in issues related to stealing of trade secrets and violation of Intellectual Property Rights (IPR) which is referred to a violation of WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs). WTO can be utilized to introduce a concrete digital industrial policy which can be applied at national and regional level to address the trade issues in cyberspace and even collaboration with World Intellectual Property Organisation (WIPO) which is working on global debate to frame regulations for copyright protection in cyberspace by its two treaties — the WIPO Copyright Treaty and WIPO Performers and Phonograms Treaty widely known as "Internet Treaties" both came to force in 2002 to protect the intellectual property as internet started expanding, these treaties will update major treaties on copyright and related rights that already exist (Agarwal & Agarwal, 2016).

h) Faith based regimes

Cyberspace which often sees in push for virtual borders by states on claiming sovereignty over cyberspace has found efforts on creating regime based on religious lines as well where the League of Arab States on 21 December 2010 signed "Convention on Combating Information Technology Offences" to develop unity and collective partnership among Arab member nations for addressing digital threats and challenges that in accordance of Islamic Law (Shari'a) comes under crime (Hakmeh, 2018). The initiative suggests in adopting a common policy for addressing such crimes committed towards citizen using IT enabling individual and members who are followers of Islamic Law to be safe in digital world with collective action against threats originating to their communities in digital space bringing in regimes based on religion and is

supported by 22 member nations of League of Arab States.

The highly oil rich region falls victim to large scale cyber attacks largest being on ARAMCO making the Cooperation Council for the Arab States of the Gulf (Gulf Cooperation Council-GCC) which did not join the Budapest Convention brings the need to either deploy a strict security architecture or to focus more on addressing challenges with collabrating other nations (Murphy & Sheppard, 2021). Another organization formed on basis of religion the OIC (Organisation of Islamic Cooperation) has established CERT by passing resolution signed by all its member nations to ensure protection to all member nations against any attacks in their digital infrastructure but is often questioned with their alliance to China as China is alleged to provide illtreatment to its Uighur Muslim population (Hooper, 2021).

i) Law enforcement bodies

For policing matters the International Criminal Police Organisation (INTERPOL) which got its present name in 1956 from its earlier International Criminal Police Commission was created in 1923, INTERPOL now comprises 194 member nations having its own Cybercrime Threat Response Team at its Cyber Fusion Centre to find ransomware and other threats that come up during the COVID 19 phases. INTERPOL identified the potential for a possible ransomware pandemic which can be caused by hacking or disabling all devices connecting critical infrastures to cybersapce inclduing healthcare systems using ransomware (Tung, 2021), it also proposed the need to partner with private sector cybersecurity firms, government agencies and computer emergency response teams (CERTs) to disrupt global ransomware gangs.

At the regional level the Europol is premier law enforcement network comprising of 27 European Union member states who are working to address issues like terrorism, cyber aided crime and other serious offenses often in association with other nations outside EU and other international organization. The European Cybercrime Centre or EC3 was founded in 2013 by Europol which focus in giving response to cybercrime in region and protect all citizens and government assets in cyberspace, in this attempt EC3 also is credited for initiating actions on several illegal markets in dark web (Foltýn, 2018).

Since there is deterrence prevailing in cyberspace where nations are secretly developing cyber offensive capabilities many nations have included cyber space as a theatre of cooperation in their military alliance group like the North Atlantic Treaty Organisation or NATO that was established in 1949 as an alliance of 28 nations bordering Atlantic Ocean. The increasing threats

from cyberspace the member nations have decided that a cyber attack on one member is an attack on all and has accepted cyberspace as fifth domain of warfare on July 2016 creating its NATO Cyber Rapid Reaction team as peace keeping force for its member nations (O'Connor & Jamali, 2020). NATO earlier had made its own Cyber Defence Policy that members on September 2014 agreed to include cyber defence as part of NATO's collective defense for its members against all threats in cyberspace and further boosted cooperation in matters related to cyberspace among member nations. NATO pledged to exert same measures for members in cyberspace that it provides in other recognized domain against threats to any member nations. The group decided on ensuring highest security to its communication system and group owned assets from cyber attacks and agreed on sharing knowledge and best practices among member states.

List of initiatives by Inter Governmental Organisations in managing cyberspace

Region	Treaty Name	Goal	Adopted/ Signed	Parties
African Union	African Union Convention on Cyber Security and Personal Data Protection	To create unified regulations and response mechanism for addressing rising privacy and security threats from cyberspace to citizens of African Union.	27June 2014	54 African nations, members of African Union (AU)
League of Arab States	Convention on Combating Information Technology Offences	To develop unity and collective partnership among member nations for addressing digital threats and challenges for enabling individuals and society of Arab States to be safe in	21 December 2010	22 member nations of League of Arab States

		digital world.		
Caribbean Community (CARICOM)	Model Legislative Texts of Cybercrime/e-Crimes	Model legislation guidelines for prevention and investigation of cyber and electronic related crime	2012	Report
Common Market for Eastern and Southern Africa (COMESA)	Cyber crime Model Bill, 2011	To provide a framework for countering threats of cybercrime	October 2011	21 member nations of COMESA
Commonwealth	Abuja Declaration on the Proposed Commonwealth Cyber Governance Model	The Declaration calls for creating a model for cyber governance which can be adopted by commonwealth and non commonwealth nations as well which will help in promoting peaceful coexistence in cyberspace	2013	all members of CTO
Commonwealth of Independent States	Agreement on Cooperation in Combating Offences related to Computer Information	To establish cooperation in fighting crimes using computer and digital network	1 June 2001	CIS members Russia, Ukraine, Belarus and Kazakhstan
Council of Europe (open	Convention on Cybercrime	Convention addresses crimes committed	23 November	members and non member

for non-member States)	(Budapest Convention)	using computer network and internet.	2001	nations of Council of Europe.
East African Community (EAC)	Framework for Cyberlaws ("Framework")	To initiate reformation in national lawa to protect rights of users and improve relations among members.	7 May 2010	EAC Member nations
Economic Community of Central African States (ECCAS)	Declaration of Brazzaville (adoption of Model Laws in ICT and Cyber security)	To support the sub region in achiving success in digital transformation.	December 2016	ECCAS member states
Economic Community of West African States (ECOWAS)	Directive C/DIR. 1/08/11 on Fighting Cyber Crime within ECOWAS	To identify critical areas of cyber related crime and implement regulations for violations	19 August 2011	15 ECOWAS member states
European Union	Directive on Security of Network and Information Systems (NIS Directive)	To boost cyber security cooperation in EU	July 2016	EU member nations
Shanghai Cooperation Organisation	Agreement on Cooperation in the Field of International Information	To create cooperation among member nations for prevention against use of internet for terrorism and	16 June 2009	SCO member nations

	Security	other disruptive activities.		
Southern African Development Community (SADC)	Model Laws on Cyber Security; Cybercrime, Data Protection and Electronic Transactions	To frame a unified cyber law for the region to provide citizens better security from transnational cyber threats.	November 2013	SADC members
French Republic	Paris Call for Trust and Security in Cyberspace	The Paris Call invites all stakeholders to work together for fighting threats to citizens and infrastructure.	12 November 2018	multi stakeholder initiative comprising states, organization and companies

Table 11- List of Intergovernmental Organisations and their attempt in establishing cyber governance (Source -Google)

3.2.4 Attempts by civil societies

The impact of cyberspace and technology on society cannot be denied; it not only acts as a platform for communication, business and interaction, but has made life easy for all users connected across globe. Civil societies popular with general audience as Non Governmental Organizations (NGOs) are mostly nonprofit organizations and sometimes with international presence often funded by government agencies but acts independently from their control. NGOs now stand on consultative role to many international groups like ECOSOC and several other initiates who add to efforts initiated by respective governments and organizations for developing society as whole which NGOs today take roles from lobbyist on policymaking to an observer to society at global platform by acting as a monitoring body to major government initiatives like eradicating diseases.

World politics and international development have undergone a radical transformation mostly because of increasing globalization. A unique characteristic of this transformation is the

increasing number and type of stakeholders organized into interest groups or nongovernmental organizations (NGOs). NGOs influence on public policy at local, national, and global levels and in nearly every aspect of policy-making and international relations has made them dominant actors in the development arena. Today at the time when the debate between multi lateral and multi stakeholder form of governance for governing the cyberspace remains the debate it is mostly the NGOs that are running it starting from beginning and till now who have managed to ensure internet continue to flourish despite several hurdles coming to it. As cyberspace has started to expand and empowered all walks of life it has also brought in more threats from cyber criminals either working individuals or supported by nation-states. Attacks varies from hacking mails or comprising system to use for Denial of Services (DoS) and Distributed Denial of Services (DDoS) attacks to ransomware and spywares for generating money, these attacks can impact every individual from common man to government and critical infrastructure architecture of country. The attack on any one above will impact life of common individual if not direct then its consequences as in a situation when an attack is waged on nation's critical infrastructure citizens are not directly concerned for it but the fact that they will not have power supply for next few hours and would not be able to charge their devices and cook impacts them socially and psychologically. The impact of psychological attack remains critical and long lasting over physical attacks as these types of psychological attacks leads them to be rebel online against either their own government being incapable of providing security or accused nation who has given such trauma. Victims of cyber attack suffer more emotionally than financially and national government's approach to mental health is often ignored this is where NGOs have played in great role to ensure that the victim returns to use internet facilities in future but with more cautious and secured way where they often make a group of other victims with ones who have overcome to interact and gather in courage and support for getting over the incident. A remarkable effort that helped in pushing the civil societies involved in cyberspace governance was in 1990 when the Association for Progressive Communication (APC) was established as a platform for global networking of civil societies by joint initiative of seven organizations Nordnet, web, Ibase, Nicarao, Pegasus, Institute of Global Communications and Greennet and now forms support to many victims of cyber bullying and harassment (Wickrematunge, 2018).

Since then there is a notable transition observed where numbers have increased and with advancement in technology and social media now in remote areas also NGOs are set up. NGOs

has taken initiative to ensure that global communications like internet are available to both poor and rich and there are several examples which stands as witness to positive roles played by NGOs in shaping society (Willmer, 2016). NGOs which often function with limited funding have been using internet to spread activism and there are several examples of it across globe now who have contributed in both ensuring digital security to users and also contributing to policy formulation.

a) Civil society initiatives in cyber governance

The race for gaining superiority in cyberspace among nations often make ordinary user either compromise its privacy or remain outside the of it, as the digital race gained momentum a gap was observed to increase between nations widely denoted as digital gap where developed nations progressed to integrate their daily life with internet and countries in Africa are lagging behind which made in nonprofit organizations to which work with vision for making internet safe and stable for every individual irrespective of any discriminating factors accordingly the World Wide Web Consortium (W3C) established in 1994 as a global forum comprising of representatives from different stakeholders are working together for framing web standards that also joins and coordinates with other cyberspace regulating organizations like IETF and Unicode Consortium to able to explore the potential of internet. The father of internet Sir Tim Berners-Lee formed his own foundation the World Wide Web foundation to lead a global digital equality where people can come and access the internet to make life better for all (Hannan, 2021). World Wide Web also hosts the Alliance for Affordable Internet or A4AI which brings in leaders from all societies across globe to contribute in policy framing that can lead to reduction of internet cost for making it affordable for all so that no global citizen can miss experiencing digital revolution.

While making information easily accessible and promoting globally remains priority emphasis also taken to cater for person with disabilities where Centre for Internet and Society (CIS) founded in 2008 works by undertaking research related to accessibility of internet for users with special needs with their needs in internet governance, privacy and security, CIS also works on policy and academic aspects that have impact from internet and ICT technologies making it a multidisciplinary research on the internet equally available for all much beyond the digital gap over area to transform the world for all (Krishnan & Ranganathan, 2009). The transformation happened in world after popularity of internet is being experienced by majority of population in

their daily life and cyberspace has now become a place for online activism as well where movements are initiated against issues though online gaining in mass support not only from region but worldwide and Electronic Frontier Foundation (EFF) established in 1990 works for that by securing rights of individuals in digital world through grassroots activism, policy analysis and more comprising a team of experts from all stakeholders of internet who work together in ensuring safety of rights with this technological advancement to help in creating a better world (Kelley, 2021).

b) Civil Societies in Cyber security

NGOs besides working for promoting reach of internet to citizens have also focused on promoting security for the users of which was mainly confined to securing the education domain which stands valuable in this era where pandemic has forced in for online learning even for kindergarten students which has often made innocent kids victim of online harassment including sexually and to counter such misadventures (Stifel, 2019). Efforts from US based nonprofit organizations established the Cybersmile foundation in 2010 has stepped up efforts to promote unity and diversity by ensuring a peaceful digital community in cyberspace with their professional help and counseling to reduce cyber bulling and other different forms of online abuse and torture, another non profit organisation HeartMob also performs same type of support to needy interestingly in real-time which later helps in guidance and recovery of the victim over it besides working on the eradication of online harassment (Kulenkampff, 2021).

Based on regional based approach the European Union also has seen efforts related to identification of fake news from its non for profit DisinfoLab that undertakes research in preventing disinformation that is being targeted towards interest of any EU member nations and citizens by ensuring that they are less prey to misleading information especially on social media. Disinfolab is credited for exposing links of terror groups with other orgnisations who attempt to create chaos like the Pakistan' ISI involvement in fueling tensions in Indian region of kashmir (Singh, 2021).

3.2.5 Technical community

Long before Facebook, Twitter became popular representation of social media networking there was a social media networking known as Interdoc formed in 1984 by International Coalition for Development Action or ICDA which is first global online networking exclusively for other nonprofit agencies (Murphy, 2020). The first known governance institution

for internet management was established in 1998 by United States as nonprofit entity with partnership of enthusiasts who dedicated their love for ensuring safety and stability in internet that exists till date as Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is the apex body who plays role of observer in internet and also assigns specific identifying number to websites so that when an address is entered in address bar it reaches the desired destination (Marda, 2016). ICANN also hosts the department of IANA (Internet Assigned Numbers Authority) which is responsible for sharing internet number to regions for internet use and updating changes in TLD (Top Level Domain) information. Apart from ICANN the development of today's cyberspace has come from nonprofit organizations that includes Internet Architecture Board (IAB) , Internet Engineering Task Force or IETF, Internet Engineering Steering Group (IESG) to works towards managing the technical aspects in activities of IETF (Internet Engineering Task Force) and Internet Standards. IESG is responsible for the protocol develop that runs the internet that later paved way for the Internet Research Task Force (IRTF) in 1989 comprising several research groups working in promoting research related to internet in field of protocol applications and technology (Kruger, 2016).

IETF which acted a forum for information exchange between all stakeholders of internet and like minded individuals from IETF who believed that internet belongs to all and it is a medium for uniting people to transform lives in 1992 formed the Internet Society with regional chapters across globe working in promoting digital networking and also establishes Internet Exchange Point or IXP to keep local data traffic to local for getting cheaper and faster local traffic flow to increasing user base. As more and more systems started connecting internet to form a network which we refer as cyberspace there was a need felt for involving the civil societies to represent the larger section of users who remains poorly represented when it comes to framing governance as it was either the technical or government that had played role in managing. The foundation for management of the large resource of websites has been managed by technical team led nonprofits the Number Resource Organization (NRO) as coordinating body for Regional Internet Registries (RIRs) established in 2003 to oversee working of RIR who further ensures the sharing of internet address (IP address) within their region. There are 5 RIRs viz AFRINIC (Africa Network Information Centre), APNIC (Asia Pacific Network Information Centre), ARIN (American Registry for Internet Numbers), LACNIC (Latin America and Caribbean Network Information Centre), RIPENCC (Réseaux IP Européens Network

Coordiantion Centre). The contribution or efforts of non profits are not limited to governance they are found to be equally supportive to users in ensuring social development and security making them a bridge between government and users (Beijnum , 2010).

It is only possible through cyberspace that a happy moment captured can be shared with others located far away even after days through shared drives and files and with Internet Archive founded in 1996 which started by archiving internet a single website page now has billions of webpage and digital version of books holding data of even 20 years back. Often referred as wayback machine the internet archive helps in retrieving data which are often not found or difficult to access in archive division of state library so that what users miss today due to changes by website owner can be actually accessed later on using this site (Harris, Beis, & Shreffler, 2021).

The freedom to access information was made possible with internet of everywhere from anywhere it was that after Wikimedia Foundation established in 2001 it provided platform where knowledge sharing and freedom to express gained support in digital world, till that time when publishing an opinion involved long exercises with the author or publishing house made it easier with Wikipedia where information not only remained free but made accessible to all with provision to edit by users. Wikipedia's open source version of allowing anyone to edit the content saw it being victim of false information was then handled with a series of change in verifying facts where it is able to notify the imperfection by adding reference or citation to be needed. The popularity of Wikipedia can be understood by the fact that it still remains the first responder to majority of questions from all domains in Google search engine which is read by many users (Jacobs, 2019).

3.2.6 Role of Academia

Academic institutions or academics has played an important role in development and functioning of internet for creating global cyberspace. The academia was one of the first groups to use the internet before being made available for general citizens as academic values have helped in shaping governance in form of framing standards for its usage. It is academic fraternity who pushed for openness and exclusiveness of internet which was earlier confined to military usage thereby introducing collaboration with other academic institutions for development of internet (Balleste, 2015). The academic suggestions for inclusiveness resulted in formation of multi stakeholder platforms like WSIS.

The initial cyber governance idea that raised in 1990s with establishment of ICANN had handful academicians working on it and the Harvard University's the Berkman Center was part of the process that took initiative in finding suggestions on functioning of DNS systems, the center also initiated a IFWP discussion platform and a website of IFWP related materials. The Berkman Center also acted as facilitator for conducting open meeting when ICANN was incorporated in 1998 to seek suggestions on the representations of stakeholders in administration of internet (Gasser, Burkert, Palfrey, & Zittrain, 2012). The Berkman Centre today has developed an academic arena of Internet Studies which is taught in several leading universities like Oxford and others across globe that focus on interdisciplinary aspects that internet carries today to address challenges faced in cyberspace governance as internet today connects people from all walks of life that can be channelized to harness the collective potential for making a better world for all by designing models and re-organizing the existing architecture to include the latest evolution in technology and its adaptability in society.

The debate over multilateral and multi-stakeholder version of approaches for cyberspace administration and challenges over issues from surveillance to intellectual property makes situation highly politicized and academic effort can help in creating coordination by making global approach as demands are increasing across stakeholders for more power. On such note it can be seen that academia is more than a "stakeholder" as it can undertake a constitutive role for future cyberspace administration in a time when governance debates are often ideological, fragmented or filled with self interest than evidence-based. Academia can also focus on the following roles:

- *Analytical Role* – Academia network can undertake role in collecting data and analyzing robustness of applied governance mechanisms globally that will help in functioning as a backbone for further research on cyberspace governance and decision making available openly for access.
- *As mediator* – the academia community being unbiased can take up the steps to serve as a mediator to bring all stakeholders and facilitate exchange of conversations among stakeholders for achieving consensus, promoting best practices.

- *Framework* – to create new framework and design new tools or code for cyberspace governance after analyzing the differences between all stakeholders

The above role will help in contributing at large to solve the difference in opinion and approach that stakeholder's attempt, academia can also impart skill based training to impart digital literacy to increasing users of cyberspace.

3.2.7 Collaborative efforts of Public Private Partnerships

The race for digital superiority is leading towards creation of two power blocks where one led by US and other relatively new by China where both has their allies, US enjoyed monopoly for decades using their technological advancement where they gave support to private companies like Google, Facebook to remain sole service provider and through laws government was able to access information from these companies and utilize them for various requirements related to their national security and interest. United States using its technological advancement has been successful in monitoring and tracking movements like data acquired from Google and Facebook searches can give them idea of mind and requirements of the user and using the cover of ensuring public security governments have initiated mass surveillance that can be extended to foreign nations as well since it is their own private giants who have users abroad therefore getting information will not be difficult owning to the law of state mandating it to share information (Mims, 2013).

By end of 2015, US became home of 11 out of 15 top ranked companies who were doing business based on internet that included Google, Facebook, Amazon, eBay, Salesforce, Yahoo, Netflix, others followed by Chinese based Alibaba, Tencent, Baidu and JD.com (Chen, 2015), resulting in shifting power in hands of these two nations. Chinese companies followed similar to what US long before in context to surveillance and spying using its indigenous private corporations like ZTE and Huawei it managed to gather global information and also control over its domestic population by creating a controlled cyberspace with limited access to global digital world, as it had blocked western application like Twitter, Facebook, Whataspp, Viber etc and owing to its large population those indigenous applications became popular thereby creating in interest among other nations. The increasing dependency on cyberspace has now made China's

ruling Chinese Communist Party (CCP) to increase its direct involvement or control in most companies (Chorzempa, 2021), Chinese government with its biggest asset of cheap manpower utilizing it to produce equipment at cheaper cost and supplying to world and using their debt trap policy in form of providing loans and sell their products to several nations making those nations their allies (Prasso, 2019).

Earlier this year another data dump analyzed by Christopher Balding who was part of team that unearthed personal information of over 2 million people from servers of Zhenhua Data that had compiled data collected to target specific individuals according to their reach and position value they hold, interestingly the data is found to be collected from professional networking sites like Microsoft owned LinkedIn and others (Rahn, 2020). The private companies today serves as data bank for open source intelligence where using techniques like data scrapping, a process used for collecting open source data containing diversified collection that collected address, marital status photograph, political association, relatives etc by many and has no uniform laws on using it can help in analysing or creating a social circle of the target (Rana & Raj, 2020).

The series of cyber attack including data breach has created a setback in reputation of United States who was one of first to promote for public private partnerships and create alliance like American Cyber Alliance (ACA), Information Sharing and Analysis Center (ISAC)s that serves as example of Public Private Partnership models in cyber security for several countries to follow, this attack has also questioned the coordination between public and private entities (Brooks, 2019). With emerging technologies like 5G, AI, Quantum computing and IoT there is a need for collaboration to analyze risks and deploy threat architecture in place to not get impacted by attack. Developed nations having almost all its critical resources connected to cyberspace like defence, oil and gas, electric grid, healthcare, commerce, transport, education that are largely owned by private it is the need of an hour to initiate the public private partnership at the larger scale.

The private players developing technologies at rapid rate can get support from government in public-private partnership as by them being there to ensure the technologies are not getting passed to others by being tricked by belligerent nations to work against their host nations as a part of any international cooperation or agreements that are happening ongoing (Meltzer & Kerry, 2021), and the government can ensure a fair competition by ensuring that

there is no total monopoly of private companies on the artificial intelligence as tech giants are buying startups working on artificial intelligence at a rampant speed (Chakravorti, 2021). The government' active involvement can help in creating and amending laws relatively soon and also help to avoid any drawbacks when in comes to facing any belligerent nation particularly at times of cyber attacks sponsored by state and also during any standoff scenario like in case of India which has huge dependency on Chinese for its critical resource including electronics and technology (Krishnan, 2021). When Indian army was in direct military confrontation with Chinese troops and Indian soldiers managed to crush the aggressive Chinese power who were trying to illegally occupy Indian territories there was a digital deterrence as India is still poorly secured at digital borders where China has upper hand with their smart phones are very popular in India, and smart phones are found recording users movements and data which they are doing under their agreement which mentions that data will be stored in China and by that way the personal data of Indians are stored in Chinese servers (Brewster, 2020). The scenarios like this needs a greater collaboration at the domestic level to address the urgent data privacy issues and push for a strong global cyber law that can address consumers holding such products which are used for spying by powerful nations like USA, China and others.

3.2.8 Conclusion

The initiatives taken by stakeholders are often limited on basis of country, region and groups as there is no global consensus on management of cyberspace's essential requisites like infrastructure, security, legal, regulations and protection of individual's human rights in the domain that focus on granting justice to deprived users in cyberspace. Cyberspace has made people connected to each other across the world more easily than earlier making it a digital village which besides bringing threats from state and non state actors often includes complicated like a state backed non state actors making threats highly diversified in nature. These complex threats ranges from social threats involving leak or exposure of personal information to life threatening attacks on critical infrastructures or traffic signaling system causing major accidents that will have loss on civilian lives.

Similarly the financial frauds including terror funding have also found new way using digital currency widely referred as crypto currency that allows in for easy transfer of money as they lack regulation unlike regular currency and absence of uniform cyber law to govern cyberspace has seen in initiatives from major stakeholders like government, corporate firms,

Inter Governmental Organizations (IGOs) and Non Governmental Organization (NGOs) either separately or often collaborated with each other to suggest a global regime for safeguarding the cyberspace which although is virtual but relies on heavy infrastructures.

The factors that surrounds cyberspace governance debate is advancement of technology which is allowing new actors to join as stakeholders and complicate the international politics related to governing of the domain. The progress which mostly comes from private players therefore calls in their involvement for security as well and accordingly the PPPs (Public Private Partnership)s model is applied on cyberspace security but the information sharing, planning investment in emerging technology that lacks regular review on sharing of work responsibility owing to changes on varying threat dimensions.

Chapter 4

Challenges for a global cyber policy

Today's Cyberspace which has about 38.6 billion IoT (internet of Things) devices connected now stands as the place for both progressive and destructive activities as it has become playground of multiple actors (Vailshery, 2021). Government did carry out attacks in

past when there was limited number of devices connected to it and now impact can be made far more severe and devastating that can include turning off the electricity from a remote corner of world to tampering with stock market for creating financial chaos. The expansion of internet today has enabled an option to attempt of infecting and paralyzing all critical infrastructure attached to it including water and healthcare thereby pushing nations to adopt strict norms to safeguard own interest causing a tensed situation and drifting away towards creation of a global cyber policy.

This chapter focuses on challenges that come to way in formulation of a global cyber policy that includes challenges in proposed models of governance and the variation in approaches of nations towards cyberspace. The chapter studies the cyber security threats that arises due to complexities of cyberspace that makes identifying the perpetrators and also the unwanted threats that rises due to advancement of technology besides the chapter also focus on dilemma from "Cyberskeptics" who perceive cyber attacks are over hyped ignore the threats to real life from cyberspace. the chapter focuses on the real life threats from cyberspace that includes personal profiling threats to smart transportation and how private companies have become an important player in the topic of cyber governance as they not only are holding majority of resources in cyberspace but are more prone to threats as they are attacked by both criminals and state backed groups for IPR secrets which include trade secrets.

4.1 Threats to cyber security and efficacy of global cyber governance models

4.1.1 Challenges in existing and proposed model of governance

Cyberspace governance or cyber governance is an emerging topic of global governance that needs a uniform global framework as cyberspace is becoming an essential tool for daily life, and crimes in cyberspace is increasing with every passing day. Nations are finding themselves in dilemma of choosing between the state controlled multi lateral model or more liberal multi stakeholder model for their approach towards making the cyberspace secured for its citizen as nations have differences in perceiving the domain. The difference in cyber offensive and cyber defensive capabilities besides culture and their vision of leading the nation also plays an important part in supporting either of two multi-stakeholder model or multi lateral model form of governance.

The state control multi lateral model also pushes for cyber sovereignty which challenges the very nature of the connecting media i.e. internet on the following:

- Cyberspace sovereignty and nature of cyberspace – the introduction of state sovereignty in cyberspace will challenge the very basic nature of cyberspace that calls cyberspace a borderless man made domain, further introducing sovereignty in cyberspace will then lead to fragmentation of cyberspace where every nation will have its own cyberspace and no or limited relation with rest of world.
- Cyberspace sovereignty and human rights – the fundamental rights of individuals related to freedom of speech will stand challenged with implementation of state sovereignty where more nations will follow policies of authoritarian nations like China where there is a strict censorship imposed and critics of government will be considered as crime leading to revival of dictatorship.
- Cyberspace sovereignty and involvement of stakeholders- establishing a state sovereignty will deny the needed place for technical community, private sector, and academia besides the civil society. The development today is mostly because of technical contribution who develops technology with intention of uniting people and devices by removing distance that is how today we can communicate at remote distance.

The debate between two (multi stakeholder and multi lateral) forms of governance also gives rise to an important question as for handling rising complex issues in cyberspace whether there is a need to establish a new institution or to integrate into already functioning institutions. The other proposed model by WGIG that suggested four models for governing the cyberspace also pushed for creating new institution and Lawrence Solum's model of internet also suggests for a transnational institution, calling for the need of an institution to oversee the challenges in cyberspace.

The idea of creating an institution or giving power to an institution to manage the cyberspace is not welcomed by nations like China and Russia who believes cyberspace is a purely state subject and does not need any involvement of other stakeholders. Further the Lawrence Solum (Solum, 2008) using his models highlights the need to wage fight against issues like child pornography and online gambling which can be agreed by many nations but his other point of cooperation i.e. freedom of speech is again a point of contention between two power blocks (USA and China). Solum further argues as how institutions often run sub-institutions as nations who send their representative to institutions tries to influence the decisions of the

institutions.

Any governance models do not talk much on its application over hidden areas like dark web which is hub of criminals for sealing illegal items and often used by nation-states as well to exploit vulnerable networks and delay in implementing a governance model denies the much needed uniform law to ensure regulation in cyberspace. The presence cyber governance framework is based on non binding agreements, declarations, recommendation and guidelines that lack concrete mechanisms to ensure that these initiatives are being applied or followed by all. The ongoing digitalization has brought in various challenges that has highlighted the importance of proper legal system to not only handle issues from state backed non state actors but to address increasing concerns from progressive technological advancements like AI that is redefining human machine relation.

4.1.2 Threats to Cyber Security

As a part of cyber defence every advanced nation has made its own security arrangements establishing its own network for military needs which is made using air gapped network systems and countries like USA has its own secret networks JWICS (Joint Worldwide Intelligence Communication Systems) and Secret Internet Protocol Router Network or SIPRNet (Weinberger, 2010) which they often share access to allies for sharing intelligence inputs like creation of country wise dedicated network like Afghanistan Mission Network (AMN) for Afghanistan (Rosenberg, 2010). Since US and its allies enjoy secret communication system whereas Russia also has its intranet "Closed Data Transmission Segment" (Gerden, 2017), and China has controlled its internet using firewalls, these networks are nourished as a preventive measure against threat of "cyber Pearl Harbor" if conducted by a nation on other its digital assets which is increasing with growing dependencies on cyberspace (Lawson & Middleton, 2016).

Cyberspace has become a ground for terrorist organizations who has turned it a safe house for them which includes recruiting, training, gathering logistics, raising funds, spreading propaganda and also promotion of terror activities (Coninsx, 2019). In this digital age terrorists can easily conduct riots using cyberspace applications like social media can be referred as cyber aided riot, besides extortion and others can be continued through weapons like ransomware which in most cases are released control of screen only when ransom amount is transferred.

The research and development related to cyberspace has various challenges in front

which starts from management of it or the legal bindings and how to balance between liberty and security. The very much fact of an attack is that it takes hard time to identify its nature and affiliation whether it is by a criminal group or group backed by state.

The nation often has to take stern steps to ensure safety of citizens which might not be appreciated by all citizens as this domain specially where Cyber skepticism section of population criticize the expenses on cyber defence as they believe there will never be a cyber war that would kill humans. And government after spending on buying costly cyber security utilities often become victim of data breach giving fuel to further criticism alongside this there are further dilemma that becomes a hurdle while formulating a cyber security plan they can be studied as follows:

a) Identifying threat actors and retaliation mechanism:

The transition in international politics which brought in use of soft power in achieving desired goal over hard power that includes use of military capacities has also been witnessed in cyberspace where nations no longer target only military installations instead they target privately owned companies, critical assets or infrastructure that are connected to cyberspace for causing high impacts but staying low as increased digitalization to business architecture has made them vulnerable from various cyber criminal groups besides non state actors making it an easy way for attacking nation-state to stay safe by blaming attack conducted by some criminal groups not backed by nation.

The increasing threats and variations observed from recent past specially after 2017 when a series of cyber attacks by WannaCry ransomware and Petya malware attacks (Davis, 2018) where WannaCry ransomware which upon attacking a system encrypted data demanding payments in crypto currency for handling back control and Petya malware that encrypted the boot record system making it difficult for operating system to locate upon restart wiping everything and making system just a piece of box. Now at 2020 when world moved online both for office and personal work it was seen a multifold rise in cyber related crimes that even targeted child as they were also introduced to online schooling system over video calls and often falling to bullying and depression. The 2020 COVID 19 made institutions like banks also to support internet banking options than visiting branch which resulted in increase of phishing attempts on users by criminals. Threats in 2020 saw an advance version of what 2018 and 2019 trends on cyber attacks were as on 2018 cyber attacks were more on healthcare institutions in

USA and Europe than banking sector occasionally seeking ransom for releasing the control and functioning of the compromised computer systems. In 2019 cyber attacks brought in how it depended upon social engineering for preying on targets, which later showed in attempts of compromising devices using email as mode of attack rising exponentially during Covid pandemic times including healthcare data (Mitchell, 2021). Stealing personal information and selling it in dark web got in more attention and it showed rising use of digital cryptocurrencies like Bitcoins for transactions, as cyber criminal groups now demand ransom in Bitcoin for unlocking the files they have encrypted (Tidy, 2021).

In above scenario it is hard to distinguish the motive and threat actors as in digital age war can be attempted by social media where back on August 2017 saw threat to US Territory of Guam when President Trump of USA launched a series of tweets to warn North Korea about its Nuclear power projection and this time attack was comments by US President on Twitter. North Korea growing furious over tweets threatened for a missile attack on Guam showing that how social media sites can initiate wars (O' Connor, 2017). It is often seen that nation backed attack on private companies like the cyber attacks on US government confirmed in December 2020, that several agencies were victims of highly sophisticated on servers of private firm Solarwinds which also associated with government agencies of several countries Europe, Asia besides United States. The perpetrators were not pointed but it had mixed reactions from victim nation US where President elect Biden said it to be from Russia and incumbent President Trump suggested it to be of Chinese origin (Dorman, 2020). The splinter race for running surveillance seems to be making a ground here in India when China and USA both are racing to deploy surveillance techniques across world.

b) False flag operations

The hacking into network of government agencies for releasing data related to citizen surveillance or for surveillance of adversaries can lead to widespread chaos in both international relations as well as inside the nation in such cases it is necessary to find the attacker so that the expose of such does not initiate any retaliation on enemy nation over presumption of being the force behind this expose, as this type of action can be carried by any third nation also to enjoy the aftermath of it, carrying of digital surveillance is not new as USA, China , Russian all are known to run surveillance program over its citizen and even other developing nations are planning to do as a part of better management of the nation to track down any offender. These

operations are widely known as “false flag cyber operations” that has its root from World War I where British and German ships would mark ensigns of mostly each other’s to deceive their enemies.

The false flag operations are very well planned and forms effective campaigning during any cyber operations (Cunningham,2020). In a false flag attack, the state-based attackers attempt in disguise of ordinary criminals often depicting actions to be similar of politically motivated hacktivists, or to be hackers backed by an entirely different country where the main purpose remains to evade from being culprit for the action. The Wikileaks revelation in 2017 where it mentioned of Central Intelligence Agency (CIA)’s Marble Framework (Burgess, 2017) that is believed to use for masking up the paths so that upon investigations it cannot be tracked back to CIA. Further study says China forms backbone to North Korea internet (Fisher, 2015), which was then found that Russia also came forward to support North Korea with internet after there was reportedly decrease in sweetness of relationship between North Korea and China (Newton & Park, 2017), and it can be further accessed that the proxy connections offered by VPN (Virtual Private Network) might not of North Korea as being shown via geo-location software which is given at a good price to the people who are curious in knowing about the internet of North Korea. This type of business has seen growth mostly due to poor governance of cyberspace and this VPN is used by attackers in waging attack from remote location. In the above scenario any attack on nations like USA who are strong in cyber weapon can launch immediate retaliation in form of DDoS and other attack which is merely due to the confusion aroused owing to the attacker’s Internet Protocol (IP) address which showed as China or Russia as North Korea uses Russian and Chinese internet for their cyberspace.

Recently it is observed that after Israel’s surveillance company Pegasus was getting attention for its technology, China launched attack on Israel’s network posing as Iran, this would serve two purpose as initially there will tension between the old rivals and further when unearthed China’s capabilities will bypass Israel’s (Cimpanu, 2021). Therefore, false flag operations need to be kept under supervision with prompt response to neutralise it and apprehend the perpetrator in preventing a full scale confrontation, some prominent cyber attacks that are viewed as false flag operations are:

-Guardians of Peace and the Sony Pictures hack, 2014

-CyberBerkut 2014-15

-Cyber Caliphate 2015

-NotPetya 2017

-Olympic Destroyer, 2018

-Turla and Oilrig 2019

c) Advancement of Technology

Now that computers are used in industries for easier and low cost management unknowing vulnerability arises which can have severe damage impact if unchecked. The critical infrastructures which also work with industrial principles are bring connected to cyberspace through SCADA (Supervisory Controlled and Data Acquisition) systems for their efficient management, SCADA is used for distribution of water, electricity and power; even though SCADA are not directly connected with internet but are managed with connected with computer or network that has internet access and the ports where SCADA devices are connected can be easily detected by machine scanning applications or browser which are able to collect machine information when any device connects to internet. In this way the less patched ports are easily exposed which can ultimately lead to fatal consequences if unchecked (Ginter,2016), Stuxnet is a classic example for it.

The advancement of technology is essentially backed by complex hardware devices including semiconductors which are a topic of contention between superpowers already (Diwakar, 2021) and it is also seen that environment forms a factor in influencing the functioning of electronic devices in this scenario the lack of extensive research won't be able to differentiate between a cyber war or environmental consequences, therefore the issues like software corruption, hardware fail, is also needs to be studied on collaborative basis against impact from physical environment factor and electromagnetic wave to ensure unwanted threats from natural sources against governance mechanisms.

Implementation of technologies like Artificial Intelligence (AI), Big Data analytics, digital simcard and Internet of Things (IoT) which is leading to "Fourth Industrial Revolution" (Oguro, 2016) with gains being creation of new business and challenges increasing including rise

in sophistication of attacks with several examples witnessed already viz German steel mill hack 2015 (Zetter, 2015) and Ukrainian power station collapse 2015 (Krigman, 2020).

Another invention that adds to further worry is deepfake technologies can make anyone a part of any video which they neither participated nor are even aware just after having multiple shots of target person from different angles. Inclusion of machine learning and AI has made it faster and efficient with passage of days and the technology has posed political turmoil where Gabon's President Ali Bongo who fell ill at Saudi Arabia on 2018 and was absent since then which brought in criticism for not having transparency in leaders's health. After few moths the Gabonese government released a video were his eyes and head did not move as per the expectation of the viewers which resulted in a belief that this video is a deep fake and consequences were so high that this gave rise to an unsuccessful military coup in the African nation. The junior army officers who attempted coup referred video as fake and that inspired them to wage it. Forensic on video has confirmed nothing manipulated in video. The video has in fact became a case study for scholars interested or working in impact of deep fakes in the political life of states **(**Breland, 2019).

On September 2020, Chinese micro blogging site Weibo released a Hollywood style video where Chinese PLA Air Force H-6K strategic bombers are seen to conduct a simulated attack on an airbase that resembles with the satellite image of US Air Force's Andersen Air Force Base in Guam (O' Connor, 2020). This propaganda video is released in time when US and Taiwan's relations are growing closer and high level visit from US to Taiwan of State's Under Secretary Keith Krach. This attack also showed China's H6 as a high potential war craft naming it as "The God of War H-6K Goes on the Attack!" The God of war goes on attack video will promote this to sell to other nations boasting of the capability of this aircraft.

Blockchain which can be defined as collection of records linked with each other and highly secured using cyryptography reducing chances of it getting altered. Even though it is in nascent stage like that of what cyberspace was in 1970s which still shows potential of exploiting unused resources. IoT and AI which has already started contributing to growth of various industries is expected to reduce involvement to a far extent has shown their potential to help in development as well as create disruption to development. Further availability of important tools for mapping like Google maps which can now give a 360^0 view of area make attackers to prepare plan for attack very easily (Murphy Jr., 2020). AI which is being developed as positive

progression is now being widely used for cyber attacks as machine learning systems are often designed to handle crucial data so that it can be error free and not influenced by human. The Self learning AI systems are empowered to identify poor configured networks which can be used to carry Zero day exploits (Manky, 2019) by gathering and processing large databases for identifying required information and make attack swift. AI can help in guessing passwords set by human with neural network which is self are learning systems performing like human brain. AI which was initially designed to ease user experience as chatbot where user can get all their queries resolved without interacting with human now stands as threats since cyber criminals have designed chatbots which are tricking user in revealing their confidential details leading to social media account hijacked (Sharma, 2017) . Further AI which was introduced in crime detection for identifying face and car license plates are often used as surveillance devices to get in information of potential target.

It is observed that now inclusion of study of humans behavior specially expression are being given deep concentration as how would political leaders express their facial movements while delivering a sad news or happy moments are being studied with this deep fake can be made deep real someday soon and as a precaution to this applications like Truepic are being raised with higher funding a $8 M to expose deep fakes, it is an application where it captures all additional information like geospatial data –GPS sensors barometric pressure and share them to Truepic's verification server after which it uploads to its website that are available for others to download (Berkhead, 2017). Another US based startup Amber which uses "hash" base authentication system to check the integrity of video similar to that of software which generally has a MD5 value and is later checked if a copied version is found to be corrupt or not. Amber has come up to secure or prevent the tampering of cameras specially of police-worn which stands as crucial tool for legal processing with its encrypted authentication. The company suggests that a combination of deepfake with video manipulation technology and security vulnerabilities can make difficult for video to confirm its integrity hence they are coming with solution of adding an encrypted hash every 30 seconds on police body camera can prevent manipulation to a long extent (Newman, 2019).

The increase in use of technology like virtual simcards that has lead to rise in crime and misuse as there is no mechanism to have check on its usage, in this procedure the user do not need to provide their own documents instead anyone including one from foreign country can get

a sim card and ask its user to download application from the service provider to use the simcard, this modus operandi is found active in Kashmir where Pakistani backed handlers are supporting extremists in India (Singh, 2020).

The existing technology that remains unregulated and advancement happening towards achieving faster teleporting of information using quantum internet in a secured manner which was more a part of sci-fi classics much like how the whole cyberspace started, quantum internet using GPS and other technology that holds potential to amplify communication further revolutionizing the digital age keeps us engaged about the potential threats that can come along.

4.1.3 Real life threats from cyberspace

Few real life threats that have happened in small intensity have shown why Confidence Building Measures are required in cyberspace to ensure stability of infrastructure and society for all. Transportation is mostly maintained by public investments and infrastructures associated with it are capable of holding large amount of data and are prone to create havoc if its functioning is tampered. The loss in case of an attack on transportation system is not merely of business and revenue but it has potential for loss of human lives and creating political unrest in country. Few prominent examples of real life are as follows:

a) IP Profiling

Edward Snowden in his series of release has shared how Canadian spy agency Communications Security Establishment Canada (CSEC) was tracking passenger days after they have completed their travel and left airport using devices information obtained from airport's internet where passengers have connected for accessing internet (Weston, 2014). The agency which primarily focuses on obtaining foreign intelligence was found targeting travels and mapping their travel which included their staying, local transportation and onward journey. This collection of such data is against privacy at one hand and even if nation is acquiring it must be ensured security in order to prevent from being misused.

b) Aviation Industry

In an airport passengers are generally from multiple countries and not from the host nation alone , aviation industry which is highly dependent on ICT for managing its resources are susceptible to various threats and impact can be more than just financial loss which can be delay

in flight departure or arrival, leak of user personal data and more grave if an incoming airline who does not have much fuel and is not given permission to land because of cyber attack which can lead to severe loss of life.

Israel's Ben Gurion airport which is one such an airport having its own 24/7/365 Security Operation Center (SOC) in its premises has managed to defend its network against 3 million attempts made in a day to breach it (Solomon, 2019). All airports do not have state of art SOC in their premises as consequences incidents like Bristol ransomware happened where in September 2018, Bristol airport had to resort using pen-paper and whiteboards after ransomware blacked out all flight information screens as they did not pay the ransom demand of attacker, thankfully not much impact was felt in flight landing but passengers had to face great difficulties. There are also reported incidents when due to security measure Wi-Fi network was shut down in one of busiest airport in world the Hartsfield-Jackson Atlanta International airport, Atlanta, following threat from a ransomware that attacked the city (Modak, 2018).

Hong Kong's leading carrier Cathay Pacific failed to prevent and data breach of about 9.4 million passengers that included their passport number, Hong Kong national Identity card numbers and also credit card information. In same year of 2018 another such an incident Air Canada application could not prevent data breach which resulted in loss of personal details of its passengers.

There are occasions when cyber attacks were carried on airport's passport control systems making passengers wait for longer hours and getting flights delayed example being Istanbul's Ataturk and Sabiha Gokcen airports (Herberger, 2016).

Other notable nation state backed attacks include claim by Sweeden's Air Traffic Control (ATC) about alleged Russian backed cyber attack which has jammed airport's traffic controlling capabilities making hundreds of flights getting stranded on November 2015 (Leyden, 2016) .

c) Smart city transportation

Cyber attacks on smart city transportation are one of the challenges that nation has because smart city transportation are highly dependent on ICT and it is already shown how technical enthusiasts can fool online maps using single or multiple devices thus forcing applications to give response of traffic blockade where actually it was an empty road (Gault, 2020).

Often poor management can lead to cyber attacks a study conducted by research team of

Kaspersky (Leyden, 2016) on the streets of Russia found that sensors used in road and traffic controlling, cameras , traffic light all had clearly inscribed their manufacturer details. It was further detected that documentations including manual suggesting what commands to be sent to the device were available in vendor's website. Further what created more trouble was its no authentication protocol for communication with sensor as anyone with a Bluetooth-enabled device and with applications having capability of guessing password using metrics like brute force and others can easily connect to sensors. The research team was able to hack into system and gather all data and modify also giving some insights how merely using social engineering can aide in comprising modern technologies.

Rush in inclusion of almost all devices to cyberspace that are powered by electricity has given new challenges as many smart devices are used with default passwords and insufficient security prevention. It can be said that attacks on smart devices at home may be an act of privacy breach but an attack on corporate office can have a loss for national economy and if attack is on transportation systems like smart cars it is definitely an act of terrorism as there can be high rate of casualty and loss to human life.

A research conducted by researchers from Michigan State University applied criminal justice theory to smart vehicles to find out loopholes in systems for potential cyber threats (Holt, 2019). The study found once attackers penetrate into Wi-Fi to which car is connected then attacker is able to get control of not only car but other devices attached to it, the attacker can alter alert systems and driver will not be alerted for an issues related to breaking systems or tire pressure.

Another research conducted by researchers from shares that cyber attacks have potential to change traffic movement (Chen, 2018), and it is worth mentioning that couple of years back on March 2018 an Uber self-driving vehicle has crashed and killed a 49-year-old person after investigation found that its emergency braking system was dysfunctional and car was still being controlled by computer (Hawkins, 2019). The increasing digitalisation making world to gradually towards linking transportation to cyberspace and country with high population density India has announced of making all its toll plazas to be made digital that will be based upon Global Positioning System (GPS) in association with Russian based firm, this type of collaborations if not given adequate security can create in a car tracking surveillance system where any nation state actor can track movement of their target person (Bhaumik, 2018).

d) Notable incidents

In 2011-12 there was a series of attacks carried by cyber criminals who were using Chinese based Internet protocol address where they successfully managed to intrude inside JPL (Jet Propulsion Laboratory) which is often referred as precious jewel in National Aeronautics and Space Administration (NASA)'s space technology crown. As per the statement of Paul Martin then Inspector General, NASA the attackers managed to get user credential of 150 NASA employees besides getting access to create/modify or delete sensitive files which are highly critical. While leaving the network they also concealed their actions to leave minimal footprints (Moe, 2012).

That was in 2012-12 and now in 2020-21 when differences between two giants have widened assuming the hackers now managing to gain access then they can definitely have either or all of the following:

-Change its direction and drift it outside of own orbit.

-Can cause collision with other satellites

-To attack another nation's satellite making it a state of war between other nations

-The satellite can be launched at ISS (International Space Station)

4.2 Public private relationship

The development post expansion of internet is mostly undertaken by private companies and advancements like cloud computing, AI and big data are innovated and funded by private companies who in turn now holds in large chunks of our personal information leading are Amazon, Alibaba, and Microsoft who have eased people's worry of carrying large quantities of data with their cloud computing innovations available at affordable prices and also making profit by dealing with our private information whenever they need in (Fernandez, 2021). Private companies have been successful to some extent in predicting our nature at large and have tried to influence global geopolitics by persuading people's opinion in cyberspace with data of

individuals ranging from financial details to behavior courtesy the applications which we the users are increasingly getting dependent on.

The government's race for controlling internet through private companies also paves way for private entities to take the control as taking Facebook as an example which during initial times tried to balance users on one side for providing platform to connect with people and for its business clients with value for investments. Things changed when government took interest in obtaining data for surveillance and gathering data it has over the years moving towards an autocratic regime as its owner Mark Zuckerberg now holding all top positions and owns several other data gathering companies like WhatsApp and Instagram purchased at very high cost besides funding startups that are working on artificial intelligence and other technologies.

Facebook has announced that communication will still be secured by end to end encryption except the business chats as it can be understood that Facebook wants to make use of this large user base where people have switched to relying on applications for getting required services from connecting people to ordering food and others where the tech giant Facebook has invested over the year now it sees this as an opportunity to integrate all its utilities to serve it to people on its Facebook page which can be more accurate, for example when a daily wage worker is shown advertisement of holidaying in Switzerland or buying in new model of supercar that do not yield result can be now changed according to the communication they have in WhatsApp along with the transactions they do using new feature of WhatsApp pay the payment bank or to an extent getting in closer to its other allied partners who holds payments bank like Jio pay courtesy the collaboration with Reliance Jio.

Not Facebook alone other giants like Google have made own form of governance where they list in services according to the payment received for search engine optimization or SEO services to stay on top. These private companies are often creating in monopoly by buying in other competitors and while doing business they are often found to not follow a fair play policy where they try to dominate small business resulting in gaining both market and political power. While private companies have stood up claiming of their fair stand suggesting their algorithm and other calculations methods used are done by machines without human interference but it remains that these machines and equations or algorithms are done by humans with already understanding that future will be more data-driven private companies have started planning for pushing their control over it.

These giant tech companies of their role as gatekeeper is questioned by small companies and United States the country where these they have headquarters have brought in under Senate for questioning as these companies have not done enough to prevent in censorship and spreading of fake news. Private companies do have their own partnerships and accord as discussed in previous chapter to prevent misuse of cyber space but are often found to be violating as Facebook being member of PAI (Partnership on AI) has not taken wholehearted efforts to fight against preventing the platform for promotion of fake AI powered videos, in case of Nancy Pelosi, speaker of US Democratic party where her an edited video showed her to be in state of drunk while speaking was not taken down or flagged as false content by Facebook even when the video was getting shared as a real video continuously (Waterson, 2019).

The increasing dependency of government and IGOs on mostly requesting private entities for details and activities of citizens for tracking or surveillance purpose as majority of services to users is provided by privates makes private players as first responders during any upheavals leading to bringing down server like the 2010 Wikileaks case where online financial contributions were stopped to this whistle blowing site by platforms like Paypal, Mastercard and others after government orders and Amazon stopped hosting the sites after initial questioning by US authorities thereby reducing presence of Wikileaks which therefore raises a query about the power private companies holds vis-a-vis government (Greenberg, 2010).

Further debates between governments and IGOs on global cyberspace governance has made private companies gain in unsaid superiority which has potential of disrupting global economy and geopolitics as well taking an example from tech giant Facebook announced of its ambitious project Libra in 2019 (Constine, 2019) as introducing a floating currency like any other national currency but with a clear intention of not interfering or indulging in competition of any form with nation's currency system has potential to disrupt global financial architecture as it can be used for money laundering and unintentional weakening of local currency where it will be used for instance.

Learning from Facebook's rise to power and threat it poses to its own government gave Chinese government a hint to threats that its own private companies can pose if not controlled which then made them to declared war against its big tech companies with its anti-trust rules and its billionaire founders where it's top giant Alibaba and Tencent has been fined by national market regulators citing their failure to seek permissions for some acquisitions, for Alibaba with

18 Billion Yuan (around 2.8 Billion US Dollars) (Keane, 2021) and a move by Tencent is placed under scanner where it wants to take search engine Sogou under its control which caught the eye of Chinese regulator as it could have the company control over large data that Chinese users create while using the search engine. The Chinese Communist Party (CCP) unlike United States does not like to share power so that big tech companies can become too bigger than state and perhaps the crackdown began towards that and Beijing's anti-trust rules is a giant step towards curbing monopoly which was reverse until now where China supported these big tech companies to expand now wants more control and the anti-trust rule book is a clear indication to tech giants that state can mark limitation to private.

China's alone effort will not be able to put a limit on the progress worldwide that is already made where private companies like US based Space X has even entered in satellite deployment who present their aim as to provide internet to remote locations using their low earth orbiting satellites which also poses a threat as anti satellite warfare where in these satellite can be used to damage other satellites as weapons (Chang, 2021), this makes it almost inevitable for some future corporate space wars. The ongoing digital revolution related to IoT (Internet of Things) for making our daily life easier are slowly yet becoming popular as smart technology which also opening up multiple threats to nation and also to user for privacy and security alongside chances of mass surveillance by enemy nation as IoT connects everyone to cyberspace in real time and voluntarily data is shared to flex our life for betterment. Private actors having all particular details of citizen can lead to shift the power structure in the existing society as they will have more details than government's databank which are merely the identity number issued for the sake of granted citizenship or casting vote.

Other notable threat issue arised when it was found that a Silicon Valley based private company Glimmerglass has offered their services for monitoring anything and everything over internet that includes private and confidential information as well including social media accounts and their clients are believed to be government agencies as well **(**Chatterjee, 2013). These tech companies like Facebook might not be doing harm to innocent user and neither going to blackmail users with compromising pictures but if their security is breached then definitely criminals can do it, further another dimension that comes to it as how Facebook has acted to prevent misinformation when it came to itself being victim, it innovated solutions by adding status to aware people for continuing to use the platform as more users are going to other

competitor like telegram and signal. The scenario of switching to alternate applications like Signals and Telegram over WhatsApp is creating rise of another actor in the governance system besides threats that includes phishing links that can appear in form of exporting contacts and chats from WhatsApp to other applications.

4.3 Nations pushing for sovereignty

Long before the first documented computer virus was found in 1986, USA at the height of cold war in 1982 managed to tamper with the coding of the software which the Soviet spies stole from a firm in Canada, little did Soviets knew that CIA (Central Intelligence Agency) anticipating this attempt of Soviets had already tampered with the software which will make the gas pipeline blast due to increase in pressure that is beyond the acceptable limits of the joints and welds, this not only affected USSR's economy due to damage but weakened psychologically (Reed,2004). This incident showed the world how lethal potentiality the malicious codes fitted in any software or "logic bomb" (Tladi, 2021) holds, it is worth mentioning that today after three decades and with billion devices connected to the cyberspace, the impact can be made far more severe and devastating which can include in turning off the electricity from a remote corner of world to tampering with stock market for creating financial chaos. Can some examples of this be given? (Stringer & Lee, 2021) The expansion of internet today has enabled an option to attempt of infecting and paralyzing all critical infrastructure attached to it including water and healthcare, making it necessary the need to have control through established regulations like other domains to avoid other belligerent states managing in implementing their dominance which will lead in to colonization and destruction. Although there are bilateral/multilateral agreements between nations often referred as cyber pacts which is often seen as a practice of increasing strategic alliance thus making groups resulting in creation of more group with nations who feel them to be threatened with the other groups thereby transforming the virtual domain cyberspace a theatre for war and militarization. Mostly the offensive events in cyberspace revolves around state sponsored attacks on giants United States, China and Russia with few events where North Korea breaks into the fortified US based companies servers and often into US government data servers making the government clueless for assessing its loss. With militarization going in the cyberspace it is often referred as theatre of future wars and no mechanism for putting in digital sanctions unlike real world where sanctions are seen over nations for violating treaties like North Korea and Iran who have severe sanctions imposed, similar sanctions are not seen on them over

connecting to cyberspace as a punishment for indulging in offensive activities on belligerent nation's civilian network that has actually made many nations to fortified their own infrastructures and developed cyber weapons that includes logic bombs and malware codes.

Getting attacked by state backed cyber actors are often referred as "new normal" where countries like Australia and Britain has been defending their servers from the attackers every day (Seals, 2017). Cyber attackers have been on constant move with almost an incident of cyber attack happening with either high impacting Aramco attacks, Ukraine power grid attack, WannaCry, US OPM and to less impacting temporary halt of servers, or defacing of sites, there is a clear impact of geopolitical events in the cyberspace. Even after myriad of these incidents there is no fruitful path established to international cyber law or cyber policy which can address these type of attacks which is not a direct armed attack and the degree which is considered as the threshold is not clear even where impacts from attacks like 2007 cyber attack on Estonia and 2010 Stuxnet on Iran are analyzed to be below the threshold mark is clearly a question on the height of threshold limit.

China who stands as example for cyber defence has placed great firewall to censor internet and also installed surveillance cameras in all important cities, today china holds distinction of having 8 in top 10 most surveillance cities in world a survey conducted by leading internet security firm Precise Security (Baltrusaitis, 2019) where facial recognition is used by government to track not only offenders but also to track movements of their Muslim community (Uyghur) (Cockerell, 2019) as part of its domestic surveillance policy. China now has made mandatory in China to record facial biometrics for new internet and mobile phone subscriptions to keep track of new members accessing internet. China's ability to curb anti government voices online and it being successful in tracking people who are involved in supporting democracy has received interest from other countries like Saudi Arabia, UAE etc and China using its position in African countries where it has acquired good control of administration using debt trap Belt and Road Initiative (BRI) (Harsono, 2020) often uses them as overseas testing ground as well.

Today China does not stand as only country to use such technologies for expanding authoritarianism it is a new participant who has progressed very fast and joined group of nations who earlier dominated the market like United States, France, United Kingdom, United States, Russia where they shared tools ranging from facial recognition technologies to tracking devices for suppressing democracy and part of large scale surveillance and censorship done by nations.

As Chinese facial recognition technology getting popular among governments of several countries due to their highly low cost when compared with other nations, the common user base has also started inclining towards its other technologies like the IoT (Internet of Things) and with its increasing uses it can be seen the day is not far when China along the line of NSA's largest program PRISM can view the world in its screen whenever it wants and moving ahead China can take a step further by making world move using remote control.

Vietnam a neighbor of China following successful of its strict domestic's censorship has implemented similar strict domestic cyber law (Sherman, 2019) which allows Vietnamese authority to read, delete or block access to other sites under national security safety. Vietnam's internet censorship is focused on carrying in citizen surveillance and data flow which directly has hate speech against government. Vietnam also support data localization giving government more access to user data and content which it strongly believes is essential for its people's online safety. Other authoritarian nations like Iran also have deployed similar internet architectures that have high restricted mode of censorships even though there is no firewall but access to outer world is restricted mostly for using social media users' needs VPN (Virtual Private Network) software on most occasions monitored by a strong cyber army who are equipped with digital surveillance devices on citizen which can include severe punishments if found violating rules of internet usage laid by government and the cyber army is equally prepared for offensive actions over other nations if required which it believes needs to be in place to prevent any future incident like US and Israel designed Stuxnet attack (Fruhlinger, 2017). Another Muslim nation Saudi Arabia often stands as leader for other Arab nations in censoring internet by blocking websites which has contents of pornography, politics and non-Islamic information. Increase in frequency on attacks on Saudi Arabia companies has also made it strict in blocking content by ISU (Internet Service Unit) to prevent another Aramco hack incident (Pagliery, 2015).

There are several other form of censorship that targets in specific domains like in case of Cuba where it regulates mostly media and journalism against government where punishments for violators goes into different degree of harassments often leading to detention has seen many people leaving the country and using proxies to spread their messages to global audience. Whereas Eritrea has different form of censorship where internet is not only slow but only few owns privilege to access it, internet can be accessed at cyber cafes which are highly under surveillance and any access to websites that authority feels are undesired can led to severe

harassments. The country has record of long term compulsory military service and highly dictatorial government; which authority does not want the world to know making internet highly restricted related to information flow in cyberspace. At the similar line European nation Belarus applies criminal measures on people posting or supporting hate speech against government which includes long term prosecution under charge of criminal activities. In above censored situations popular apps like Facebook, Twitter, Telegram etc that gets frequently blocked on temporary basis by authorities or have been blocked completely has indirectly given opportunity to cyber criminals either independent or state sponsored to prepare a clone version and circulate it among users as unofficial or beta version which can give access to those users and through it many things can be done like promoting fake news or creating violence.

Cyber power nations like United States, Russia, Israel, China etc have high tech capabilities of penetrating into other nation's cyber network. The nation state backed cyber threat actors or groups are classified with generic term advanced persistent threat (APT), it is identified with their pattern of working and path they follow for waging attack. APT groups like other cyber criminal groups steal data and cause damage resulting in economy often disrupting the same target again and over long period time even for years, these are suspected and not confirmed, a popular research network crowdstrike (Meyers, 2019) which uses cryptonym system for adversary categorizations are as follows

Nation-State-Based Adversaries

- Bear = Russia
- Buffalo = Vietnam
- Chollima (a mythical winged horse) = North Korea
- Crane = South Korea
- Kitten = Iran
- Leopard = Pakistan
- Panda = China
- Tiger = India

Non-Nation-State Adversaries

- Jackal = Activist groups
- Spider = Criminal groups

Country	Identified pattern of working	Active APTs
China	The working pattern resembles aims laid down in the Made in China 2025 plan; the targets are focused on energy, technology and healthcare sectors. The targets often include civilian who are directly or indirectly involve in defense sectors. APT-41/40/30/27/19/18/17/16/14/12/10/4/3/1 (Dynamic Panda) all referred to china	-Anchor Panda (APT14) -Deep Panda (APT19) -Goblin Panda (APT27) -Mustang Panda -Samurai Panda (APT 4)
Iran	Target attributes which are focused on global companies which are strategically importance to countries who are opposition to Iran in particular. The group is identified as Clever Kitten and found to initiate attack with web vulnerability scanning and exploiting web browser.	APT-33/34/39 (Elfin) / (Charming Kitten).
North Korea	are identified to be focused more on espionage and currency generation, the attackers mostly involved in breaking into financial institutions which included attack on SWIFT (Society for Worldwide Interbank Financial Telecommunication) systems. They are believed to be behind the Sony pictures hack in 2014 and WannaCry.	Stardust Chollima (APT38) or with the name Lazarus Group
Pakistan	The Pakistani based adversary is identified with its unique target pattern that involves using social engineering and spear phishing to target Indian defense establishments and assets. Example being using corona virus themed phishing scam and Excel injected with macro code that is based on RAT (Remote Access Trojan) which includes naming of files which closely resembles Indian government's policy like one being Pay Matrix Projected after 7th CPC (3).xls which is similar to India's 7th Central Pay Commission's advice on salaries of government employees.	APT 36
Russia	The group sends both phishing mails and also builds domains	-Cozy Bear

	which resembles to original ones from where they collect credentials to attack their victims mostly focusing on US based organizations related to government, aerospace, NGO, defense, education sector and European military organizations. Russia is also attributed to be origin of a group also has been observed to focus on industries running on SCADA (Supervisory Control and Data Acquisition), energy and government agencies. This group Voodoo Bear is identified to be behind Ukrainian energy sector attacks in 2015 (Greenberg, 2017).	(APT29) -Fancy Bear (APT28) -Venomous Bear -Voodoo Bear

Table 12- Nation-State-Based Adversaries (Source - https://www.fireeye.com/current-threats/apt-groups.html)

The other noted groups are APT- 32 (Ocean Lotus) which is referred to Vietnam, the Equation Group refers to USA, the Machete Group of South America. Besides direct state backed groups there are few non-state criminal groups as well who holds potential to disrupt government digital functioning are as follows:

- Cobalt Spider
- Dungeon Spider
- Mummy Spider
- Salty Spider (Sality)
- Wicked Spider

4.4 Public Private Partnerships

From the above study it can be suggested that government and private should work together in handling threats in cyberspace as data in cyberspace is largely handled by private whereas the legal enforcement is with government hence a coordinated effort will help in making a secured cyberspace. There are also some challenges to this which can be understood as follows:

Challenges to public sector

- 1. Varying approaches of nation:

Different nations across world has different approaches to cyberspace which also includes varied opinions data localization, law enforcement and interests like politics, culture and language making it difficult to prosecute cyber criminals

- 2. Difference in international politics

Difference among nations has been delaying in framing a global cyber policy and norms

- 3. Relation with private sector

There are times when users execute malicious activity using applications that are of private sector which makes government impose strict regulations which ranges from providing access to data base to keeping last update of the accused to government. This creates tension impacting trust and cooperation between both entities.

Challenges to private sector

- 1. Challenges in market

Technological advancement happens almost every day and keeping update often requires higher cost which can have impact on users both in time of delay in delivery time and cost.

- 2. Increasing interdependency

As we are including AI, Machine learning to increase cyberspace potential this is urging for interdependency on other independent entities and for that it requires further intervention for governance as being company they neither have engagement with varied entities and lack the needed investment.

As we have seen in previous chapters that it is possible in cyberspace that an individual or a group holds potential to challenge a nation and the rise of new actors in cyberspace with every passing day due to multiple factors urge the government and private to come together in making the cyberspace peaceful. The advancement of technology which is essential also gives more power to the non-state actors to often disrupt proceedings as stakeholders and complicate the international politics related to governing of the domain that includes penetrating network of two belligerent nations and creating tension between them. Till date most of the progress are coming from private players making government also rely on them for multiple issues including security issues that calls for a more coordinated PPPs (Public Private Partnership) approach.

4.5. Regulating the cyberspace and the challenges

Cyberspace governance at large has many challenges with each stakeholder arguing by suggesting to be more essential over others but the main regulatory challenge that emerge when framing a policy are broadly of two category that stands as how to match with upcoming issues that arise with technical advancements or aftermath of it and secondly how to address traditional issues like that of cyber aided crimes which often become transnational and are becoming complicated with increasing user and less updated laws governing it. Few issues which makes difficult for framing a global cyber policy they are as follows:

4.5.1 Data localization

Data localization is referred to storage of data within territorial jurisdiction of a nation-state which helps in creating jobs and boosting country's economy besides contributing in data sovereignty which means data of individual citizen would be within respective government only and not with other countries. Data localization eases government's effort in accessing data of offenders which would not have been easily possible if hosted abroad as it is sometimes difficult in obtaining permission from that country, excluding possibility of surveillance data localization helps in ensuring better privacy for citizens' data.

Data localization has challenges involved as it requires advanced infrastructure which many countries do not possess and at same time poor security measure will invite attacks from cyber criminals and it will be loss to nation. The complications like data handling in case of cross border transactions where data will be required to store at different places which might bring increase in cost which will need to be borne by users and data localization defeats the primary goal of free flow of data and prevents continuation of bilateral or multilateral treaties relations related to cooperation in cyberspace and ICT which includes global job creation and data sharing.

4.5.2 Regulating online media

The journalism which works on 5W (Who, What When, Where, Why) and 1H (how) principle has been increasingly shifting its aim from acting as watchdog to waging attack on people sometimes. Social media and online platforms have given power to individual in promoting their ideas and often make it appear in form of news agency by carrying microphone and identity card in display which at one side helped in getting attention of events or incidents

that mainstream media under pressure from government did not cover and at same time these actors incited violence or promoted propaganda. It was witnessed during COVID 19 crisis many online news diverted there reports to other topics away from important topics like national security, economy, pandemic and instead reported manipulated stories.

There are no proper defined guidelines on the functioning of online media houses besides the availability of proxy servers or the use of cyberspace network can allow such media house or individual to bypass restriction by registering their channel from some other country. The case of world's largest democracy which also supports freedom of speech and has more than 450 news channels is governed by NBA (News Broadcasters Association) which is established by news channels only and the result of complaining against any news channel to them is just get a warning or issue apology. The channel may not abide by the decision as it a non-statutory body made up of competing channels urging a need to bring all such under a regulated body. More or less the same approach is followed by other nations as well who have made their own groups and become victim, prosecutor and judge to any issues that arises.

4.5.3 Foreign Investment in Technology

In a hope to become self-sufficient or Aatmanirbhar in digital era a focus is made for developing indigenous technology and applications but what when the funding and partnership is with foreign companies who are accused of not being fair in practice. The partnerships are worth millions and that do bound for data sharing later which gets used for generating wealth and taking it away from host country. The foreign companies after collaboration with local company gets more benefits which later becomes loss for whole nation and profit for just the company as in the case of WhatsApp merger with Reliance Jio which has large user base in India having has details of Aadhar number with PAN (Permanent Account Number) card and bank account now has actually given option to USA owned Facebook. To access Indian users details if US based WhatsApp wants and also to financial statements courtesy Aadhar card which further can be to remove the clearance of Indian government incase US authorities want to check on financial status of any Indian citizen.

The merger gave WhatsApp in penetrating into India's online payments business which was earlier denied where think tank Centre for Accountability and Systemic Change (CASC)

filed PIL or Public Interest Litigation before nation' top court highlighting fact that WhatsApp has not totally complied with norms of data localization and data of users should not be allowed for storing in foreign servers. But with Jio-mart an e-commerce initiative by the joint brands will definitely help in bypassing such laws as it will be always the parent company's face coming to play in documentation and disrupt banking and other business system in India and find ways to penetrate into Indian business architecture which might start with advertisement in their status and many more (Gurung, 2020) with it which will now make it is possible hopefully that USA can also run surveillance on India and use Indian users as testing objects similar to guinea pigs for any new initiatives of them as they already have several incidents of hacking in their products earlier including loopholes which allows unauthorized users to become part of any group through searching index of search engines (Wildon, 2020). Now that WhatsApp Pay has been approved by National Payments Corporation of India (NPCI) on its United Payment Interface (UPI) it now has entered the country's digital payment system where it can now have in details of all card transactions making its parent Facebook as one stop solution for government in tracking criminal or gathering information.

Not just US based WhatsApp the Chinese have done it long back in a relatively stealth manner making strong ties in Indian technology and it is found that 18 out of 30 top Indian unicorns are actually Chinese funded, these technology has control over Indian user's data that ranges from personal data to choices of food etc.

4.5.4 Defining threshold for cyber crimes.

Federal Bureau of Investigation (FBI) in coordination with other law enforcement agencies in US and abroad conducted Operation Wire in year of 2018 which till date remains as one of the largest crackdowns on cyber aided crime and a year later a similar Operation rewired (Miller, 2019) managed to create a create fear among criminals for some time. Cyber crime today is not dependant on conducting keyboard based hacks only, it has now seen various tricks were incorporated to carry the fraud which worked on Business Email Compromise (BEC) model where criminals used tricks like social engineering combined with computer intrusion making victims transfer money to accounts belonged to criminals pretending to be a trusted

partner of the organizations. In case criminals are unable to get money transferred at least they will be successful in getting crucial information contributing to existing data available on darknet for sale.

This fraud was tracked by Internet Crime Complaint Center (IC3) in 2013 and Operation Wire Wire conducted in 2018 followed by reWired in 2019 that worked to stop BEC scam which is often referred as cyber enabled financial fraud that applies act of deception and aid in committing with other frauds as well. Other scams like romance scams are increasing as people today prefer finding love online which is why Tinder and other applications are making huge money and also increasing sexual violence and chances of honey trap that involves corporate and sometime nation states as well.

The absence of a threshold limit for considering a crime as threat to nation is felt in post COVID 19 WFH (Work from Home) with fake hiring scams increasing and more cyber attacks on users to exploit their low economy situation needs to be addressed.

4.5.6 Censorship

There are many examples when nations have exerted their power to shutdown internet first noted being Egypt's internet shutdown during protests of Arab Spring in 2011 which showed that governments have capability to shutdown internet of their nation disconnecting completely from cyberspace. After 2011, internet shutdown has been done by many nations in particular region or country as whole; few continue being shut till date. According to reports published by Accessnow titled KeepItOn publishes in its latest report that even world's largest democratic nation India has resorted to highest number of internet shutdown also being for longest duration (Alawadhi, 2021) due to threats from internet being used by Pakistani backed terrorists for creating chaos and violence on security forces in region.

a) Impact due to censorship

Outcome to such initiatives of blocking and censoring in cyberspace over attempt to introduce digital sovereignty has been leading to multiple impacts in life of common users who are apolitical and lest interested in other global matters. The issues arising from blocking or

censoring of internet flows are impacted directly the users and indirectly the nation itself that can be studied as follows:

b) Introducing VPN

Today online users are more technically sound because of restrictions as they are using techniques which can help them bypass filtering mechanisms received though peers, blocking or restricting content in one nation does not wipe it from whole cyberspace, due to conflict of interest since ages the ideological differences are also witnessed in data blocking where some block political speech where some block pornography and gambling. The sources which are censored by one nation are not collectively removed from cyberspace which can easily be accessed by using tools like VPN which allows in browsing blocked contents by travelling through alternate paths making users vulnerable to cyber criminals.

The internet which was designed to be supporter of freedom of speech and help in knowing truth has also fallen into traps where software like Virtual Private Network or VPN which was created with idea that users can browse websites which are banned by their governments as part of censorship. As things have started becoming a dual use object the VPNs now are hidden truth, it is found that during peak of corona virus (COVID-19) when nations were isolating each other to break the chain of infection spreading, US President Donald Trump announced ban late Wednesday on anyone who has travelled to European Schengen area, this effort is to prevent new cases from entering US. A social media user with the name Dr AZ Treed tried accessing the same media network with different geo location using VPN and result was surprising, the headline in Europe had different with that of America (Treed, 2020) (pic below)

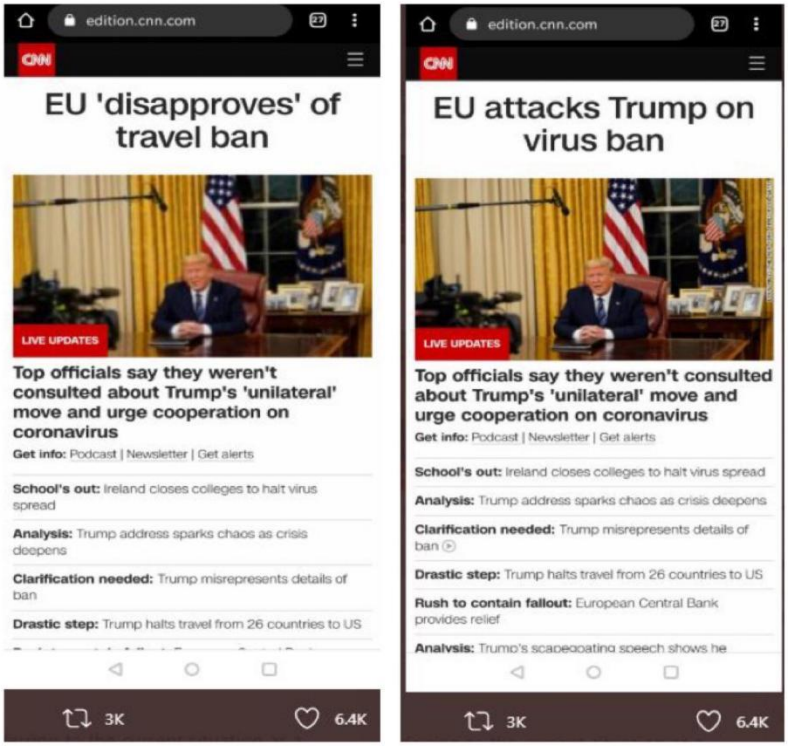


Image 1 - Change of headline for reporting same issue identified using VPN (Source - https://twitter.com/disastrid?lang=en)

The tampering of headlines as seen above happens for viewers as per geographical locations which helps not only increasing Television Rating Point (TRP) for news agencies but boosts morale of viewers/citizens of respective nations that shows the power of their ruling government which in turn support the news channel for its effective functioning and often good source of funding too.

c) Denying services to legitimate users and halting academic progress

The blocking of content denies legitimate users from knowledge too , instance when Pakistan blocked access to YouTube in 2008 (McCullagh, 2008) on cause of non Islamic content uploaded in site, blocking denied scholars from watching education videos too as YouTube contains videos of all categories. After pandemic when more institutions are moving to online mode of learning it will be found that legitimate links will be marked under false positive and blocked due to high restriction applied by government through ISPs over compressed attachments downloads from source which will have high traffic.

d) Opportunity for cyber criminals and non state actors

Over blocking or censoring internet usage makes it obvious that data might be moved to darkweb and users will involve in using illegal means to access data and involving more in darkweb will lead to further addiction to other illegal materials. Users who access to censored or blocked sites actually loss their privacy and often gives away their confidential data related to biometrics or credit card details which also weakens national security as these compromised data are sold in darkweb which has also got login credentials of users and biometrics (Riley, 2019).

e) Increasing threat to privacy and human rights

The global situation in cyberspace is not free as idealized by many under right to freedom, in cyberspace there are banned or censorship on particular type of category viewing whether its pornography, social media or particular form of journalism in either or other country which cannot be solved as its referred linked to individual culture.

4.5.7 Failure in implementing IHL

While cyberspace remains a highly contested space and nations increase their offensive capabilities as this is highly economical over traditional forms of attacking, cyber operations does not remain merely myth anymore with its lethal capabilities been witnessed already. The International Humanitarian Law or IHL which stands against any forms of warfare including cyber warfare has suggested for applying limitation of cyber operations during armed conflicts. The International Committee of Red Cross (ICRC) which is focused on ensuring no threat to innocent civilians by cyber operations conducted by nation states as more than military it is civilian population that are connected to cyberspace and any cyber attacks both during peace time and when at armed conflict must be limited to military assets only. Although IHL is not accepted or observed by all nations and neither UN has made it mandatory for all member states to follow that always leave with fear in minds of innocent civilians.

4.6 Institutions becoming proxies

ITU and ICANN are increasingly becoming proxies for the larger tussle of getting command for ruling the cyberspace. ICANN since its creation 1998 has been storing data and making it accessible to public about information of any domain that is registered under its WHOIS database. The WHOIS database is considered to have violated European Union's data

protection law which supports that data will be stored of users only if there is a necessity. Now the catch remains that not all database of WHOIS is found to be correct as there are companies who offer proxies services to hide identity of owners. Now those who cannot but proxy services are to get their privacy exploited and they are subjected under national laws and made to share data as well if deemed to be necessary.

USA stood as top contributor of UN agencies which helped it to have influence on this global body but with Trump administration reducing contribution (Shendruk, Hillard & Roy, 2020) has grabbed the eyes of China who now sees this opportunity to expand its control on the global body which can help in becoming global superpower.

China has increased its contribution to UN to many folds which has got many favors in turn as well as china now has its diplomats across key positions in UN that includes ITU (International telecommunication union) that facilitated global expansion of Huawei besides other agencies that includes aviation and food. As China contributed 12% UN regulated budget in it managed to include Belt and Road initiative as a part of sustainable development goals (Yeo, 2021)

UN which is believed to be unbiased is often accused to be an extension of jurisdictions of powerful nations and reports which are released from UN are expected to be unbiased has turned to be biased which triggered clash among nations, example can be United Nations Human Rights Council (UNHRC) report on Kashmir where a Pakistani cleric Zafa Bangash then residing at Canada openly came and claimed to have influenced the report through personal correspondent with then high commissioner of Human rights (Dehlvi, 2018). This type of reports that has involvement of outsiders from designated committee followed by shares in social media has managed to give the attacking nation Pakistan two benefits one initiating protest in Kashmir and other by ruining India and Canada relation as the cleric who did was on Canadian soil and has not arrested the cleric on his alleged involvement in modification of crucial report.

China's influence over WHO was seen during online forums conducted by World Health Organisation (WHO) where it not only denied in learning from Taiwan's success in preventing spread of pandemic but systemtic use of social media managed in confining impact of this virus through a well-planned and systematic effort that helped in proper distribution of masks by linking all government affiliated pharmacies under a centrally digitalized platform (Leonard, 2020) helping in containing the virus actually was not reconigsed by UN who followed China's

path focused on censoring Taiwan. During the annual meeting of WHO which was held online this year showed how comments were being blocked with the word Taiwan and Formusa (Taiwan was formerly called) which made netizens try for other key words like China Wuhan, pneumonia, china virus even Winnie the pooh (Xi Jinping is often referred due to facial similarity). Facebook did come up denying its role in censorship making it left with the admin of the event that is World Health Organisation that have access to a range of filters which gives them power to block specific words from appearing (Everington, 2020). Netizens found a workaround with replacing T@iwan and it worked but this type of censorship does raise questions on institutions.

4.7 Cyberspace and challenge to society

On February 8, 1996, Cyber-libertarian John Perry Barlow presented his famous "A declaration of the Independence of cyberspace" (Barlow, n.d.) where he claimed cyberspace will be a free space where government will not be able to control or hold someone expressing their views or opinion. It is observed that people are increasingly drifting towards a new kind of reality which is augmented reality a mixed of both real and virtual. There is a clear visibility that online life has become part of daily life which includes constant live update and sharing of status in social media accounts including revealing of locations, companions, sharing tracking links to friends and so on. The world now has 4.54 Billion active internet users worldwide (Johnson, 2021).

The involvement of cyberspace and democracy is not unknown anymore with Russia's involvement in USA presidential election and on similar accounts in few other countries where the information received by voters during campaigning is crucial and how states launching disinformation has managed to change outcome of result is clearly seen in USA election. The citizens are guaranteed fundamental rights by every nation and many perceive that in cyberspace also those fundamental rights should be granted, fundamental rights like freedom of expression and right to access unclassified information have received a setback in virtual word when few nations challenge freedom of cyberspace and implement their own rules and censor internet access. According to report by Freedom House report it finds that there is a continuous decline in global freedom for 13th time. (Tharoor, 2021) where in the world's largest democracy it is being seen that digital freedom is under threat where the government is increasing banning opposition groups or initiating legal actions against its leaders, the media persons are also charged with anti-

national acts often getting prosecuted or placed under house arrest. Similarly, the domain has become a place for promotion of conspiracy theories which often find its way to create polarization in society and cyberspace that had empowered people but has failed in preventing to ensure from the platform being misused for spreading misinformation which further multiplies exponentially using methods like Bots which ultimately helps in extremists committing violent acts that create differences in society.

4.7.1 The cyber psychology

Hacking does not always mean hacking into someone's device but it can also be in someone's mind for getting desired outcome as wanted. During the US presidential election campaign, it was both hacking minds alongside hacking devices, Russians created several social media accounts to campaign to influence the election, few successful drives include creating twitter accounts one being "Tennessee GOP" with handle of @TEN_GOP (Kessler, 2018) which successfully got more than 100,000 followers and was able to make desired impact by spreading propaganda which included photos, animations to keep it further shared in chain networks. Russians went attacking psychology of voters in such way that it created fake accounts for supporting Hillary too with campaign for supporting Muslims in America. The rally for Hillary Clinton never took place and people saw it a failure and supported the thought that she is not liked by majority of Americans hence no one turned up. Russian supported hackers then hacked into John Podesta's account, who was chairman of campaign for Hillary Clinton, hackers created fake mail accounts and used technique of spear-phishing which depicts mail from a trusted source and influence the recipients of mail in sharing in confidential informational meant for close persons. Hackers were able to steal more than thousands of mails and published at WikiLeaks an international non-profit organization which publishes news leaks and classified information received through anonymous sources. Although WikiLeaks founder denied receiving information from Russian government but involvement of Russian government involvement was proved when Department of Justice convicted Russian intelligence officers behind the hack of presidential election (Schmidt & Perlroth, 2020).

Attackers did used all possible techniques available to hide from law enforcement agencies they used false identities for lunching websites where they made emails public and used digital currencies like Bitcoins for all financial transactions required for the hack.

If properly analyzed it can be found that Facebook and Google can affect the real world

behavior and emotions without even triggering user's awareness who remain clueless and with increasing digitalization the future of today's kids are also played with where all efforts are being made to tap into fear of parents who feel coding or giving costly computer training is need of the hour to ensure that their kids are not left behind, where private education companies using misleading promotions (Rakheja, 2020) and other strategies to pump in money for their courses which parents are burdening on their kids for sake of achieving advanced computer knowledge at far premature age .

4.7.2 Cyberspace and social engineering

Recently hack of Twitter which compromised accounts of celebrities, businessman and former president of United States showed again why hacking is not confined to just skills of computing but needs social engineering to make it work better. Graham Ivan Clark a 17 year old was able to hijack 130 accounts of influencers and make $120,000 in crypto currency by convincing the IT employee of Twitter that he is a fellow employee who needs access credentials to company's support platform (Conger & Popper, 2020). Imagining this guy to be a group of black hat hackers who had an intention of taking down a government, the outcome would have been severe. It is always found that cyber hackers who are carrying this hacks are not merely experimenting for fun they always have a motive which can be either money or political propaganda. Hackers who do it for money often hijack websites demanding ransom and in second case the hackers try influencing elections like the Russian meddling in US Presidential elections.

The cyber espionage on US military network in 2008 which is believed as significant breach in history of American military cyber security could not find confirm the foreign spy agency but shared that more than 100 foreign intelligence agencies were targeting to penetrate US military network. This hack on US military network did give rise to counter offenses on other foreign agencies whom they believe to have carried out attack (Stewart, 2010).

The challenges like # couple challenge, # 10 year challenge are tricking us to publish our private info into public and there is essentially no check on the motive by governments on this to flag it as safe or unsafe tracking its origin (O'Neill, 2019). The morphed pictures for deep fakes pornography or revenge porn often created using pictures available in social media leads in mental health trauma for many and often it is heard by victims of such frauds that people upload

pictures to let people see and is available for sharing as well without actually any consent on it.

4.7.3 Making social map

Xiaomi, popular Chinese smart devices brand that has wide range of products from air purifier to mobiles and other utilities came to limelight when cyber security researcher Gabi Cirlig found the company recording user data related to search queries on browser even when it is done in incognito (a safe mode of browser which is believed to flush caches after closing of tabs) (Brewster, 2020). Similarly, other applications that users use like of dating, shopping, songs are collecting large scale of data of a single user which is often referred as metadata that can easily help in tracking a person. In this way even applications like music is capable of tracking user's listening habits and describe mood of users and accordingly customized advertisements and other violence propaganda can be made to appear in user's screen with an intention to manipulate user's thinking.

The gathering of data in majority of applications are found to be backed by companies with approved user consent that it takes during first time user manual which is by compulsion needs to be agreed else device would not start. In most cases data is found to be transferred to company's server for their further product development but in cases like Xiaomi a Chinese brand where it was found to be transferred to server hosted by Chinese based tech giant Alibaba, with remote severs in other countries like Russia and Singapore create fear for it being used by government as Chinese brand are bound to give access to their government whenever they ask for it making it clear that that ordinary users who run for an affordable devices always stand a chance to share their privacy in exchange for the discount they are receiving.

China has recently seen rise of few startup working on behavior analysis of users, and one such is Sensors Data which has raised good funding. Chinese browser Baidu has also mechanism for collecting log of users and another browser with name Cheetah Mobile which was getting immensely popular at a time now has been removed from Google Play Store over their activities of data collection (Vonau, 2020).

4.7.4 Removing digital gap

Even though Google launched balloon powered internet service in Kenya but it is yet to bring whole African population on cyberspace (Feleke, 2020). The Digital Economy Report

highlighted the increasing digital gap between nations like China and USA on progressive role in occupying the digital superpower race whereas nations especially from Africa and Latin America are much behind which is playing factor for digital inequality (Murthy, Kalsie & Shankar, 2021). Major technology players in cyberspace are from either USA or china like Microsoft, Apple, Amazon, Google, Facebook, Alibaba, Tencent , we chat these players often enjoy support from respective and are capable of acquiring competitors and influencing policy makers across globe in bringing more digitalization to everyday life whereas at same time forgetting to bring digital equality by supporting developing nations.

Spotify's CEO and several other European Technology leader have written wrote to European Commission (Ghosh, 2017) that internet giants abuses their privilege positions and it needs a serious attention as internet giants are using their platforms into gatekeepers. The giants are often promoting search results based on their services availed than a fair one besides they are denying consumer welfare urging it a need to bring it under proper rules.

4.8 Drawbacks in regulations for securing the cyberspace

The challenge for policy makers remain significant as existing legal frameworks is not prepared to handle the ongoing advancements in technology for instance AI has potential to influence judgment in courts as the evidence considered in judicial system comprises voice, signature, image and video where all of these can be tampered with AI that has been proved in multiple occasions (Reynolds, 2020). At time when already AI powered news anchor is tested (Kuo, 2018) displaying successful in editing facial expression and speech in an ongoing video, voice can now be produced by software with raw material using VoCo by Adobe "*Photoshop*-for-voice" and other system like creating images from text has also been on research using generative adversarial networks (GANs) (Reed et al., 2016) therefore it is clear that a cyber criminal or a state sponsored cyber hacker will soon be able to interfere into judicial system and manipulate proceedings of judgment in a real world.

The focus on creating in a smart city has got it to be latest in threat list where whole city is planned to be connected to cyberspace for efficient and smart management is new arena for threats, nations have started collaboration for creating smart cities(India, China and other nation example), here not only user will be using smart devices but main critical infrastructures will also be linked to cyberspace like water, transportation and power which is already been witnessed of being compromised. Imagining a situation where India and China developing a

smart city and a state backed APT (Advanced Persistent Threats) hacking it to vandalize it, this will lead to growing mistrust and probably a small scale war between two nations accusing each other to be main culprit behind attack. The complete city which will be designed for implementing IoT including critical infrastructure might involve use of AI too and using AI will help in supporting smart city with several updates like weather forecast, condition of infrastructures. Since IoT devices can be accessed or controlled from outside the premises using cloud and mobile device it will be a challenge to ensure complete security to such a city as whole which by in large include Industries/factories, cameras and other device, critical infrastructure, building, transportation, banks, medical devices and hospitals.

The attacks seen by state sponsored on the race of creating vaccines that first saw two Chinese national being accused by US department of Justice in July 2020 followed by attack on Dr Reddy's Lab who was contractor of Russia's Sputnik V vaccine in India and series of efforts by China, Russia, Iran and North Korea over British vaccine maker AstraZeneca (Liu, 2020). The series of threats also included attacks over ordinary citizens in form of phishing mails that are far from getting over as they might have injected with backdoor that can help in connect all of comprised devices to wage DDoS attacks or to spread misinformation and influence politics.

There are practically no regulations in place that monitor power of tech giants like Google and Facebook who are denying content owner the deserved share which is recently highlighted by Australia which pushed for media law (Meade, 2020) that challenges these tech giants approach of using the content created by local media agencies in their news sites and feeds using which they get in user's attention leading to advertisement but the media agencies are not paid appropriately paid for it, it is to be found that Google and Facebook maintains news feed without having their own news reporter. It is also seen that these tech giants also employ different policies for its users according to the nation they are based for example when WhatsApp came out with their new data sharing policy for worldwide it excluded EU in order to comply with their GDPR creating in worldwide backfire to the company.

Most challenge that has evolved during the COVID pandemic phase was the shift to cyberspace for all work and it was found that on several occasions third party applications who facilitated the online sessions between students and teachers asked to get access of

system besides having access to facial data. The situation worsened when the AI powered system could not identity a student Areeb Khan even after being with a proper internet connectivity feared his dark skin complexion is an issue which immediately gathered in global response but later was able to complete the exam after the platform intervened (Asher-Schapiro, 2020)

Till date cyberspace challenges are mostly considered as topic to be of software and hardware limited to the desktop, mobile or router at large but the submarine cables that are actually carrying the data remain vulnerable to attack from foreign country's navy or Unmanned Underwater Vehicle (UUV). There are several occasions where it is seen that disruption in submarine cable has created major blackout in internet services (fig.1). Further rising space war situation in form of satellites being used for internet connectivity where private players Starlink are leading can be at line of threat to global security as their loss of control can create clashes with other satellites. Therefore, the challenge to existing legal framework remains for it being non updated and insufficient representation of all contents that are making up the cyberspace.

Internet blackout caused due to damage of submarine cables

Year	Country	Reason	Impacted nations
2006	Taiwan	Earthquake	Hong Kong , South East Asian nations
2007	Vietnam	Theft	Vietnam and South East Asia
2008	Egypt	Ship's anchor	North Africa, Oman
2009	Taiwan	Typhoon	Singapore, Malaysia , Hong Kong , china , Taiwan
2012	United States	Hurricane	Europe and North America
2013	South East Asia	Intentionally cut by diver	South East Asia , Europe
`2017	Hong Kong	Typhoon	Singapore, Hng Kong, Australia

Table 13 – Internet blackout by damage to submarine cable (Source - https://subtelforum.com/category/cable-faults-maintenance/)

Now that pushing for regulation with an example from India as how user who select DND (Do Not Disturb) for not receiving any promotional calls from companies face difficulties while receiving any courier packages as for verification purpose courier agencies

prefer sending OTP (one time password) to ensure the authenticity of receiver and whoever has activated DND do not receive any OTP and for that the delivery person asks for picture of government ID proof this creates in further issues than solving the sole delivery purpose.

4.9 Some other challenges

The absence of effective global regulatory framework and sanction mechanism with increasing advancement can bring in complicated scenarios if not addressed for instance now an airline which is flying over 40,000 feet providing WiFi access and crime is conducted using it then under which jurisdiction will it fall as by the time the crime might get detected he will be in a different country's airspace. Similar to this can be the cruise ships sailing on high seas beyond EEZ (Exclusive Economic Zone) and crime is conducted then under which jurisdiction will the crime be considered. At time when cyber insurance is not well promoted across ground level on users and scenarios that are not falling under any regulations prompt for immediate consideration otherwise they can create huge chaotic scenario in future.

The above situation can get further complex if it is found that attacker is of nationality A and hacks nation B to store data at server hosted at nation C and owner of the server has nationality of D and on paper director if of Nationality E. this type of situation before it happens need to be created in order to ensure that criminal cannot bypass law by routing not only his online access but his physical movement.

As the threshold of cyber war is not defined, in case of a full-fledged war declared and using precision technology the attack is back tracked and is found to be hosting at a place where it has got other equipment related to civilian utilities, what will be the scenario as it is seen that even conducting surveillance requires heavy infrastructures as companies like Pegasus who are carrying large scale surveillance also relies on heavy infrastructures Pegasus (Kumar, 2021).

4.10 Conclusion

The ability of becoming part of borderless cyberspace has not only improved regular communication but has made everything easy for us, like ordering food, buying any items or sharing a special moment with someone special. Even it is now possible to keep up with what is happening at any parts of globe in a click and can be kept tracked with minute by minute update on same. In the initial days when internet was mostly a repository has now been converted to a platform for everyone to become content creators and publishers making it a tool of development

which needs to be made available to all human as a basic right and while doing so the query for ensuring security to the basic rights in cyberspace also becomes a topic of concern.

Governing the cyberspace is itself surrounded by complications where the utilities are developed and owned by private entities but larger consumer is the civil society and government mostly for the data it stores that makes the application of traditional method of governance a lesser choice. Debate in governance of cyberspace as to include all contributors to form a multi stakeholder model of governance or to create a government led multi lateral form of governance, which is actually crating path towards a balkanization situation where nations are introducing own laws and directives at their national level for regulating the usage of this borderless communication media.

As there are no barriers to enter into cyberspace besides requiring internet connectivity this domain is increasingly seen as battleground as attacking a nation in cyberspace is a relatively low cost affair for nation-states and sometimes exploited by non state actors too and in worst scenarios these non state actors are directed by nations to attack the adversaries. The increasing dependency of people on cyberspace nations are trying to push for a mechanism that can help them to secure their people and interest for which they are suggesting for their supportive mechanism at global level to ensure that their regulatory framework does not get challenged as bypassing retractions in cyberspace are not a big deal with tools that are freely available.

The differences in opinion among nations has started witnessing how tensions in real world is getting reflected in virtual world with direct impact on daily life, further the ongoing tension between USA and China resulting in espionage and cyber attacks is leading the world towards a bipolar virtual world one led by USA and its allies and other block by China and its allies. This bipolar virtual world can also lead to cyber balkanization where there will be eventually rise of other groups as well thereby increasing the digital gap as developed nations will be trying to dominate over nations who remains poorly connected. The race in strengthening geopolitical presence is also observed using cyberspace as a tool where free connectivity and high speed internet is facilitated to maintain stronghold in region which can later be exploited for other usage that includes gaining economy and further the absence of strong legal framework makes it very difficult to manage all challenges that arises out of ongoing technical advancement

and misuse of it.

Chapter 5

Conclusions and Recommendations

The word cyberspace first made its presence felt in both academic and science fiction during second half of twentieth century creating interest among people about evolution of new human machine relation. The human machine relation that started with the invention of internet today forms the backbone of information and communication technology (ICT) where almost all devices are being equipped to be part of cyberspace easily, thus enabling to digitalise the world at a rapid rate. In this digital era the information or data is viewed as the new oil and there is a race to acquire control over it, where users want to control citing it a privacy, criminals want to get hold for selling or misusing it and nations wants to have control in order to ensure national security.

As majority of the threats arising in cyberspace are transnational in nature, nations are increasingly attempting to install mechanisms that includes introducing sovereignty, developing both defensive and offensive measures to counter any cyber attacks. The like-minded nations are collaborating to form alliance and influence global policy related to establishment of a suitable governance framework that can help them to stay secured in this virtual domain, that is already declared as the fifth domain of warfare after land, air, water and space.

The race for controlling data is not just between governments, it also includes other stakeholders particularly big corporate houses like Google, Amazon, Facebook who largely was known to be a platform for business and communication now holds potential to influence election outcomes as the private companies who are directly providing services to user has more outreach to user's content and having power to decide what to be shown to users. The lack of

proper fact checking often leads to promotion of fake news that creates widespread chaos and law and order crisis making it a need to introduce a global cyberspace governance framework to ensure a safe digital globalisation with people living in harmony

Conclusion from the present study on "Global Cyber Governance: Convergence and Discord" in understanding the cyberspace and its administration is as below:

Chapter one: Introduction

The way of looking at life and world has got a makeover with advancement of ICT technologies where information or data is compared as new oil and nations are trying to colonize it for proving their supremacy in this human made domain thereby getting it already declared as fifth domain of warfare.The cyberspace which is used to refer the virtually created world formed upon linking of network of computers and other ICT devices using internet, stands to be a tool for conducting surveillance and policing system.

Cyberspace on one side continues to expand with more users from the remote locations also getting added courtesy the advancement in technology whereas at same time nations are applying censorship that prohibits them to be part of the domain thereby leaving the digital gap. Data transferred from a mobile location to another often perceived as a virtual entity today particularly with utilities like WiFi and cloud but these technologies are actually outcomes of merging in multiple technologies that depends heavily on hardware infrastructures from other critical domains like satellite (air), submarine cables (water), computers and laptops (land) therefore framing a policy on cyberspace governance must include these physical utilities also.

Chapter two: Cyberspace Governance and International Relations

The governance in cyberspace has involved mostly influence of US and other western countries in large due to multiple reasons like initial development and user base but with rapid increase of global users especially Latin America, Indian subcontinent and China as internet becoming widely available has raised multiple players in the domain including non state actors. The inclusion of other stakeholders in policy making and governance are though welcomed but they are relatively new and even the issues increase among themselves specially being the issue of developing vs underdeveloped nations in the cyberspace.

As cyberspace remains dependant on hardware therefore multiple stakeholders are involved like private companies, academia, civil society to influence the policy formulation but

the geopolitical struggle between technical advanced nations like China and US where direct combat is not witnessed owing to vast distance but cyber war is seen with both of them engaging in deploying hardware to assert their supremacy in influencing geopolitics that includes laying submarine cables across continents and increasing race for acquiring overseas base to get a landing ground for the cables enabling them for better maintenance and data analysis centre besides ensuring security.

Further once nations and their allies manage to get their dependency relived from existing cables to shift to the new cables comprising like-minded nations or allies they can employ offensive tactics by deploying Unmanned Undersea Vehicles (UUV) which have dual potential of being a peace time submarine cable observer and during wartime they may activate their sensors to break all cables.

Chapter three: Role of stakeholders in cyberspace governance: Analysis of evolving global regimes.

The global organizations fail to address the critical threats like privacy, child pornography which is a topic where world has united to stop it, owing to increasing influence of particular countries in the hierarchy. The lack of efforts in stopping militarization of cyberspace and cyber attacks has only given rise to new alliances where new agreements are made to counter belligerent nations often indirectly giving the private tech giants power to formulate laws. Private tech giants like Google, Facebook, Apple and others comes centre stage as well with their own policies that are largely designed for sake of revenue through advertisement but increasing bonding between humans and cyberspace but with access to multiple features to track messages, calls, etc can actually influence people in choosing for what people buy and eat ultimately to whom to vote and behavior towards. The race for richest position between Elon Musk and Jeff Bezos that extended to satellite is an indication that they have power to influence global power politics. The revelation of Cambridge Analytica, data dumps like Zhenhua Data leak and others that can create metadata profile of an individual which will be based on conversation and other activities gives an idea how critical cyberspace is to human life.

Cyberspace from what was actually designed as a medium of communication tool has now become a domain of contention for nations. The scenario is not a concern for technical experts alone but for a nation and world as now not only our mobile and computer but whole critical infrastructure of the country is connected to cyberspace where a single breach can lead to

fatal results impacting humans. These data breaches carried over on a single person to over a large company has great consequences as people in digital age are likely connected each other through any mutual sources making it a far serious concern. An intrusion in one network can give attackers access to multiple other network using it. Therefore, the multi stake holder model of governance is itself a case study for the International Relations model as the power in cyberspace moves in the courts of all stakeholders often with private players then with governance institutions and shifting with civil society in an undefined time intervals depending upon situation. Generally, it is a false impression where multi stakeholder model is often mistaken as all stakeholder is needed to intervene equally in all matters instead it can be defined to their requirement of intervention as matters related to governance can be handed to states as in cases of cyber offenses where criminals are located in different nations under different law can be brought to justice more smoothly as states can only initiate extradition or legal proceedings and no other stakeholders. Similarly, for technical matters related to cyberspace operations can be left largely to private players with an observer role from rest.

Chapter four: Challenges for a global cyber policy

Modern day digitalisation has made it possible for a student in remote region of Africa to access courses from top education institute situated at Europe or Asia whereas at same time digitalisation made countries go apart with a twitter war like the China-Australia spat over morphed pictures. In this digital age both government and its citizens have supported the move in moving all citizens services online for transparencies refers that more data will be now hosted in cyberspace making it prone to increased threats from criminals or APTs or Advanced Persistent Threat groups backed by nations. These types of attacks when successful can not only bring down their target but also the morale of target nation as hacking and revealing personal details of national leaders holds potential to often compel leaders in having offensive cyber capabilities.

The approach by nations in creating strong cyber law like European Union's GDPR (General Data Protection Regulation) that sets guidelines related to collection and processing of user's personal information clashes with the principle idea of free flow of data and there are many countries who do not have proper cyber law that can issue norms for this dual use technology. The lack of cyber law also has direct impact on international relations, global security and economy, where nations also often try to ensure their opinion in governance and it is now necessary to bring an international legal architecture for handling cyber affairs globally

under a uniform code in order to preserve its open and free nature.

As the tension rises over controlling the data in cyberspace, cyber war seems to have began already and with increasing civilian utilities linked to cyberspace it is obvious that cyber war in future will not be confined between military to military engagements it will impact the civilian population as well. Further the failure in bringing guidelines related to conduct on cyber warfare is expected to create complications which is also due to opinions from a section of society being cyberskeptics who still perceive cyber attacks are not capable to inflict any harm to human life ignoring the attacks on critical infrastructures. It is because of cyberskeptics the nations often ignore threats to its youth from killer games like blue whale that provokes the killing of people besides the rise in change of human behaviour can eventually result in cyborg referring to fusion of animal and machine. These above scenarios might not pose as direct threat to a nation immediately but if not stopped they can slowly be used in transforming youth towards radical terrorism causing widespread chaos and this predator games do hold potential to ruin belligerent nation's future.

Chapter five: Major Recommendations

The cyberspace which functions based on data also known as the new oil is created, stored and shared in networks or devices which are operated across border with multiple legal regulations applicable over it often makes it difficult to handle critical issues like that of cyber crimes which uses routed internet connection. From the study and based on existing governance models proposals (WSIS, WGIG and Lawrence Solum) it is suggested that the global cyberspace governance model can be made at two stages being the global and national level respectively, where at the global level UN ITU can act as coordinator and at national level the government can manage the cyberspace where the roles of principle stakeholder i.e. Inter-Governmental Organizations (IGO), Government, Private organizations, civil societies including academia can be as follows:

i) Inter Governmental Organization (IGO): UN' special branch ITU as the coordinator can implement the following:

a) ITU can create a Monitoring Group (MoG) comprising representatives from all stakeholders to observe sudden changes in websites of organisations having presence in

multiple countries by categorising them under academia, business, entertainment and others (telecom, social networking, gaming, aviation, NGOs and IGOs) helping in easy identification of origin of threats.

b) Creating Cyber Peace Keeping Force (CPKF) on line of United Nations Peace Keeping Force (UNPKF) to initiate disarming process during an ongoing cyber attack in association with private corporations as they are the primary service providers to users.

c) Creation of a Incident Response Team (IRT) within CPKF where it can coordinate with other IGOs and respective government agencies at the origin of attack for preventing transnational crimes and fast response for nabbing offenders from their physical location by taking help from local enforcement agencies.

d) IRT upon identification of the source or origin of attack as an authoritarian nation not ready to cooperate / nation with compromised digital infrastructures can be placed under Cyber Sanction Committee (CSC) to impose blockade or temporary ban on internet usage allowing only selective internet usage under educational category in support with private service providers. Continuation of lifting of digital blockade to be lifted only upon discussion at the Forum in coordination with UNSC.

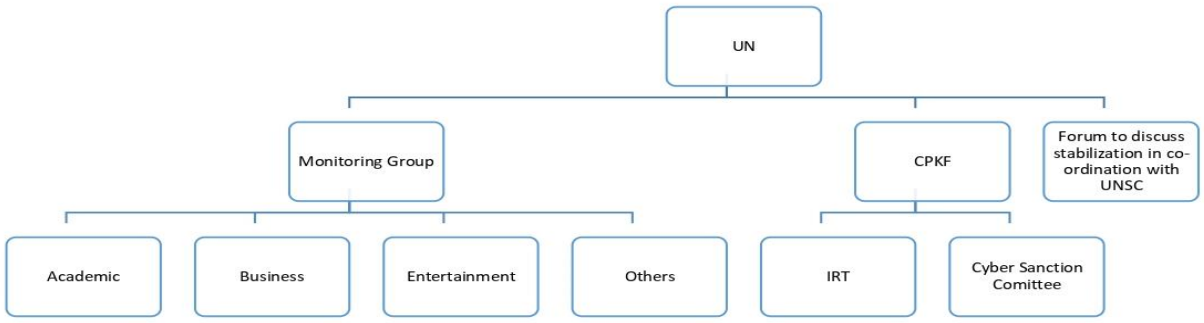


Figure 5 - The suggested cyber governance model with UN ITU as coordinator at global level, (Source-Author)

e) The Monitoring Group (MoG) can further establish a sub-group or directly look after social media platforms to ensure that every private corporation owned social media platform has a mandatory fact check account pinned on message section on top so that users can verify every forwarded link on basis of doubt and once it is found fake the

circulation must be stopped tracking it to the offender and blocking it by the platform itself, with MoG having its own fact checking team as well.

f) The MoG in association with civil societies can further observe the companies alleged attempt towards establishing monopoly like private tech giants who being platforms themselves are not denying place to other similar applications. MoG can further check on the data collected by mobile phone brands which are aligned with authoritarian regimes to inform the national government and users where they are operating to notify on the data they are collecting.

g) The UN ITU can focus in bringing consensus at UN's General Assembly over the following topics to establish a comprehensive international treaty for attaining goals like:

-Controlling activities of cyber hackers group within respective member nation

-Decide threshold limit to cyber attack on critical resources particularly over aviation and other transportation of a nation to allow initiating a total war.

-The UN office at member nation's capital city to act as local coordination centre in case of detection of attack and assistance to transnational crimes.

-Creating a global observatory body to employ real time monitoring real time attacks on critical resources and government institutions across world.

-Create mechanism to track flow of digital currency in order to prevent illegal usage.

-Establish law against hacking in any form on bionic prosthetic devices.

-Establish online court to address transnational cyber related issues.

-Once the crime is proved of having involvement from a nation then UN ITU to have right in placing sanctions with its Sanction Committee on official accounts of the nations across all platforms and same to be applied in case the country does not act in nabbing the criminal despite providing evidence.

-Establish forum to discuss stabilization in coordination with UN Security Council to lift the sanctions after assessing the scenario.

ii) Governmental supervision: To ensure all nations are equally respected with decision making process on cyberspace governance and cooperate with globally established body for ensuring safety of cyberspace. Further this model urges governments to take proactive steps in following:

a) Creation of IRT (Incident Response Team) for offensive cyber operations including drone operation and support regular defence forces for a full scale retaliation. Alongside a National

Cyber Threat Analysis Centre (NCTAC) functioning under head of state directly so that in case of requirement of cyber retaliation the response does not gets struck under bureaucratic approval and file number allocation.

b) Creation of Cyber Security Guard (CSG) under National Cyber Threat Analysis Centre (NCTAC) must have a team dedicated to provide security to critical infrastructures and technology involving smart cities specially transportation and energy, the team must maintain close liaison with the private company owning the firm.

c) Special emphasis on recruitment of Independent researchers or hackers must be given who are proactive in finding vulnerabilities by various means including bug bounty and hackathons in association with academia, private companies to avoid other nations from getting these brains drained from their nation ending up going abroad and creating codes that then manipulated and used on them. Further the CSG can work in coordination with scientific research organisations in real time checking of malfunctioning of devices due to natural phenomenon like electromagnetic waves, altitude etc.

d) A body Cyber Observer Group (COG) for monitoring small startup and new applications that receives FDI (Foreign Direct Investment), and can then all FDI shares can be purchased by government and accordingly rules in FDI and agreements can be made if the technology is critical to national security specially in relation to cyberspace.

e) Promotion of virtual court on cyber breaches for fast track hearing including pushing at global level to fight for country's right legally to understand further the legal arm can also act as coordination centre for preventing interstate cyber crimes as there can be cases where criminals being at country might use services of foreign servers and local police officials might not have necessary clearance to attack foreign servers hosted at friendly nation.

f) Create specific regulatory body on basis of applications and their functioning.

g) To make it mandatory for social media platforms to highlight the number of time a particular message is being shared in order to track the origin of news if it is provocative or fake.

h) To ban new devices, sim card and email accounts from posting in social media for 72 hours and can make only 10 friends to which there can be exceptional to diplomatic visitors where necessary

exceptions can be made.

i) Making companies cite reasons for taking down the post and will have authority to ban user for repeated violation but must cite a copy to government.

j) Setup an Office of Coordination of Cyber Crime (OC3) to act as nodal office with a portal to report in all cyber attacks or phishing on citizens to find similarity for global nexus or The functioning of the OC3 can be as follows:

- To formulate separate teams for observing activities of server and web content separately of all government websites and from private ones who are directly involved in critical infrastructures including digital identification details like digital Identity card and banking information details.
- To initiate legal proceedings at Domestic and International level upon identification of breach of security.
- Whenever any application gets popular in country with increasing user base then government needs to be create account and keep a pinned tab for fact checking where users can share a link to get it authenticated as a part of it being a torch bearer of safety and privacy even if the application has their own.
- Respective government can employ mechanism on lines of (http://www.archive.org) to keep update of regular website changes and since there will not be major changes daily it can be easily compared specially focusing on design, home page and change in communication address this will make it clear if the website is defaced as in majority of hacking attempts the home page content is altered to promote any propaganda.Every checked data must be assigned a value similar to MD5 that can avoid rechecking of same data thereby reducing chances for negative effect in speed of internet bandwidth.
- The companies can be classified under categories like NGO, Academia, Small scale business, medium scale business and large scale business, advance tech and others once this is done then the can identify DDoS easily as it normal for a site like Google to receive thousands of requests at a specific time but not a small NGO and categorization can help in analyzing it better.

- Changes observed can be reported to IT team of concerned organization for verification on a 2-way mode comprising email and over telephone, in a case of breach the mail server can get comprised sending in false reply but manual telephonic verification can help it to be concrete.
- Issuing of dedicated call centre NCH (National Cyber Helpline) to address national toll free cyber emergency number for organizations and corporate separately that can be used to report it for cyber attacks.
- Ensure cyber insurance is provided at subsidised rate to all companies working with technology that is critical to national security and ensure proper compensation is received in case of any cyber breach.

k) There should not be discrimination of any sort where in a greater portion focused on companies who have higher turnover or pays tax, the attention should be distributed according to threat level that can be as follow

- For big companies

Since majority companies already have their cyber security team they will already have team to secure internal networks here the support can be to wage offensive attack on the hosts from where attacks are coming as corporate do not have permission to launch offensive attacks.

- For small companies

As being startup they lack funding to have in a cyber security team and holding in critical information like facial recognition details for instance eyeglass companies who are using 3D facial images to give in experience can be provided security to both server where they store data and also to website where there can be attempts to inflict XSS (cross site scripting).

l) Promotion of government owned mail servers and domains particularly making it essential for linkages with banks and other essential services so that personal data can be protected from being hosted at other countries, so that financial race between Google and Facebook does not turn users into a product for their business.

m) Finally to create awareness among citizens that using internet which is reaching the devices from somewhere unless it is a peer to peer dedicated cable line laid for it therefore government can be made to provide the first layer of security as it does on border and then we can hire our own personal guards to secure our area/network same can be implemented in network security where government can secure the gateway and we can secure our own network to at least reduce the threats by large.

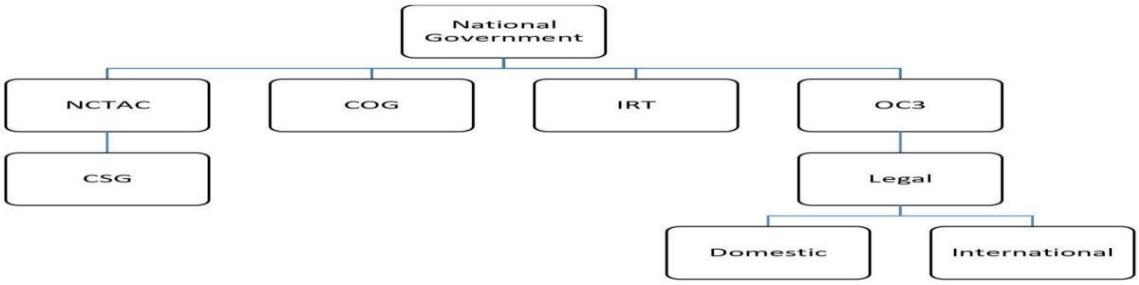


Figure 6 - Suggested model with national government as the coordinator. (Source- Author)

iii) The Private Sector: Since private sector is service provider to user and they own majority of the technical infrastructure through which we are connected to cyberspace and they provide us with the first user manual in form of agreement while using their platform needs stricter role beyond achieving their dream of being top in richest table. Suggested model expects the private sector to exhibit the following:

a) To focus on making cyberspace as market place and impose regulation in consultation with senate or parliament of the respective nation

b) Act as platform to indulge in fair play and not use their position to crush small firms by giving their own services preferential treatment over other competitor that are using their platform.

c)Formulate team to inform government about threats that can emerge with new technology in order to reform existing law or creation of new law making safe environment for all

d)Support innovation by supporting local institutions instead of shifting to their country of origin

e) Failure to play fair or taking biased action by social media platforms like how no action against Mahathir Mohammad who openly advocated the killing of French nationals and accounts of Taliban leaders but blocked account of President Trump and other leaders citing violation of policy.

iv) Civil Society: Civil societies needs to play its crucial role of representing the larger section of stakeholders that is common users in cyberspace governance matters as it is seen failure in doing so leads to both government and private entities pushing their desired regulations and measures. Civil society should undertake the following:

a) To represent opinion of common users about impact of new treaties signed by government or private players and provide opportunity to user in sharing their concerns over any digital issues

b) Raising issues over process of user generated content and moderation over online platforms.

c)Ensure to involve all people who over remain unheard and take leadership in engaging young to educate common people about good governance practices

d)Create cordial relationships with other stakeholders and individuals including other civil society groups who can contribute to issues involving in human rights, intellectual property, international trade and other issues relevant to cyberspace governance.

v) Academia:

a) Promote academic research on internet studies.

b) creating awareness of cyber hygiene at all levels including providing counselling to needy.

c) advising government and policy makers on the possible impacts from the ongoing advancements in technology that will enable to bring regulations by the same time when technology comes to market helping in formulating relevant cyber laws.

Future of Internet

Possible outcomes in near future with an absence of uniform cyber governance architecture.

- There will be multiple internet inside one country, some service providers offering verified identification while other will promise privacy, mostly funded by US who will advocate for splinternet to contain the increasing Chinese influence.

- The internet will fragment, global connectivity will happen through separate channels and protocols depending upon security threats, cyber policy of nations and cooperation between them. An unregulated cyberspace over the years can divide it into a three different segments as image below (Fig 3). where one side will be US and its allies including five eye members and on second will be China and the nations whom it will trap under its belt and road initiative finally one with India leading the digital NAM where countries like Indonesia, Vietnam, Thailand that

do not wish to join either of the power blocks. Nations like Russia and other few others possibly can go totally isolated with RuNet like architecture.

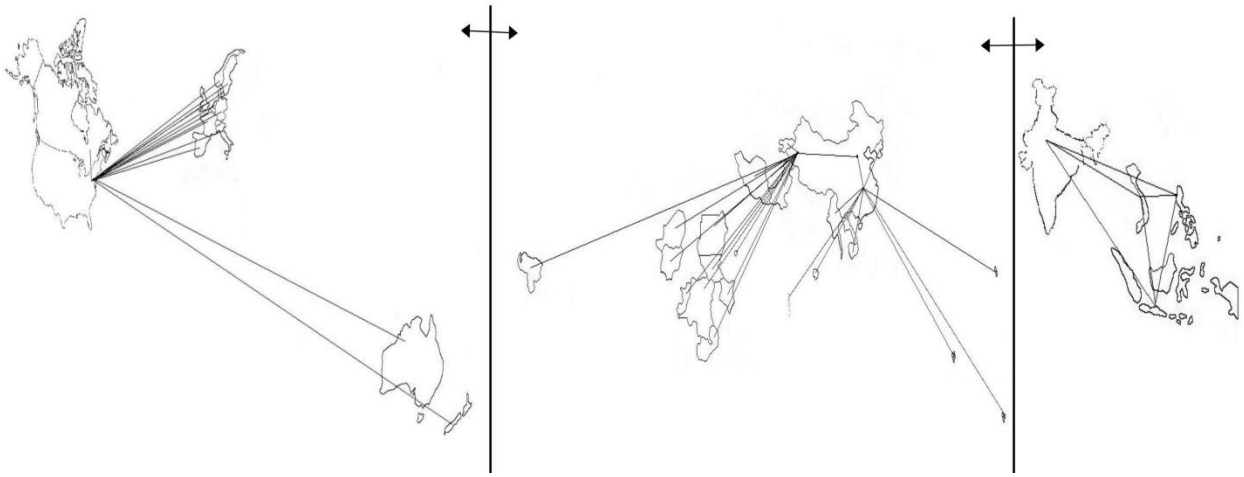


Figure 7 - The possible outcomes in near future with an absence of uniform cyber governance architecture with global cyberspace getting fragmented (Source- Author)

- In the scenario of cyberspace getting divided on basis of regional organisation (ASEAN, EU, AU, OAS, PIF, SAARC, etc) or on based of associations or alliances of mutual co-operations like (IBSA, OIC, OPEC, NATO, SCO, GCC, QUAD, Five Eyes, etc) or with other nations, the UN can act as a nodal agency for managing the flow of data across networks (Fig 4). As each groups or nations might start using their own protocol for communication like IPv4/ IPv6 etc therefore for conversion UN can be the station.

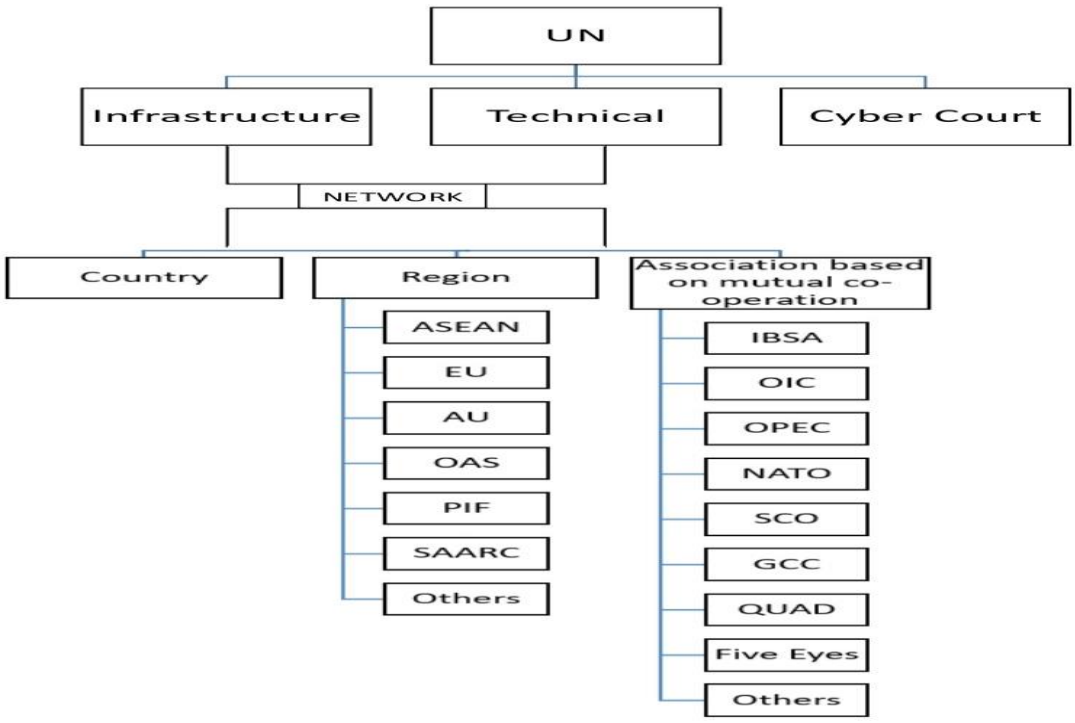


Figure 8 - The possible flow of data in fragmented cyberspace divided on basis of regional organisations with UN ITU acting as nodal agency (Source- Author)

-In the fragmented cyberspace the data flow from any user in any of any region to other will have to undergo checks at several stages which will screen for any content of potential anti-national interests and can block it any stage, screening at the checking at the border gateway of sender's own country and then either at one or two stages depending on the destination where there will be single check for allied member nations followed for screening of keywords and then to recipient whereas if it is outside the allied members then it has to pass through are recognised global agency like UN for technical conversion of the data according to the protocols in place (fig 5).

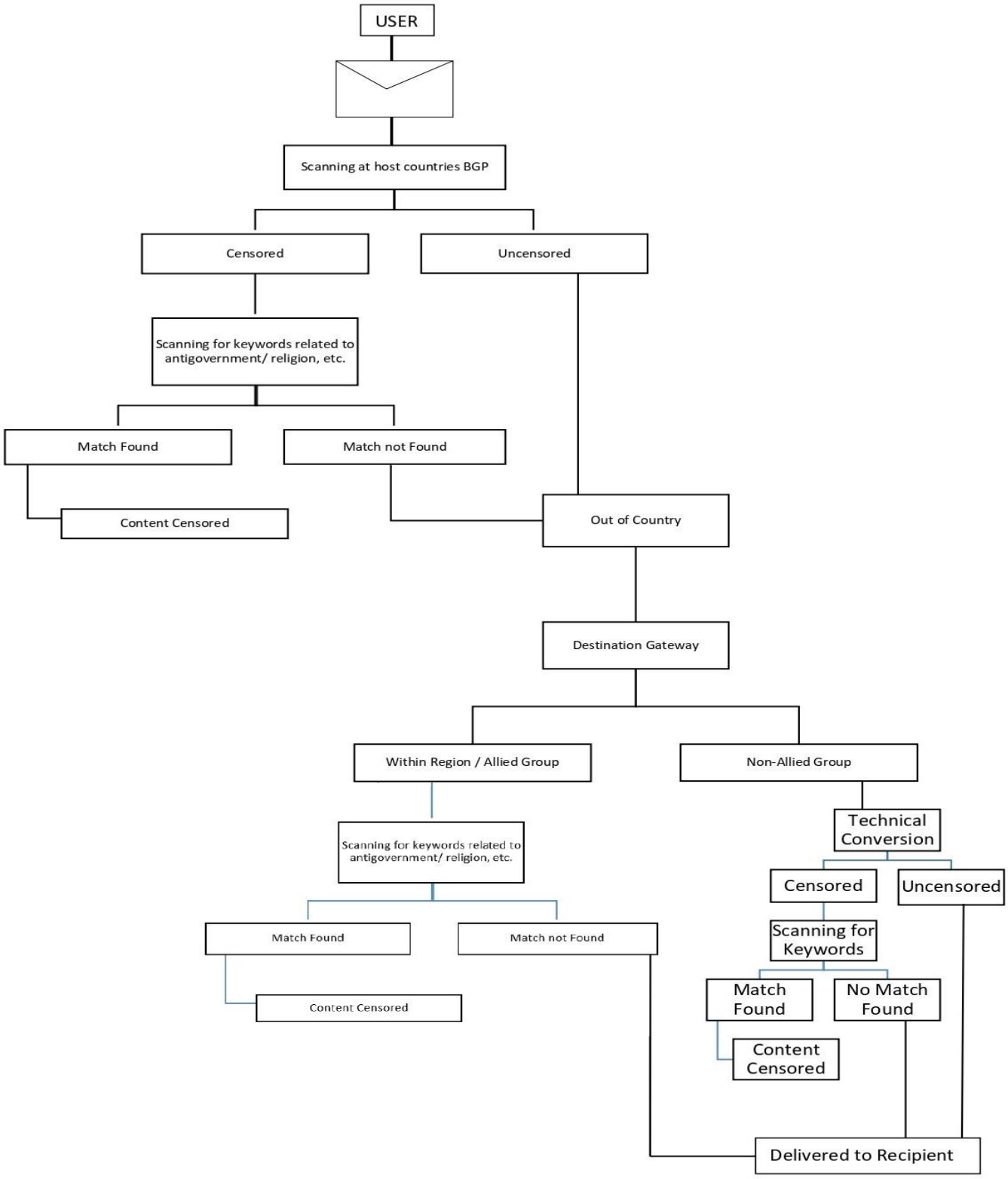

USER
Scanning at host countries BGP
Censored
Uncensored
Scanning for keywords related to antigovernment/ religion, etc.
Match Found
Match not Found
Content Censored
Out of Country
Destination Gateway
Within Region / Allied Group
Non-Allied Group
Scanning for keywords related to antigovernment/ religion, etc.
Match Found
Match not Found
Content Censored
Technical Conversion
Censored
Uncensored
Scanning for Keywords
Match Found
No Match Found
Content Censored
Delivered to Recipient

Figure 9 - The possible flow of data in fragmented cyberspace (Source- Author)

-A near future can be of localisation or nationalisation of DNS where nations can support the idea for managing their own data related to DNS or address book which will be available only for intranet like in case of RuNet and other censored internet models like China and others.

- Rise in “cyborg” with extreme changes in behavior will be found who are more inclined to the cyberspace than of the real world, rise in drone wars and human controlled by machines

Data flow during a cyber sanction / cyber war

- Apart from the global cyberspace model governance nations must proceed for an alternate and self reliance closed internet model like RuNet which will make it capable to have domestic connection, even if external powers get successful in disrupting the internet supply by breaking the submarine cables.
- The internet use to be authenticated for which government must slowly plan to introduce in user id and password based authentication based on national ID.
- To establish contact with private players in providing uninterrupted access to academic institutions in viewing education contents like in YouTube and other academic sites under multi stakeholder observation.
- Employing a strict data flow similar to (fig 5) with observation to the flow of data where a message from user will be checked for keywords particularly programming related to attempted cyber attack or provocative in any form then allowed to be passed outside country.
- Observing the behaviour of nation in waging of attack, where if authoritarian nation denies cooperation or cites compromised digital infrastructures with external actors having control of their network can be placed under prolong sanction in coordiantion with UNSC.
- Establishing a strict gateway with multiple checks (Fig 6) at all level can help in avoiding un-authorised access and identification of culprit easily.

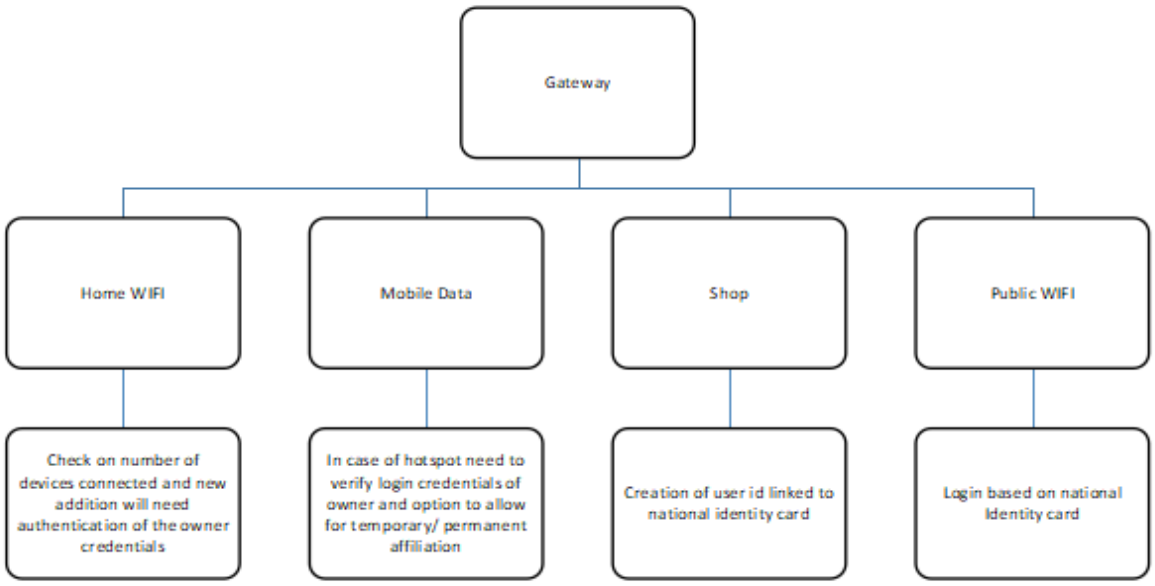


Figure 10 - Tentative data flow gateway with multiple checks during cyber blockade (Source-Author)

Arguments in support of hypothesis

5. The increasing digitalisation has made our world more wired to cyberspace where a user can not only be predicted using technology like artificial intelligence and big data analytics but can also be influenced to think in the desired way which can further impact the national security and international relations.
6. The lack of adequate governance in cyberspace has made power to be with a handful section where technical advanced nations like US, China, Russia alone are trying to decide the flow of data. After government the private players owing to their direct hold on data are often challenging the government thereby framing their own policies which might be of against national interest to many nations thus urging in framing of a governance system which would prevent from colonizing cyberspace and securing civilian assets.
7. Ongoing technological advancement like creation of deep fake videos possess can even challenge the judiciary evidences proves that existing cyber regulations are inappropriate to deal with emerging frontiers of cyber governance.

8. Social media debates that often based on morphed pictures and videos often triggers war between nations on social media that can have direct bearing on ground therefore cyber diplomacy can be a tool applied in cyber governance to deal with complex international relations in the virtual world to address the fake information

Future scope of study

As the future becomes technology driven with all daily life activities getting linked to cyberspace, there is a need to ensure standardisation of cyberspace governance and with the complexities increasing the focus can be laid on following:

- Challenges for introducing splinternet/nation based sovereignty in flow of data. .
- Making UN as an apex organisation to regulate cyberspace.
- How deep un-authorised network penetration by nation backed actors will be considered as an act of war.
- Conducting study on potential errors caused because by involvement of external sources like radioactivity / altitude on the hardware devices enabling to gauge the impact of natural factors in functioning of cyberspace and its implication over international relations.

Bibliography

Agarwal , D., & Agarwal , R. (2016). Needless pressure to change copyright laws. Retrieved 8 July 2020, from https://www.thehindubusinessline.com/opinion/needless-pressure-to-change-copyright-laws/article8557036.ece

Aggarwal, V. (1998). *Institutional Designs for A Complex World: Bargaining, Linkages, and Nesting* (pp. 1-44). Ithaca: Cornell University Press.

Ahmed, Y. (2021). Why WhatsApp users in Europe can opt-out of New WhatsApp privacy policy but users in India cannot?. Retrieved 12 May 2021, from https://www.indiatoday.in/technology/news/story/why-whatsapp-users-in-europe-can-opt-out-of-new-whatsapp-privacy-policy-but-users-in-india-cannot-1793555-2021-04-21

Alawadhi, N. (2021). India had highest number of Internet shutdowns at 109 in 2020: report. Retrieved 25 March 2021, from https://www.business-standard.com/article/current-affairs/india-had-highest-number-of-internet-shutdowns-at-109-in-2020-report-121030301203_1.html

Alstyne, M., & Brynjolfsson, E. (1997). Electronic Communities: Global Village or Cyberbalkans?. Retrieved 9 April 2019, from http://web.mit.edu/marshall/www/papers/CyberBalkans.pdf

Arimatsu, L. (2019). Silencing women in the digital age. Cambridge International Law Journal, 8(2), 187-217. doi: 10.4337/cilj.2019.02.02

Arkko, J. (2016). 30 Years of Engineering the Internet. Retrieved 2 January 2020, from https://www.ietf.org/blog/30-years-engineering-internet

Arthur, C. (2013). Tech giants may be huge, but nothing matches big data. Retrieved 21 May 2019, from https://www.theguardian.com/technology/2013/aug/23/tech-giants-data

Asher-Schapiro, A. (2020). 'Unfair surveillance'? Online exam software sparks global student revolt. Retrieved 10 December 2020, from https://www.reuters.com/article/us-global-tech-education-feature-trfn-idUSKBN27Q1Q1

Atwan, A. (2015). *Islamic State The Digital Caliphate* (pp. 15-32). California: University of California Press.

Bain, B. (2009). Obama unveils new cybersecurity strategy -- FCW. Retrieved 19 April 2020, from https://fcw.com/articles/2009/05/29/web-obama-cyber-czar-strategy-speech.aspx

Balakumar, K. (2020). Twitter flags tweets with manipulated media in India - This is how it works. Retrieved 7 January 2021, from https://www.techradar.com/in/news/twitter-flags-tweets-with-manipulated-media-in-india-this-is-how-it-works

Ball, K. (2017). African Union Convention on Cyber Security and Personal Data Protection. International Legal Materials, 56(1), 164-192. doi:10.1017/ilm.2016.3

Balleste, R. (2015). *Internet Governance: Origins, Current Issues, and Future Possibilities* (pp. 1-25). London: Rowman & Littlefield Publishers.

Baltrusaitis, J. (2019). Top 10 Countries and Cities by Number of CCTV Cameras. Retrieved 2 August 2020, from https://www.precisesecurity.com/articles/Top-10-Countries-by-Number-of-CCTV-Cameras

Bannerman, N. (2020). ICPC rallies government to prioritise subsea connectivity. Retrieved 16 January 2021, from https://www.capacitymedia.com/articles/3825252/icpc-rallies-government-to-prioritise-subsea-connectivity-amid-covid-19-outbreak

Barker, S. (2018). Singapore & UK Governments commit to building cybersecurity capacity for Commonwealth. Retrieved 9 March 2020, from https://securitybrief.asia/story/singapore-uk-governments-commit-building-cybersecurity-capacity-commonwealth

Barkham, P. (2017). Russian tanker sails through Arctic without icebreaker for first time. Retrieved 3 January 2020, from https://www.theguardian.com/environment/2017/aug/24/russian-tanker-sails-arctic-without-icebreaker-first-time

Barlow, J. (n.d.)A Declaration of the Independence of Cyberspace. Retrieved 12 November 2020, from https://www.eff.org/cyberspace-independence

Barrett, J. (2021). EXCLUSIVE Pacific ISLAND turns to Australia for undersea cable after spurning china. Retrieved June 26, 2021, from https://www.reuters.com/world/asia-pacific/exclusive-pacific-island-turns-australia-undersea-cable-after-spurning-china-2021-06-24/

Basu, I. (2021). India joins global undersea cable race with Reliance Jio's help. Retrieved 17 June 2021, from https://www.asiafinancial.com/india-joins-global-undersea-cable-race-with-reliance-jios-help

Beens, R. (2020). Council Post: The State Of Mass Surveillance. Retrieved 2 January 2021, from https://www.forbes.com/sites/forbestechcouncil/2020/09/25/the-state-of-mass-surveillance/

Beijnum, I. V. (2010). 90% of IPv4 address SPACE Used; ipv6 move looking messy. Retrieved March 03, 2020, from https://arstechnica.com/tech-policy/2010/01/90-of-ipv4-address-space-used-ipv6-move-looking-messy/

Below, K (2014).The Utility of Timeless Thoughts: Hannah Arendt's Conceptions of Power and Violence in the Age of Cyberization. In B. Müller, J.F. Kremer (Eds.), *Cyberspace and*

International Relations: Theory, Prospects and Challenges (pp.95-114). Springer Berlin Heidelberg

Bennett, B. (2021). Here's why Facebook and Google are building submarine cables | Scoop News. Retrieved 18 April 2021, from https://www.scoop.co.nz/stories/HL2104/S00046/heres-why-facebook-and-google-are-building-submarine-cables.htm

Berkhead, S. (2017). Truepic app lets journalists instantly verify images, videos. Retrieved 12 April 2020, from https://ijnet.org/en/story/truepic-app-lets-journalists-instantly-verify-images-videos

Berners-Lee: World Finally Realizes Web Belongs to No One | Internet Hall of Fame. (2012). Retrieved 20 May 2019, from https://www.internethalloffame.org//blog/2012/06/06/berners-lee-world-finally-realizes-web-belongs-no-one

Bhargava, Y. (2020). Govt blocks 43 more mobile apps, including AliExpress, Alipay Cashier and CamCard. Retrieved 8 January 2021, from https://www.thehindu.com/news/national/govt-blocks-43-more-mobile-apps-including-aliexpress-alipay-cashier-and-camcard/article33170211.ece

Bhaumik, A. (2018). Russia offers India electronic system to collect toll. Retrieved 15 April 2020, from https://www.deccanherald.com/national/russia-offers-india-electronic-696113.html

Biggio, G. (2019). Cyber Operations and the Humanization of International Humanitarian Law: Problems and Prospects. Retrieved 4 October 2020, from https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1161&context=cjlt

Blitz, M. (2017). Navy Divers and Their Daredevil Mission to Spy on the Soviet Union at the Bottom of the Sea. Retrieved 21 November 2019, from https://www.popularmechanics.com/technology/security/a25857/operation-ivy-bells-underwater-wiretapping

Borsook, P. (1995). How Anarchy Works. Retrieved 18 April 2020, from https://www.wired.com/1995/10/ietf

Bratton, B. (2016). *The stack* (pp. 42-80). Cambridge, Massachusetts: The MIT Press.

Brauchli, M. (2013). 'Cool War: The Future of Global Competitionn' by Noah Feldman. Retrieved 21 January 2021, from https://www.washingtonpost.com/opinions/cool-war-the-future-of-global-competitionn-by-noah-feldman/2013/06/14/7cae1b44-c873-11e2-8da7-d274bc611a47_story.html

Breland, A. (2019). The bizarre and terrifying case of the "deepfake" video that helped bring an African nation to the brink. Retrieved 15 February 2020, from https://www.motherjones.com/politics/2019/03/deepfake-gabon-ali-bongo/

Brenner, M. (2020). The Benefits of 5G for Business. Retrieved 30 November 2020, from https://www.nutanix.com/theforecastbynutanix/technology/the-benefits-of-5g-for-business

Brewster, T. (2020). Exclusive: Warning Over Chinese Mobile Giant Xiaomi Recording Millions Of People's 'Private' Web And Phone Use. Retrieved 3 November 2020, from https://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/#6abf85311b2a

Bridgwater, A. (2016). Can Artificial Intelligence Answer Our Email?. Retrieved 29 September 2020, from https://www.forbes.com/sites/adrianbridgwater/2016/02/18/can-artificial-intelligence-answer-our-email/?sh=30ec7c97cb42

Brooks, S. (2020). 5 most dangerous social media challenges to warn your kids about. Retrieved 18 January 2021, from https://www.wfla.com/wfla-plus/5-most-dangerous-social-media-challenges-to-warn-your-kids-about

Browning, R. (2020). From GDPR to LGPD: Lei Geral de Proteção de Dados Compliance. Retrieved 17 December 2020, from https://www.thirdandgrove.com/insights/lgpd-lei-geral-de-protecao-de-dados/

Buchanan, B. (2020). *The Hacker and the State* (pp. 129-148). Cambridge, Massachusetts: Harvard University Press.

Buntz, B. (2019). Charter of Trust: Siemens, NXP, Partners' Growing Alliance. Retrieved 21 July 2020, from https://www.iotworldtoday.com/2019/07/24/charter-of-trust-siemens-nxp-partners-growing-alliance/

Burgess, M. (2017). WikiLeaks drops 'Grasshopper' documents, part four of its CIA Vault 7 files. Retrieved 10 April 2020, from https://www.wired.co.uk/article/cia-files-wikileaks-vault-7

Burns, P. (2005). International Harmonized Research Activities - Intelligent Transport Systems (IHRA-ITS) Working Group Report. Retrieved 18 May 2020, from https://trid.trb.org/view/809631

Cao, S. (2020). Will Starlink Satellites Become Space Junk One Day? SpaceX Has an (Imperfect) Plan. Retrieved 8 December 2020, from https://observer.com/2020/10/spacex-starlink-satellite-collision-risk-space-debris/

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs, 92(1)*, 43-62. doi: 10.1111/1468-2346.12504

Cave, D., Ryan, F., & Xiuzhong Xu, V. (2019). Mapping more of China's tech giants: AI and surveillance. Retrieved 5 April 2020, from https://www.aspi.org.au/report/mapping-more-chinas-tech-giants

Cavelty, M. (2008). *Cyber-Security and Threat Politics US Efforts to Secure the Information Age* (pp. 24-38). Abingdon: Taylor & Francis.

Cerf, V., & Kahn, R. (1974). A Protocol for Packet Network Intercommunication. *IEEE Transactions On Communications*, *22*(5), 637-648. doi: 10.1109/tcom.1974.1092259

Chakravorti, B. (2021). Big Tech's Stranglehold on Artificial Intelligence Must Be Regulated. Retrieved 12 August 2021, from https://foreignpolicy.com/2021/08/11/artificial-intelligence-big-tech-regulation-monopoly-antitrust-google-apple-amazon-facebook/

Chatterjee, P. (2013). Glimmerglass Intercepts Undersea Cable Traffic for Spy Agencies | corpwatch. Retrieved 10 October 2020, from https://www.corpwatch.org/article/glimmerglass-intercepts-undersea-cable-traffic-spy-agencies

Chen, Q. (2018). Hackers could engineer traffic jams, by using their cars to lie to smart traffic lights - City Monitor. Retrieved 24 July 2021, from https://citymonitor.ai/transport/hackers-could-engineer-traffic-jams-using-their-cars-lie-smart-traffic-lights-3964

Cheng, E. (2020). China's yuan could become the world's third largest reserve currency in 10 years, Morgan Stanley predicts. Retrieved 13 January 2021, from https://www.cnbc.com/2020/09/04/chinas-yuan-rmb-to-become-third-largest-reserve-currency-by-2030-morgan-stanley.html

Cheong, D. (2017). Digital warfare - the new global arms race. Retrieved 12 February 2020, from https://www.straitstimes.com/singapore/digital-warfare-the-new-global-arms-race

Chimtom, N. (2016). Cameroon's dilemma in fighting cybercrime. Retrieved 18 January 2020, from https://www.africanindy.com/business/cameroons-dilemma-in-fighting-cybercrime-5073265

Chorzempa, M. (2021). China's campaign to regulate Big Tech is more than just retaliation. Retrieved 11 August 2021, from https://asia.nikkei.com/Opinion/China-s-campaign-to-regulate-Big-Tech-is-more-than-just-retaliation

Cimpanu, C. (2021). Chinese cyber spies targeted Israel posing as Iranian hackers. Retrieved 12

August 2021, from https://therecord.media/chinese-cyber-spies-targeted-israel-posing-as-iranian-hackers/

Clark, A. (2003). *Natural-Born Cyborgs Minds, Technologies, and the Future of Human Intelligence* (p. 58). New York: Oxford University Press.

Clark, E. (2021). Is Elon Musk Revolutionizing Rural Internet with Starlink?. Retrieved 21 April 2021, from https://blog.twinstate.com/rural-internet-revolution-with-starlink-satellite-internet

Clarke, A. (1945). Extra Terrestrial Relays- Can Rocket Stations Give World Wide Radio Coverage. Retrieved 12 January 2020, from http://clarkeinstitute.org/wp-content/uploads/2010/04/ClarkeWirelessWorldArticle.pdf

Clarke, L. (2021). Technical standards-setting is the next China-US showdown - Tech Monitor. Retrieved 25 June 2021, from https://techmonitor.ai/technology/technical-standards-setting-shaping-up-next-china-us-showdown

Coalson, R. (2019). Explainer: Russia Takes A Big Step Toward The 'Internyet'. Retrieved 5 September 2020, from https://www.rferl.org/a/explainer-russia-sovereign-internet-law-censorship-runet/30248442.html

Cockerell, I. (2019). Inside China's Massive Surveillance Operation. Retrieved 10 February 2020, from https://www.wired.com/story/inside-chinas-massive-surveillance-operation

Coe, T. (2015). Where does the word cyber come from? | OUPblog. Retrieved 13 May 2021, from https://blog.oup.com/2015/03/cyber-word-origins

Collins, B., & Zadrozny, B. (2020). Pro-Trump operatives coordinated viral #StopTheSteal events. Facebook shut them down. Retrieved 7 January 2021, from https://www.nbcnews.com/tech/tech-news/pro-trump-operatives-coordinated-viral-stopthesteal-events-facebook-shut-them-n1246655

Conger, K., & Popper, N. (2020). Florida Teenager Is Charged as ‘Mastermind’ of Twitter Hack. Retrieved 10 October 2020, from https://www.nytimes.com/2020/07/31/technology/twitter-hack-arrest.html

Coninsx, M. (2019). Responding to terrorist use of the internet | Global Initiative. Retrieved 5 January 2021, from https://globalinitiative.net/analysis/terrorist_use_internet/

Constine, J. (2019). Featured Article Facebook announces Libra cryptocurrency: All you need to know. Retrieved 14 June 2020, from https://techcrunch.com/2019/06/18/facebook-libra/

Corera, G. (2020). ISIS 'still evading detection on Facebook', report says. Retrieved 14 January

2021, from https://www.bbc.com/news/technology-53389657

Corr, A. (2019). The big business of self-censorship over China - UCA News. Retrieved 14 April 2020, from https://www.ucanews.com/news/the-big-business-of-self-censorship-over-china/85391

Craig, A., & Valeriano, B. (2018). Realism and Cyber Conflict: Security in the Digital Age. Retrieved 22 May 2020, from https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/

Cross, T. (2018). Council Post: New Changes To Wassenaar Arrangement Export Controls Will Benefit Cybersecurity. Retrieved 14 November 2020, from https://www.forbes.com/sites/forbestechcouncil/2018/01/16/new-changes-to-wassenaar-arrangement-export-controls-will-benefit-cybersecurity/?sh=52d30fa5ed60

Crossette, B. (2001). Diplomatically, French Is a Faded Rose in an English Garden (Published 2001). Retrieved 9 March 2020, from https://www.nytimes.com/2001/03/25/world/diplomatically-french-is-a-faded-rose-in-an-english-garden.html

Cumming, E. (2014). William Gibson and Neuromancer: the man who saw tomorrow. Retrieved 21 May 2021, from https://www.theguardian.com/books/2014/jul/28/william-gibson-neuromancer-cyberpunk-books

Cunningham, D. (2020). *Cyber Warfare - Truth, Tactics, and Strategies* (pp. 144-153). Birmingham: Packt Publishing.

Dalakov, G. The First Computer Virus of Bob Thomas (Complete History). Retrieved 26 February 2020, from https://history-computer.com/Internet/Maturing/Thomas.html

Daleno, G.(2015). CNMI declares emergency. Retrieved November 11, 2020, from https://www.guampdn.com/news/local/cnmi-declares-emergency/article_5fb71baf-3e17-53ea-9777-a3abe6350c77.html

Dashab, M. (2018). A reflection on Lanzarote Convention of the Council of Europe for the Protection of Children against Sexual Exploitation and Sexual Abuse. Public Law Researsh, 20(60), 125-155. doi: 10.22054/qjpl.2018.28005.1702

Datta, S. (2014). Snowden documents: UK spy agency hacked Reliance cables, accessed data. Retrieved 22 February 2019, from https://www.hindustantimes.com/india/snowden-documents-uk-spy-agency-hacked-reliance-cables-accessed-data/story-S6uGCkRzaTqanhwFoLL1bK.html

Davis, J. (2018). WannaCry, Petya 1 year later: The good, the bad and the ugly. Retrieved 20 November 2020, from https://www.healthcareitnews.com/news/wannacry-petya-1-year-later-good-bad-and-ugly

Dayman, D. (2018). What is GDPR and Why is it Important?. Retrieved 15 September 2020, from https://www.validity.com/blog/what-is-gdpr-and-why-is-it-important

de Alcântara, B. (2018). SCO and Cybersecurity: Eastern Security Vision for Cyberspace. International Relations And Diplomacy, 6(10). doi: 10.17265/2328-2134/2018.10.003

de Bossey, C. (2005). Report of the Working Group on Internet Governance. Retrieved 18 August 2019, from https://www.wgig.org/docs/WGIGREPORT.pdf

De Groot, J. (2020). What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019. Retrieved 1 December 2020, from https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection

Dehlvi, G. (2018). UN human rights chief's Kashmir report a result of his close links with Pakistan - The Sunday Guardian Live. Retrieved 14 June 2020, from https://www.sundayguardianlive.com/news/un-human-rights-chiefs-kashmir-report-result-close-links-pakistan

Delerue, F., Desforges, A., & Géry, A. (2019). A Close Look at France's New Military Cyber Strategy. Retrieved 13 May 2020, from https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/

Dilipraj, E. (2018). CYBERSPACE REGULATION: THE NEED OF THE HOUR. Retrieved 20 January 2020, from https://www.academia.edu/36547730/CYBERSPACE_REGULATION_THE_NEED_OF_THE_HOUR

Dorman, J. (2020). Trump contradicts Pompeo as he breaks his silence on SolarWinds cyberattack and shifts focus to China instead of Russia. Retrieved 25 December 2020, from https://www.businessinsider.in/politics/world/news/trump-contradicts-pompeo-as-he-breaks-his-silence-on-solarwinds-cyberattack-and-shifts-focus-to-china-instead-of-russia/articleshow/79818601.cms

Duggal, H. (2021). Mapping internet shutdowns around the world. Retrieved 28 March 2021, from https://www.aljazeera.com/news/2021/3/3/mapping-internet-shutdowns-around-the-world

Easterbrook, F. (1996). Cyberspace and the Law of the Horse. *University Of Chicago Legal Forum*, 207-214. Retrieved from https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2147&context=journal_articles

Elias Dec, J. (2017). China has unveiled a digital ID system linked to WeChat. Retrieved 23 November 2020, from https://in.pcmag.com/china/118268/china-has-unveiled-a-digital-id-system-linked-to-wechat

Ellinghaus, W., & Forrester, L. (1985). A U.S. Effort to Provide a Global Balance: The Maitland Commission Report. Journal Of Communication, 35(2), 14-19. doi: 10.1111/j.1460-2466.1985.tb02227.x

Emmons, T. (2021). Retrospective 2020: DDoS Risk Higher Than Ever. Retrieved 29 January 2021, from https://www.akamai.com/blog/security/part-i-retrospective-2020-ddos-was-back-bigger-and-badder-than-ever-before

English, J. What is Fiber Optics (Optical Fibre) and How does it Work?. Retrieved 2 March 2020, from https://searchnetworking.techtarget.com/definition/fiber-optics-optical-fiber

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory?. International Political Science Review, 27(3), 221-244. doi: 10.1177/0192512106064462

Ermert, M. (2015). Internet Governance Forum: Ten Years After - Intellectual Property Watch. Retrieved 11 November 2020, from https://www.ip-watch.org/2015/11/16/internet-governance-forum-ten-years-after

Ermert, M. (2015). Internet Governance Forum: Ten Years After - Intellectual Property Watch. Retrieved 11 November 2020, from https://www.ip-watch.org/2015/11/16/internet-governance-forum-ten-years-after

Everington, K. (2020). WHO Facebook video feed blocks word 'Taiwan' | Taiwan News | 2020/11/12. Retrieved 2 January 2021, from https://www.taiwannews.com.tw/en/news/4051742

Faria, J. (2020). Internet penetration in Africa 2020 | Statista. Retrieved 27 December 2020, from https://www.statista.com/statistics/1176654/internet-penetration-rate-africa-compared-to-global-average

Farrell, M. (2016). Quietly, symbolically, US control of the internet was just ended. Retrieved 15 November 2020, from https://www.theguardian.com/technology/2016/mar/14/icann-internet-

control-domain-names-iana

Farzan, Z. (2021). Sri Lanka's commitment for enhanced cooperation stressed at the 28th ASEAN Regional Forum (ARF). Retrieved 12 August 2021, from https://www.newsfirst.lk/2021/08/10/sri-lankas-commitment-for-enhanced-cooperation-stressed-at-the-28th-asean-regional-forum-arf/

Fascendini, F. (2015). Imagine a Feminist Internet: The conversation is on! | Association for Progressive Communications. Retrieved 14 January 2021, from https://www.apc.org/en/news/imagine-feminist-internet-conversation

Fasenfest, D. (2010). Government, Governing, and Governance. Critical Sociology, 36(6), 771-774. doi: 10.1177/0896920510378192

Feleke, B. (2020). Google launches balloon-powered internet service in Kenya. Retrieved 18 December 2020, from https://edition.cnn.com/2020/07/08/africa/google-kenya-balloons/index.html

Fidler, D. (2014). Le cyberspace, c'est moi?: Authoritarian Leaders, the Internet, and International Politics. Retrieved 5 January 2021, from https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2672&context=facpub

Fisher, M. (2015). Yes, North Korea has the internet. Here's what it looks like. Retrieved 7 May 2020, from https://www.vox.com/2014/12/22/7435625/north-korea-internet

Flew, T. (2017). Country rules: the 'splinternet' may be the future of the web. Retrieved 12 February 2021, from https://theconversation.com/country-rules-the-splinternet-may-be-the-future-of-the-web-81939

Foltýn, T. (2018). Europol sets up EU-wide team to fight dark web crime | WeLiveSecurity. Retrieved 2 September 2020, from https://www.welivesecurity.com/2018/06/01/europol-eu-team-fight-dark-web

Fouquet, H. (2021). China's 7,500-Mile Undersea Cable to Europe Fuels Internet Feud. Retrieved 8 March 2021, from https://www.bloomberg.com/news/articles/2021-03-05/china-s-peace-cable-in-europe-raises-tensions-with-the-u-s

Freeman, S. How Dictators Work. Retrieved 18 April 2020, from https://people.howstuffworks.com/dictator2.htm

Fried, D. (2018). 100 Years Later, Wilson's Fourteen Points Deserve Another Look. Retrieved

10 February 2020, from https://www.atlanticcouncil.org/blogs/new-atlanticist/100-years-later-wilson-s-fourteen-points-deserve-another-look

Froelich, P. (2020). France, China developing biologically engineered supersoldiers: report. Retrieved 21 January 2021, from https://nypost.com/2020/12/19/france-china-developing-biologically-engineered-super-soldiers

Fruhlinger, J. (2017). What is Stuxnet, who created it and how does it work?. Retrieved 26 April 2020, from https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Fuchs, C. (2013). Digital prosumption labour on social media in the context of the capitalist regime of time. *Time & Society, 23(1)*, 97-123. doi: 10.1177/0961463x13502117

Gallagher, R. (2018). The Powerful Global Spy Alliance You Never Knew Existed. Retrieved 18 May 2019, from https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors

Gan, G. (2021). Filling the gaps: Asia Pacific's cyber capacity building. Retrieved 14 July 2021, from https://www.thejakartapost.com/academia/2021/06/23/filling-the-gaps-asia-pacifics-cyber-capacity-building.html

Garrity, J. (2020). Funding to connect the remaining unconnected in Asia Pacific | APNIC Blog. Retrieved 9 June 2020, from https://blog.apnic.net/2020/01/08/funding-to-connect-the-remaining-unconnected-in-asia-pacific/

Gasser, U., Burkert, H., Palfrey, J., & Zittrain, J. (2012, February 18). Accountability and transparency AT ICANN: An independent Review (final report). Retrieved September 03, 2021, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1998905

Gault, M. (2020). How to Fake a Traffic Jam on Google Maps. Retrieved 14 September 2020, from https://www.vice.com/en_in/article/9393w7/this-man-created-traffic-jams-on-google-maps-using-a-red-wagon-full-of-phones

Gaurav, K. (2020). Taiwanese Apple contract manufacturers to invest $900 million in India: Report. Retrieved 1 November 2020, from https://www.republicworld.com/technology-news/gadgets/taiwanese-apple-contract-manufacturers-to-invest-900-dollars-million-in-india.html

Geere, D. (2011). How the first cable was laid across the Atlantic. Retrieved 30 April 2019, from https://www.wired.co.uk/article/transatlantic-cables

Gerden, E. (2017). Dedicated military intranet to help defend Russian armed forces. Retrieved 11

November 2020, from https://www.scmagazineuk.com/dedicated-military-intranet-help-defend-russian-armed-forces/article/1474829

Ghosh, S. (2017). Here's the letter Spotify's founders wrote to the EU complaining Apple and Google are abusive. Retrieved 19 December 2019, from https://www.businessinsider.com/spotify-deezer-rocket-internet-letter-european-commission-2017-5?r=UK&IR=T

Ghosh, S. (2019). How the 'Jio effect' brought millions of Indians online and is reshaping Silicon Valley and the internet. Retrieved 11 February 2021, from https://www.businessinsider.in/home/how-the-jio-effect-brought-millions-of-indians-online-and-is-reshaping-silicon-valley-and-the-internet/articleshow/70723349.cms

Gillespie, A. (2019). *Cybercrime: Key Issues and Debates* (2nd ed., pp. 99-131). London: Routledge.

Gold, J. (2021). Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?. Retrieved 29 March 2021, from https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what

Goldstein, P. (2016). What is NSFNET: How This Old Tech Sparked Scientific Research Opportunities. Retrieved 18 August 2020, from https://fedtechmagazine.com/article/2016/11/nsfnet-served-precursor-internet-helped-spur-scientific-research

Goodwin, T. (2015). The Battle Is For The Customer Interface. Retrieved 5 May 2020, from https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/

Greenberg, A. (2010). Visa, MasterCard Move To Choke WikiLeaks. Retrieved 9 May 2020, from https://www.forbes.com/sites/andygreenberg/2010/12/07/visa-mastercard-move-to-choke-wikileaks/?sh=654ed1912cad

Greenberg, A. (2017). A Brief Tour of Russia's Infrastructure Hacking Teams. Retrieved 9 June 2020, from https://www.wired.com/story/russian-hacking-teams-infrastructure

Greppi, E. (2018). International Humanitarian Law in Cyber Operations. Retrieved 10 November 2020, from https://www.ispionline.it/it/pubblicazione/international-humanitarian-law-cyber-operations-20372

Guay, J., & Rudnick, L. (2017). What the Digital Geneva Convention means for the future of

humanitarian action - UNHCR Innovation. Retrieved 5 January 2020, from https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action

Gurung, M. (2020). Whatsapp Will Soon Bring Advertisements To Make Money; Your 'Status' Will Be Used For Ads?. Retrieved 2 November 2020, from https://trak.in/tags/business/2020/04/25/whatsapp-will-soon-bring-advertisements-to-make-money-your-status-will-be-used-for-ads

Ha, A. (2020). Facebook-backed Libra Association rebrands as Diem. Retrieved 31 December 2020, from https://techcrunch.com/2020/12/01/libra-association-rebrands-as-diem

Haaster, J., Gevers, R., & Sprengers, M. (2016). *Cyber guerilla* (pp. 1-15). Amsterdam: Elsevier.

Hakmeh, J. (2018). Cybercrime Legislation in the GCC Countries Fit for Purpose?. Retrieved 2 June 2020, from https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh.pdf

Halappanavar, A. (2020). Submarine Cable Network: The Global Sovereign Asset. Retrieved 28 November 2020, from https://usanasfoundation.com/submarine-cable-network-the-global-sovereign-asset

Hallaert, J. (2020). The Tragedy of International Organizations in a World Order in Turmoil. Retrieved 4 January 2021, from https://ecipe.org/publications/tragedy-of-international-organizations/

Han, Z., & Paul, T. (2020). China's Rise and Balance of Power Politics. The Chinese Journal Of International Politics, 13(1), 1-26. doi: 10.1093/cjip/poz018

Hannan, M. (2021). How the World Wide Web changed our lives on its 30th anniversary. Retrieved 7 August 2021, from https://www.thenational.scot/news/19495205.thirty-years-internet-world-wide-web-changed-lives/

Hardy, S. (2018). SAIL submarine cable installation completed. Retrieved 18 June 2020, from https://www.lightwaveonline.com/network-design/high-speed-networks/article/16675847/sail-submarine-cable-installation-completed

Harris, K., Beis, C., & Shreffler, S. (2021, August 13). The internet Archive has been fighting for 25 years to keep what's on the web from disappearing – and you can help. Retrieved August 14, 2021, from https://theconversation.com/the-internet-archive-has-been-fighting-for-25-years-to-keep-whats-on-the-web-from-disappearing-and-you-can-help-163867

Harsono, H. (2020). China's Surveillance Technology Is Keeping Tabs on Populations Around

the World. Retrieved 24 September 2020, from https://thediplomat.com/2020/06/chinas-surveillance-technology-is-keeping-tabs-on-populations-around-the-world

Hart, Jeffrey. (2005). The G8 and the Governance of Cyberspace. 10.4324/9781315248035-9.

Hawkins, A. (2019). Serious safety lapses led to Uber's fatal self-driving crash, new documents suggest. Retrieved 5 November 2020, from https://www.theverge.com/2019/11/6/20951385/uber-self-driving-crash-death-reason-ntsb-dcouments

Haworth, J. (2019). ASEAN nations strengthen cybersecurity ties through new cooperation agreement. Retrieved 1 November 2019, from https://portswigger.net/daily-swig/asean-nations-strengthen-cybersecurity-ties-through-new-cooperation-agreement

Herberger, C. (2016). Cybersecurity in the Real World: 4 Examples of the Rise of Public Transportation Systems Threats | Radware Blog. Retrieved 3 July 2020, from https://blog.radware.com/security/2016/04/cybersecurity-4-public-transportation-threats

Hern, A. (2017). Thirty countries use 'armies of opinion shapers' to manipulate democracy – report. Retrieved 15 February 2020, from https://www.theguardian.com/technology/2017/nov/14/social-media-influence-election-countries-armies-of-opinion-shapers-manipulate-democracy-fake-news

Hirji, Z. (2015). Benchmarks: December 1, 1959: Antarctic Treaty Signed. Retrieved 3 October 2020, from https://www.earthmagazine.org/article/benchmarks-december-1-1959-antarctic-treaty-signed

Hodges, A. (2014). *Alan Turing: The Enigma* (pp. 212-214). London: Vintage, Penguin Random House.

Holt, T. (2019). How vulnerable is your car to cyberattacks?. Retrieved 17 November 2020, from https://msutoday.msu.edu/news/2019/how-vulnerable-is-your-car-to-cyberattacks/

Hooper, S. (2021). OIC's cyber agency working with Huawei despite Uighur surveillance concerns. Retrieved 2 May 2021, from https://www.middleeasteye.net/news/oic-cyber-agency-working-with-huawei-despite-uighur-surveillance-concerns

Hopkins, N., Easen, N., & Young, S. (2000). CNN.com - China: If ICANN, so can we. Retrieved 22 April 2020, from http://edition.cnn.com/2000/ASIANOW/business/11/20/ebiz.icann/index.html

Hove, K. (2017). The SADC Model Law on Computer Crime and Cybercrime: A Harmonised

Assault on the Right to Privacy?. Retrieved 11 April 2020, from https://www.linkedin.com/pulse/sadc-model-law-computer-crime-cybercrime-harmonised-assault-kuda-hove

Hurd, I. (2015). International Law and politics of diplomacy. In I. Neumann, V. Pouliot, O. Sending (Eds.), *Diplomacy and the Making of World Politics* (pp. 31-54). Cambridge, United Kingdom: Cambridge University Press.

Huston, G. (2020). Opinion: Defining Cyber Governance | APNIC Blog. Retrieved 8 November 2020, from https://blog.apnic.net/2020/08/07/opinion-defining-cyber-governance/

Inman, P. (2019). Mark Carney: dollar is too dominant and could be replaced by digital currency. Retrieved 14 February 2020, from https://www.theguardian.com/business/2019/aug/23/mark-carney-dollar-dominant-replaced-digital-currency

Iscrupe, L. (2020). Project Loon | Updates on Google's Alternative Internet Solution. Retrieved 1 December 2020, from https://www.allconnect.com/blog/google-project-loon

Issaias, A. (2019). Analysis of the Data Protection Act 2019 in Kenya | Bowmans. Retrieved 7 July 2020, from https://www.bowmanslaw.com/insights/intellectual-property/snapshot-analysis-of-the-data-protection-act-2019/

Jackson, S. (2021). Digicel estimates 100m hack attempts in the Caribbean. Retrieved 14 July 2021, from https://jamaica-gleaner.com/article/business/20210711/digicel-estimates-100m-hack-attempts-caribbean

Jacobs, J. (2019, April 08). Wikipedia isn't officially a social NETWORK. but the harassment can get ugly. Retrieved November 03, 2020, from https://www.nytimes.com/2019/04/08/us/wikipedia-harassment-wikimedia-foundation.html

Jesdanun, A. (2010). Internet agency approves domains in native scripts. Retrieved 14 October 2020, from https://phys.org/news/2010-03-internet-agency-domains-native-scripts.html

Johnson, J. (2021). Internet users in the world 2021 | Statista. Retrieved 12 April 2021, from https://www.statista.com/statistics/617136/digital-population-worldwide

Johnson, J. (2021). Internet users in the world 2021 | Statista. Retrieved 6 March 2021, from https://www.statista.com/statistics/617136/digital-population-worldwide

Johnson, K. (2019). Partnership on AI's Terah Lyons talks ethics washing, moonshots, and power. Retrieved 7 May 2020, from https://venturebeat.com/2019/08/27/partnership-on-ais-

terah-lyons-talks-ethics-washing-moonshots-and-power/

Joyce, D. (2015). Privacy in the digital era: Human rights online?. *Melbourne Journal Of International Law,* 16(1), 270-285.

Kant, I. (1983). *Toward Perpetual Peace and Other Writings on Politics, Peace, and History* (pp. 82-83). Indianapolis: Hackett Publishing Company.

Katoch, P. (n.d.) Surgical strike in cyberspace. Retrieved 18 October 2020, from http://www.spslandforces.com/experts-speak/?id=166&h=Surgical-strike-in-cyberspace

Katz, D., & Ford, P. (1993). TUBA: replacing IP with CLNP. IEEE Network, 7(3), 38-47. doi: 10.1109/65.224020

Keane, M. (2021). China's record fine against Alibaba spells the end of big tech's romance with the state. Retrieved 21 April 2021, from https://theconversation.com/chinas-record-fine-against-alibaba-spells-the-end-of-big-techs-romance-with-the-state-158878

Kelley, J. (2021). EFF at 30: Freeing the Internet, with Net Neutrality Pioneer Gigi Sohn. Retrieved 30 July 2021, from https://www.eff.org/deeplinks/2021/07/eff-30-freeing-internet-net-neutrality-pioneer-gigi-sohn

Kelly, S., Truong, M., Shahbaz, A., Earp, M., & White, J. (2017). Manipulating Social Media to Undermine Democracy. Retrieved 15 November 2020, from https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy

Kessler, A. (2018). Who is @TEN_GOP in the Mueller indictment?. Retrieved 2 September 2020, from https://edition.cnn.com/2018/02/16/politics/who-is-ten-gop/index.html

Kharpal, A. (2020). Power is 'up for grabs': Behind China's plan to shape the future of next-generation tech. Retrieved 13 November 2020, from https://www.cnbc.com/2020/04/27/china-standards-2035-explained.html

Kinyua, B. (2021). How China is Winning the Subsea Internet Cable Competition in Africa. Retrieved 28 March 2021, from https://www.maritime-executive.com/editorials/how-china-is-winning-the-subsea-internet-cable-competition-in-africa

Koerner, B. (2016). Inside the OPM Hack, the Cyberattack That Shocked the US Government. Retrieved 13 August 2019, from https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government

Krigman, A. (2020). Ukrainian Power Grid Attack - Blog | GlobalSign. Retrieved 13 January

2021, from https://www.globalsign.com/en/blog/cyber-autopsy-series-ukranian-power-grid-attack-makes-history

Krishnan, A. (2021). China still 'largest source of critical items' for India. Retrieved 4 February 2021, from https://www.thehindu.com/news/national/china-still-largest-source-of-critical-items-for-india/article33704790.ece

Krishnan, S., & Ranganathan, S. (2009). Deconstructing 'Internet addiction'. Retrieved 16 June 2020, from http://www.hindu.com/2009/08/30/stories/2009083052781400.htm

Kropotov, V., Lin, P., Hacquebord, F., & Yarochkin, F. (2017). A Closer Look at North Korea's Internet. Retrieved 16 November 2019, from https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-north-koreas-internet

Kruger, L. (2016). The Future of Internet Governance: Should the United States Relinquish Its Authority over ICANN? Retrieved June 16, 2020, from https://sgp.fas.org/crs/misc/R44022.pdf

Kuhn, T. (1970). The Structure of Scientific Revolutions. Retrieved 18 November 2019, from https://www.lri.fr/~mbl/Stanford/CS477/papers/Kuhn-SSR-2ndEd.pdf

Kulenkampff, N. (2021). Navigating online harassment: How to take control | ZDNet. Retrieved 6 August 2021, from https://www.zdnet.com/article/navigating-online-harassment/

Kumar, A. (2021, July 25). All you wanted to know about Pegasus but didn't know who to ask. Retrieved July 28, 2021, from https://www.indiatoday.in/india/story/all-you-wanted-know-about-pegasus-spyware-controversy-nso-israel-india-1832051-2021-07-24

Kundaliya, D. (2020). GCSC proposes rules to guide states towards responsible cyber behaviour. Retrieved 4 January 2021, from https://www.computing.co.uk/news/4023329/gcsc-rules-responsible-cyber-behaviour

Kuo, L. (2018). World's first AI news anchor unveiled in China. Retrieved 15 November 2020, from https://www.theguardian.com/world/2018/nov/09/worlds-first-ai-news-anchor-unveiled-in-china

Kurra, B. (2011). How 9/11 Completely Changed Surveillance in U.S. Retrieved 20 April 2020, from https://www.wired.com/2011/09/911-surveillance

Lack, D. (1983). *Darwin's Finches* (2nd ed., pp. 70-134). Cambridge: Cambridge University Press.

Lamm, G. (2017). Microsoft slams U.S. government for 'stockpiling' cyberattack vulnerabilities. Retrieved 15 November 2019, from

https://www.bizjournals.com/seattle/news/2017/05/15/microsoft-slams-nsa-windows-ransomeware-attack.html

Lavallée, B. (2016). The Story Behind the First Reliable Trans-Atlantic Submarine Cable Laid 150 Years Ago. Retrieved 11 September 2020, from https://www.ciena.com/insights/articles/The-First-Trans-Atlantic-Message-150-Years-Ago-prx.html

Lawson, S., & Middleton, M. (2016). View of Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016. Retrieved 11 November 2020, from https://firstmonday.org/ojs/index.php/fm/article/view/9623/7736

Lee, D. (2016). Has the US just given away the internet?. Retrieved 10 October 2019, from https://www.bbc.com/news/technology-37527719

Lee, D. (2016). Has the US just given away the internet?. Retrieved 15 April 2020, from https://www.bbc.com/news/technology-37527719

Lee, D., & Kwek, N. (2015). North Korean hackers 'could kill', warns key defector. Retrieved 21 October 2019, from https://www.bbc.com/news/technology-32925495

Leiner, B. (1997). Brief History of the Internet. Retrieved 6 November 2020, from https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf

Lempert, R. (2013). PRISM and Boundless Informant: Is NSA Surveillance a Threat?. Retrieved 1 July 2020, from https://www.brookings.edu/blog/up-front/2013/06/13/prism-and-boundless-informant-is-nsa-surveillance-a-threat

LEONARD, A. (2020). How Taiwan’s Unlikely Digital Minister Hacked the Pandemic. Retrieved 10 October 2020, from https://www.wired.com/story/how-taiwans-unlikely-digital-minister-hacked-the-pandemic/

Fernandez, R. (2021). How Big Tech is becoming the Government. Retrieved 24 February 2021, from https://www.somo.nl/how-big-tech-is-becoming-the-government

Robertson, J., & Riley, M. (2018). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Retrieved 5 September 2020, from https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Lessig, L. (2000). Code Is Law. Retrieved 11 March 2020, from https://www.harvardmagazine.com/2000/01/code-is-law-html

Lété, B. (2021). The Paris Call and Activating Global Cyber Norms. Retrieved 18 March 2021, from https://www.gmfus.org/news/paris-call-and-activating-global-cyber-norms

Leuthard, D. (2018). It's time to strengthen global digital cooperation. Retrieved 15 July 2020, from https://www.weforum.org/agenda/2018/12/its-time-to-strengthen-global-digital-cooperation/

Leyden, J. (2016). Guess what's 'easily hacked'? Yes, that's right: Smart city transport infrastructure. Retrieved 7 November 2020, from https://www.theregister.co.uk/2016/04/22/smart_transport_hackable

Leyden, J. (2016). Sweden 'secretly blames' hackers – not solar flares – for taking out air traffic control. Retrieved 25 June 2020, from https://www.theregister.com/2016/04/12/sweden_suspects_russian_hackers_hit_air_traffic_control/

Leyden, J. (2019). ARPANET anniversary: The internet's first transmission was sent 50 years ago today. Retrieved 2 February 2020, from https://portswigger.net/daily-swig/arpanet-anniversary-the-internets-first-transmission-was-sent-50-years-ago-today

Leyes, Z. (2015). What is BGP | Border Gateway Protocol Explained. Retrieved 10 October 2020, from https://www.imperva.com/blog/bgp-routing-explained

Licklider, J. (1960). Man-Computer Symbiosis. IRE Transactions On Human Factors In Electronics, HFE-1(1), 4-11. doi: 10.1109/thfe2.1960.4503259

Lillington, K. (1999). EU may stifle e-commerce - GIP. Retrieved 26 February 2020, from https://www.irishtimes.com/business/eu-may-stifle-e-commerce-gip-1.228439

Lynch, J. (2018). Trump's national cyber strategy praised by experts. Retrieved 23 November 2020, from https://www.fifthdomain.com/congress/policy/2018/09/21/trumps-national-cyber-strategy-praised-by-experts/

Lyons, K. (2018). 'Palau against China!': The tiny ISLAND standing up to a giant. Retrieved August 21, 2020, from https://www.theguardian.com/global-development/2018/sep/08/palau-against-china-the-tiny-island-defying-the-worlds-biggest-country

Madrigal, A. (2010). The Man Who First Said 'Cyborg,' 50 Years Later. Retrieved 8 August 2019, from https://www.theatlantic.com/technology/archive/2010/09/the-man-who-first-said-cyborg-50-years-later/63821

Malcomson, S. (2016). *Splinternet How Geopolitics and Commerce Are Fragmenting the World*

Wide Web (pp. 139-172). New York: OR Books.

Malik, Y. (2017). Smart, Connected and IoT Based Devices. What's The Difference?. Retrieved 23 October 2020, from https://medium.com/smart-connected-and-iot-based-devices-whats-the-difference-36fc1bdc36b2.

Mammadov, S. (2020). Silk Road on the Ice: A convenient route for Eurasian cooperation. Retrieved 17 November 2020, from https://news.cgtn.com/news/2020-09-18/Silk-Road-on-the-Ice-A-convenient-route-for-Eurasian-cooperation--TSXp8DtQd2/index.html

Manky, D. (2019). AI-based Fuzzing Could Change Security. Retrieved 12 July 2020, from https://www.fortinet.com/blog/industry-trends/how-aif-will-affect-the-cybercrime-economy

Manos, D. (2013). What is Snowden's impact on health IT?. Retrieved 8 February 2020, from https://www.healthcareitnews.com/news/hero-or-traitor-what-snowdens-impact-public-trust-health-it

Marda, V. (2016). Internet democratisation: Iana transition leaves much to be desired. Retrieved May 03, 2020, from https://www.hindustantimes.com/analysis/internet-democratisation-iana-transition-leaves-much-to-be-desired/story-t94hojZjDXqS4LjNSepZlN.html

Margolin, J. (2016). Russia, China, and the Push for "Digital Sovereignty". Retrieved 12 March 2020, from https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/

Markoff, J. (2010). Google Asks Spy Agency for Help With Inquiry Into Cyberattacks. Retrieved 17 January 2021, from https://www.nytimes.com/2010/02/05/science/05google.html

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336. doi: 10.1016/j.clsr.2019.06.007

Maroz, N. (2019). Regionalization of international cooperation in the fight against cybercrime. Catholic University Law Review, 10(2), 218-227.

Mathiason, J. (2009). *Internet Governance* (pp. 97-126). New York: Routledge.

Matsumoto, F. (2021). Chinese bids on Pacific cable raise alarm in US and Australia. Retrieved 8 January 2021, from https://asia.nikkei.com/Politics/International-relations/Chinese-bids-on-Pacific-cable-raise-alarm-in-US-and-Australia

May, T., & Woods, M. (1979). Alpha-particle-induced soft errors in dynamic memories. IEEE Transactions On Electron Devices, 26(1), 2-9. doi: 10.1109/t-ed.1979.19370

Chang, K. (2021). A piece of debris whizzes past the Crew Dragon. Retrieved 26 April 2021, from https://www.nytimes.com/2021/04/23/science/space-junk.html

Diwakar, A. (2021). 'Chip Wars': US, China and the battle for semiconductor supremacy. Retrieved 5 April 2021, from https://www.trtworld.com/magazine/chip-wars-us-china-and-the-battle-for-semiconductor-supremacy-45052

McCartney, P. (2020). Bahamas ranks low in ECLAC cybersecurity report - The Nassau Guardian. Retrieved 2 January 2021, from https://thenassauguardian.com/bahamas-ranks-low-in-eclac-cybersecurity-report/

McCartney, S. (2001). *ENIAC* (p. 112). New York: Berkley Books.

McCue, T. (2019). How Can I Tell If My Internet Provider Is Throttling (Slowing) My Connection Speed?. Retrieved 24 September 2020, from https://www.forbes.com/sites/tjmccue/2019/06/27/how-can-i-tell-if-my-internet-provider-is-throttling-slowing-my-connection-speed/

McCullagh, D. (2008). How Pakistan knocked YouTube offline (and how to make sure it never happens again). Retrieved 14 August 2020, from https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/

McGlinchey, S. (2017). Diplomacy. Retrieved 17 December 2020, from https://www.e-ir.info/2017/01/08/diplomacy/

Mcintosh, D. (2021). Early Warning Cybersecurity System Implemented – Jamaica Information Service. Retrieved 24 May 2021, from https://jis.gov.jm/early-warning-cybersecurity-system-implemented/

McKune, S. (2015). An Analysis of the International Code of Conduct for Information Security. Retrieved 5 November 2019, from https://citizenlab.ca/2015/09/international-code-of-conduct/

Meade, A. (2020). Australia is making Google and Facebook pay for news: what difference will the code make?. Retrieved 8 January 2021, from https://www.theguardian.com/media/2020/dec/09/australia-is-making-google-and-facebook-pay-for-news-what-difference-will-the-code-make#:~:text=The%20Australian%20government%20tabled%20world,Facebook's%20newsfeed%20and%20Google's%20search

Meltzer, J., & Kerry, C. (2019). Cybersecurity and digital trade: Getting it right. Retrieved 12 November 2020, from https://www.brookings.edu/research/cybersecurity-and-digital-trade-

getting-it-right

Meltzer, J., & Kerry, C. (2021). Strengthening international cooperation on artificial intelligence. Retrieved 25 February 2021, from https://www.brookings.edu/research/strengthening-international-cooperation-on-artificial-intelligence/

Mercer, D. (2019). Global Connected and IoT Device Forecast Update. Retrieved 19 November 2019, from https://www.strategyanalytics.com/access-services/devices/connected-home/consumer-electronics/reports/report-detail/global-connected-and-iot-device-forecast-update

Metz, C. (2012). Larry Roberts Calls Himself the Founder of the Internet. Who Are You to Argue?. Retrieved 31 August 2019, from https://www.wired.com/2012/09/larry-roberts

Meyers, A. (2019). APTs & Adversary Groups List - Malware & Ransomware | Crowdstrike Adversary Universe. Retrieved 6 October 2020, from https://www.crowdstrike.com/blog/meet-the-adversaries

Mihr, A. (2017). *Cyber Justice: Human Rights and Good Governance for the Internet* (1st ed., pp. 15-35). New York: Springer.

Miller, M. (2019). Hundreds arrested worldwide in operation targeting cyber schemes. Retrieved 12 April 2020, from https://thehill.com/policy/cybersecurity/460775-hundreds-arrested-worldwide-in-operation-targeting-cyber-schemes

Miller, S. (2020). As states explore online voting, new report warns of ‘severe risk’ -- GCN. Retrieved 20 August 2020, from https://gcn.com/articles/2020/06/08/mit-cautions-online-voting.aspx

Mims, C. (2013). Google, Facebook, MICROSOFT, others allegedly allow the US government to "watch your ideas form as you type". Retrieved April 17, 2020, from https://qz.com/91909/nsa-fbi-secret-surveillance-google-facebook-microsoft-yahoo-aol-and-skype/

Miranda, R., Casebeer, W., Hein, A., Judy, J., Krotkov, E., & Laabs, T. et al. (2015). DARPA-funded efforts in the development of novel brain–computer interface technologies. Journal Of Neuroscience Methods, 244, 52-67. doi: 10.1016/j.jneumeth.2014.07.019

Mitchell, H. (2021). Health data hacking incidents spike 42% during pandemic: report. Retrieved 24 March 2021, from https://www.beckershospitalreview.com/cybersecurity/health-data-hacking-incidents-spike-42-during-pandemic-report.html

Mitnick, K. (2019). *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data* (pp. 232-233). New York: Little, Brown and Company.

Modak, S. (2018). Atlanta Airport Shuts Down Wi-Fi Following Cyber Attack on City. Retrieved 11 September 2020, from https://www.cntraveler.com/story/atlanta-airport-shuts-down-wi-fi-following-cyber-attack-on-city

Monroy, M. (2020). New German military exercises with Israel – Matthias Monroy. Retrieved 11 December 2020, from https://digit.site36.net/2020/01/10/new-german-military-exercises-with-israel/

Morris, S., & Kehl, D. (2014). The Highs and Lows of the Net Neutrality Debate in 2014. Retrieved 18 December 2019, from https://slate.com/technology/2014/12/net-neutrality-debate-2014-the-open-internet-rules-roller-coaster.html

Murphy Jr., B. (2020). Google Maps Just Introduced a Controversial New Feature That Drivers Will Probably Love but Police Will Utterly Hate. Retrieved 22 December 2020, from https://www.inc.com/bill-murphy-jr/google-maps-just-introduced-a-controversial-new-feature-that-drivers-will-probably-love-but-police-will-utterly-hate.html

Murphy, B. (2020). Interdoc: The first international non-governmental computer network | Association for Progressive Communications. Retrieved 1 November 2020, from https://www.apc.org/en/about/history/interdoc

Murphy, H., & Sheppard, D. (2021). Saudi Aramco confirms data leak after $50m cyber ransom demand. Retrieved 29 July 2021, from https://www.ft.com/content/272259b0-8e98-4b49-8047-f4b8a2d33e95

Murthy, K., Kalsie, A., & Shankar, R. (2021). Digital economy in a global perspective: is there a digital divide?. Transnational Corporations Review, 13(1), 1-15. doi: 10.1080/19186444.2020.1871257

Liu, A. (2020). AstraZeneca staffers targeted in suspected hacking scheme amid work on COVID-19 vaccine: report. Retrieved 5 February 2021, from https://www.fiercepharma.com/pharma/astrazeneca-staffers-targeted-suspected-hacking-amid-work-covid-vaccine-report

Adams, M. (2019). A warning about tallinn 2.0 ... whatever it says. Retrieved September 11, 2020, from https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-

says

Mzekandaba, S. (2019). SA is 'safe haven for cyber criminals'. Retrieved 1 February 2020, from https://www.itweb.co.za/content/lwrKxv3JO1Lqmg1o

Najžer, B. (2020). *The Hybrid Age International Security in the Era of Hybrid Warfare* (pp. 61-82). London: I B TAURIS.

Nakashima, E. (2011). Obama administration outlines international strategy for cyberspace. Retrieved 25 September 2020, from https://www.washingtonpost.com/world/obama-administration-outlines-international-strategy-for-cyberspace/2011/05/16/AFokL54G_story.html

Nakashima, E. (2013). Chinese hackers who breached Google gained access to sensitive data, U.S. officials say. Retrieved 19 December 2020, from https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html

Nakashima, E., & Warrick, J. (2012). Stuxnet was work of U.S. and Israeli experts, officials say. Retrieved 15 November 2020, from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Navarria, G. (2016). How the Internet was born: from the ARPANET to the Internet. Retrieved 31 October 2019, from https://theconversation.com/how-the-internet-was-born-from-the-arpanet-to-the-internet-68072

Netanel, N. (2000). Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory. California Law Review, 88(2), 395. doi: 10.2307/3481227

Nettey, N. (2019). Interrogate application of Int'l law in cyberspace – Ursula to International Community. Retrieved 8 February 2021, from https://citinewsroom.com/2019/11/interrogate-application-of-intl-law-in-cyberspace-ursula-to-international-community/

Neumann, I (2002). Discussion Papers in Diplomacy: The English School on Diplomacy. Retrieved 9 July 2020, from https://www.clingendael.org/sites/default/files/pdfs/20020300_cli_paper_dip_issue79.pdf

Newman, L. (2019). Amber Authenticate Protects Video Footage From Deepfakes and Tampering. Retrieved 19 September 2020, from https://www.wired.com/story/amber-authenticate-video-validation-blockchain-tampering-deepfakes

Newton, M., & Park, D. (2017). Russia Is Now Providing North Korea With Internet: What That Could Mean For Cyber Warfare. Retrieved 17 October 2020, from https://www.forbes.com/sites/outofasia/2017/12/01/russia-is-now-providing-north-korea-with-internet-what-that-could-mean-for-cyber-warfare/?sh=2d3dfb9c386b

Nitu, A. (2011). International Legal Issues and Approaches Regarding Information Warfare. *Journal of Information Warfare Vol. 10, No. 2 (2011), Pp. 48-57 (10 Pages), 10*(2), 48-57.

Nohe, P. (2018). What is an Air Gapped Computer?. Retrieved 1 June 2020, from https://www.thesslstore.com/blog/air-gapped-computer

Nordquist, R. (2020). Is Twitter Destroying Our Language or Rejuvenating It?. Retrieved 14 January 2021, from https://www.thoughtco.com/tweet-definition-1692478

Nye, J. (2014). The Regime Complex for Managing Global Cyber Activities. Retrieved 2 April 2019, from https://www.hks.harvard.edu/publications/regime-complex-managing-global-cyber-activities

O' Connor, T. (2017). North Korea says it will bomb Guam If Trump keeps tweeting threats. Retrieved 17 November 2020, from https://www.newsweek.com/north-korea-attack-us-territory-guam-trump-keeps-tweeting-threats-684716

O' Connor, T. (2020). U.S. calls video showing China bomb U.S. air base "attempt to coerce, intimidate." Retrieved 19 November 2020, from https://www.newsweek.com/us-call-video-show-china-bombing-air-base-coerce-intimidate-1533894

Ó Siochrú, S. (2007). United Nations Development Programme (UNDP) | Global Information Society Watch. Retrieved 1 April 2020, from https://giswatch.org/institutional-overview/civil-society-participation/united-nations-development-programme-undp

O'Higgins Norman, J. (2020). Tackling Bullying from the Inside Out: Shifting Paradigms in Bullying Research and Interventions. International Journal Of Bullying Prevention, 2(3), 161-169. doi: 10.1007/s42380-020-00076-1

OAS. (2012). Dialogue on Cyber Security at the OAS. Retrieved 14 October 2020, from http://www.thebahamasweekly.com/publish/oas-media-releases/Dialogue_on_Cyber_Security_at_the_OAS25646.shtml

O'Connor, T., & Jamali, N. (2020). NATO assessing damage from SolarWinds hack, Canada issues alert. Retrieved 2 January 2021, from https://www.newsweek.com/nato-assessing-

damage-solarwinds-hack-canada-issues-alert-1554964

Oguro, K. (2016). RIETI - Big Data—Key to the 4th Industrial Revolution. Retrieved 5 November 2020, from https://www.rieti.go.jp/en/papers/contribution/oguro/07.html

Okuttah, M. (2010). East Africa: EAC Eyes Trade Growth With Cyber Laws. Retrieved 9 June 2020, from https://allafrica.com/stories/201006240090.html

O'Neill, K. (2019). Facebook's '10 Year Challenge' Is Just a Harmless Meme—Right?. Retrieved 7 January 2021, from https://www.wired.com/story/facebook-10-year-meme-challenge/

Opp, R. (2021). Digital is changing development. UNDP is changing too. | United Nations Development Programme. Retrieved 1 May 2021, from https://www.undp.org/blogs/digital-changing-development-undp-changing-too

Ott, C. (2018). What You Should Know About The 24/7 Cybercrime Network. Retrieved 9 July 2020, from https://www.dwt.com/files/uploads/documents/publications/What%20You%20Should%20Know%20About%20The%2024.pdf

Oude Elferink, A. (1992). Environmental protection in the Arctic—the ROVANIEMI PROCESS. Marine Pollution Bulletin, 24(3), 128-130. doi:10.1016/0025-326x(92)90239-3

Outer, D. (2008). Whose Summit? Whose Information Society. Retrieved 27 April 2020, from https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/47502/IDL-47502.pdf?sequence=1

Oye, K. (1985). Explaining Cooperation under Anarchy: Hypotheses and Strategies. *World Politics, 38*(1), 1-24. doi:10.2307/2010349

Paganini, P. (2016). NATO officially recognizes cyberspace a warfare domain. Retrieved 29 October 2020, from https://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html

Pagliery, J. (2015). The inside story of the biggest hack in history. Retrieved 8 June 2020, from https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html

Park, D., Summers, J., & Walstrom, M. (2017). Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks - The Henry M. Jackson School of International Studies. Retrieved 6 October 2019, from https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks

Parke, P. (2016). More Africans have phone service than piped water - CNN. Retrieved 16 October 2020, from https://edition.cnn.com/2016/01/19/africa/africa-afrobarometer-

infrastructure-report/index.html

Paul, K. (2019). What is Libra? All you need to know about Facebook's new cryptocurrency. Retrieved 11 March 2020, from https://www.theguardian.com/technology/2019/jun/18/what-is-libra-facebook-new-cryptocurrency

Paul, K. (2020). What you need to know about the biggest hack of the US government in years. Retrieved 30 December 2020, from https://www.theguardian.com/technology/2020/dec/15/orion-hack-solar-winds-explained-us-treasury-commerce-department

Peng, X. (2018). The Internet Global Village - International Law and Technology Interoperability Association. Retrieved 30 August 2020, from https://iltia.org/project/the-internet-global-village/

Perez Grandi, A., Sarri, A., & Paggio, V. (2021). What Europe's SMEs need to do for a cyber-secure future. Retrieved 2 July 2021, from https://www.weforum.org/agenda/2021/06/cybersecurity-for-smes-europe/

Peter, L. (2018). What makes Russia's new spy ship yantar special? Retrieved August 19, 2020, from https://www.bbc.com/news/world-europe-42543712

Peters, A. (2017). This Company Brings Free Mobile Internet To 40 Million People Globally. Retrieved 2 July 2020, from https://www.fastcompany.com/40496157/this-company-brings-free-mobile-internet-to-40-million-people-globally

Pisch, S. (2011, January 18). Nexans wins contract FOR Libya-Greece cable - it News Africa - up to date technology news, it news, Digital news, Telecom News, Mobile NEWS, Gadgets news, analysis and reports. Retrieved August 31, 2020, from https://www.itnewsafrica.com/2011/01/nexans-wins-contract-for-libya-greece-cable/

Plaut, M. (2010). Book says hacker tried to stop Mandela coming to power. Retrieved 16 June 2019, from https://www.bbc.com/news/world-africa-11630092

Poh, M. (2020). 20 Dictionary Words Originated From The Internet - Hongkiat. Retrieved 26 December 2020, from https://www.hongkiat.com/blog/dictionary-words-from-internet

Pohl, R. (2019). *An analysis of Donna Haraway's A Cyborg Manifesto* (pp. 30-45). London: Macat International Limited.

Pomerleau, M. (2019). Here are the problems offensive cyber poses for NATO. Retrieved 11 June 2020, from https://www.fifthdomain.com/international/2019/11/20/here-are-the-problems-offensive-cyber-poses-for-nato/

Prasso, S. (2019). China's Digital Silk Road Is Looking More Like an Iron Curtain. Retrieved 10 May 2020, from https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain

Priest, D., Timberg, C., & Mekhennet, S. (2021). Private Israeli spyware used to hack cellphones of journalists, activists worldwide. Retrieved 27 July 2021, from https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

Prinsloo, L. (2018). Google's Solution for African Internet: Balloons. Retrieved 6 January 2020, from https://www.bloomberg.com/news/articles/2018-11-16/google-s-solution-for-african-internet-balloon

Pullman, D. (2021). Operator of tonga's internet cable can't rule out sabotage: Tonga - the Expat reporter. Retrieved July 19, 2021, from https://tonga.expatreporter.com/2021/03/24/tonga-repair-internet-cabel/

Qingqing, C. (2019). Huawei's undersea cable project moves forward in SE Asia - Global Times. Retrieved 16 November 2020, from https://www.globaltimes.cn/content/1155060.shtml

Rahn, W. (2020). Zhenhua data leak exposes China's new 'hybrid warfare' | DW | 29.09.2020. Retrieved 15 December 2020, from https://www.dw.com/en/zhenhua-data-leak-exposes-chinas-new-hybrid-warfare/a-55083540

Rajan, A. (2020). No such thing as the internet. Retrieved 26 November 2020, from https://www.bbc.com/news/entertainment-arts-54514574

Rakheja, H. (2020). WhiteHat Jr Told To Remove Misleading Ads After Social Media Furore. Retrieved 2 December 2020, from https://inc42.com/buzz/whitehat-jr-told-to-remove-misleading-ads-after-social-media-furore

Rampal, N. (2019). More than 350 Internet shutdowns in India since 2014. Retrieved 1 May 2020, from https://www.indiatoday.in/diu/story/more-than-350-internet-shutdowns-in-india-since-2014-1629203-2019-12-18

Rana, L., & Raj, S. (2020). Data Scraping And Legal Issues In India - Intellectual Property - India. Retrieved 2 August 2020, from https://www.mondaq.com/india/copyright/900156/data-scraping-and-legal-issues-in-india

Ratner, P. (2018). The 7 longest ruling dictators in the world. Retrieved 18 January 2019, from https://bigthink.com/paul-ratner/the-7-longest-ruling-dictatorships-in-the-world

Raymond, M. (2012). The Internet as a Global Commons?. Retrieved 23 April 2020, from https://www.cigionline.org/publications/internet-global-commons/

Reed, S., Akata, Z., Yan, X., Logeswaran, L., Schiele, B., & Lee, H. (2016). Proceedings of the 33rd International Conference on Machine Learning. In *Proceedings of Machine Learning Research* (pp. 1060-1069). New York, NY, USA: JMLR:W&CP volume 48. Retrieved from http://proceedings.mlr.press/v48/reed16.html

Reed, T. (2004). *At the Abyss: An Insider's History of the Cold War* (pp. 267-269.). New York: Ballantine Books.

Resnick, P. (2014). RFC 7282 - On Consensus and Humming in the IETF. Retrieved 14 March 2020, from https://tools.ietf.org/html/rfc7282

Reynolds, M. (2020). Courts and lawyers struggle with growing prevalence of deepfakes. Retrieved 1 December 2020, from https://www.abajournal.com/web/article/courts-and-lawyers-struggle-with-growing-prevalence-of-deepfakes

Richard, R. (2020). China next-generation artificial intelligence development plan. Retrieved 18 November 2020, from https://24pm.com/ia-par-secteur/international/chine/582-china-next-generation-artificial-intelligence-development-plan

Rid, T. (2013). *Cyber War Will Not Take Place* (pp. 113-139). New York: Oxford University Press.

Riley, D. (2019). Digital identity sales on the rise through newly popular 'dark web' site - SiliconANGLE. Retrieved 2 November 2020, from https://siliconangle.com/2019/08/21/digital-identity-sales-rise-newly-popular-dark-web-site

Riotta, C. (2020). DOJ charges Russian intelligence officers for high-profile cyberattacks. Retrieved 27 December 2020, from https://www.independent.co.uk/news/world/americas/russia-cyber-attack-us-chanrged-doj-b1159592.html

Rodenhäuser, T., & Mačák, K. (2021). Even 'cyber wars' have limits. But what if they didn't? - World. Retrieved 18 March 2021, from https://reliefweb.int/report/world/even-cyber-wars-have-limits-what-if-they-didn-t

Rosenberg, B. (2010). Battlefield network connects allied forces in Afghanistan -- Defense Systems. Retrieved 16 December 2020, from https://defensesystems.com/articles/2010/09/02/c4isr-2-afghan-mission-network-connects-allies.aspx

Roy, R., Volz, D., & Purnell, N. (2019). U.S. Campaign Against Huawei Runs Aground in an Exploding Tech Market. Retrieved 26 June 2020, from https://www.wsj.com/articles/india-a-pivotal-internet-market-isnt-buying-u-s-campaign-against-huawei-11550762080?mod=article_inline

Rudolph, C., Creese, S., & Sharma, S. (2020). Cybersecurity in Pacific Island nations. Communications Of The ACM, 63(4), 53-54. doi: 10.1145/3378550

Russell, A. (2013). OSI: The Internet That Wasn't. Retrieved 12 May 2019, from https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt

Ryan, J. (2012). FBI Director Says Cyberthreat Will Surpass Threat From Terrorists. Retrieved 17 May 2019, from https://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/#xd_co_f=YzZiNzZhMWUtMTU4NS00YTQ2LWIxYTMtYTVjYWNhZGNjNzZm~

Saad, C., & Gosal, E. (2019). Autonomous weapons systems: how to work towards a total ban?. Retrieved 4 November 2020, from https://www.cba.org/Sections/International-Law/Articles/2019/Autonomous-weapons-systems-how-to-work-towards-a#_ftnref1

Saakashvili, E. (2021). The global rise of Internet sovereignty - Coda Story. Retrieved 13 November 2020, from https://www.codastory.com/authoritarian-tech/global-rise-internet-sovereignty/

Satariano, A. (2019). Russia Sought to Use Social Media to Influence E.U. Vote, Report Finds. Retrieved 14 September 2019, from https://www.nytimes.com/2019/06/14/business/eu-elections-russia-misinformation.html

Schmidt, M., & Perlroth, N. (2020). U.S. Charges Russian Intelligence Officers in Major Cyberattacks. Retrieved 2 March 2021, from https://www.nytimes.com/2020/10/19/us/politics/russian-intelligence-cyberattacks.html

Moe, J. (2012). Hackers took control of NASA operation - Marketplace. Retrieved 9 February 2020, from https://www.marketplace.org/2012/03/02/hackers-took-control-nasa-operation/

Scroxton, A. (2019). What will succeed the National Cyber Security Strategy?. Retrieved 19 March 2020, from https://www.computerweekly.com/news/252473088/What-will-succeed-the-National-Cyber-Security-Strategy

Seals, T. (2017). NSA: There's a New Normal on the Nation-State Front. Retrieved 2 April 2019, from https://www.infosecurity-magazine.com/news/nsa-theres-a-new-normal-nation

Sean. (2020). China and Huawei propose a new internet protocol with a built in killswitch - Gizmochina. Retrieved 16 July 2020, from https://www.gizmochina.com/2020/03/31/china-and-huawei-propose-a-new-internet-protocol-with-a-built-in-killswitch

Seebeck, L. (2019). Why the fifth domain is different | The Strategist. Retrieved 18 January 2021, from https://www.aspistrategist.org.au/why-the-fifth-domain-is-different

Tarnoff, B. (2016). How the internet was invented. Retrieved 9 February 2020, from https://www.theguardian.com/technology/2016/jul/15/how-the-internet-was-invented-1976-arpa-kahn-cerf

Seewoosurrun, S. (2016). Cyber security: Central African States adopt model cross-border laws - Platform Africa - Economic News for Emerging Market. Retrieved 15 November 2020, from https://www.platformafrica.com/2016/12/07/cyber-security/

Servon, L. (2002). *Bridging the Digital Divide Technology, Community and Public Policy* (1st ed., pp. 21-24). Massachusetts: Blackwell.

Shahwan, S. (2019). How governments can use cyber tools irresponsibly to preserve power - Atlantic Council. Retrieved 18 November 2020, from https://www.atlanticcouncil.org/blogs/new-atlanticist/how-governments-can-use-cyber-tools-irresponsibly-to-preserve-power/

Sharma, K. (2017). What happens when hackers attack chatbots. Retrieved 16 February 2020, from https://venturebeat.com/2017/05/29/what-happens-when-hackers-attack-chatbots/

Sharma, R. (2014). Coca-Cola, BT Partner to Offer Free WiFi Access from Vending Machines in South Africa. Retrieved 6 September 2020, from https://www.thefastmode.com/technology-solutions/2534-coca-cola-bt-partner-to-offer-free-wifi-access-from-vending-machines-in-south-africa

Sharma, S. (2021). Pegasus scandal shows we are living in George Orwell's 1984. Retrieved 29 July 2021, from https://theprint.in/campus-voice/pegasus-scandal-shows-we-are-living-in-george-orwells-1984/704434

Shendruk, A., Hillard, L., & Roy, D. (2020). Funding the United Nations. Retrieved 17 November 2020, from https://www.cfr.org/article/funding-united-nations-what-impact-do-us-contributions-have-un-agencies-and-programs

Sherman, J. (2019). Vietnam's Internet Control: Following in China's Footsteps?. Retrieved 2 July 2020, from https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-

footsteps/

Sheth, H. (2020). No free Wi-Fi: Google to discontinue its free Wi-Fi program for stations. Retrieved 25 February 2021, from https://www.thehindubusinessline.com/info-tech/no-free-wi-fi-google-to-discontinue-its-free-wi-fi-program-for-stations/article30849649.ece

Shieber, J. (2019). Amazon joins SpaceX, OneWeb and Facebook in the race to create space-based internet services. Retrieved 19 November 2020, from https://techcrunch.com/2019/04/04/amazon-joins-spacex-oneweb-and-facebook-in-the-race-to-create-space-based-internet-services/

Singh, A. (2021). Disinfo lab's support for India makes TWITTER lose its BUTTONS, removes its blue badge in a retaliatory move. Retrieved August 10, 2021, from https://tfipost.com/2021/08/disinfo-labs-support-for-india-makes-twitter-lose-its-buttons-removes-its-blue-badge-in-a-retaliatory-move/

Singh, M. (2020). Virtual SIM cards a new cause of concern for Army in Jammu and Kashmir. Retrieved 28 December 2020, from https://www.newindianexpress.com/thesundaystandard/2020/oct/25/virtual-sim-cards-a-new-cause-of-concernfor-army-in-jammu-and-kashmir-2214700.html

Smith, A. (2021). Microsoft launches new APAC cybersecurity council. Retrieved 3 June 2021, from https://www.technologyrecord.com/Article/microsoft-launches-new-apac-cybersecurity-council-124240

Smith, B. (2018). 34 companies stand up for cybersecurity with a tech accord - Microsoft On the Issues. Retrieved 20 September 2020, from https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/

Solomon, S. (2019). Israeli airports fend off 3 million attempted attacks a day, cyber head says. Retrieved 16 November 2020, from https://www.timesofisrael.com/israeli-airports-fend-off-3-million-attempted-attacks-a-day-cyber-head-says

Solum, L. (2008). Models of Internet Governance. Retrieved 17 December 2020, from https://www.researchgate.net/publication/228257049_Models_of_Internet_Governance

Somaiya, R. (2010). Hundreds of WikiLeaks Mirror Sites Appear. Retrieved 14 March 2019, from https://www.nytimes.com/2010/12/06/world/europe/06wiki.html

Souter, D. (2021). Inside the Digital SOCIETY: Children's rights in the digital society. Retrieved May 03, 2021, from https://blogs.lse.ac.uk/medialse/2021/04/12/inside-the-digital-society-

childrens-rights-in-the-digital-society/

South Atlantic Inter Link Connecting Cameroon to Brazil Fully Connected. (2018). Retrieved 3 May 2019, from https://newswire.telecomramblings.com/2018/09/south-atlantic-inter-link-connecting-cameroon-brazil-fully-connected

Stadnik, I. (2017). What Is an International Cybersecurity Regime and How We Can Achieve It?. Masaryk University Journal Of Law And Technology, 11(1), 129-154. doi: 10.5817/mujlt2017-1-7

Starosielski, N. (2015). *The undersea network* (pp. 240-280). North Carolina: Duke University Press.

Stashwick, S. (2018). New Chinese Ocean Network Collecting Data to Target Submarines. Retrieved 16 February 2020, from https://thediplomat.com/2018/01/new-chinese-ocean-network-collecting-data-to-target-submarines

Stein, J. (2016). What 20,000 pages of hacked WikiLeaks emails teach us about Hillary Clinton. Retrieved 6 February 2020, from https://www.vox.com/policy-and-politics/2016/10/20/13308108/wikileaks-podesta-hillary-clinton

Stewart, P. (2010). Spies behind 2008 cyber attack, U.S. official says. Retrieved 15 September 2020, from https://www.reuters.com/article/us-usa-cyber-attack-idUSTRE67P00X20100826

Stewart, P. (2010). Spies behind 2008 cyber attack, U.S. official says. Retrieved 4 November 2020, from https://www.reuters.com/article/us-usa-cyber-attack-idUSTRE67P00X20100826

Stifel, M. (2019). The Importance of Civil Society in the World of Cybersecurity. Retrieved 7 May 2020, from https://www.globalcyberalliance.org/the-importance-of-civil-society-in-the-world-of-cybersecurity/

Stringer, D., & Lee, H. (2021). Why Global Power Grids Are Still Vulnerable to Cyber Attacks. Retrieved 10 March 2021, from https://www.bloomberg.com/news/articles/2021-03-03/why-global-power-grids-are-still-so-vulnerable-to-cyber-attacks

Stronski, P., & Ng, N. (2018). Cooperation and Competition: Russia and China in Central Asia, the Russian Far East, and the Arctic. Retrieved 12 July 2020, from https://carnegieendowment.org/2018/02/28/cooperation-and-competition-russia-and-china-in-central-asia-russian-far-east-and-arctic-pub-75673

Suwanprateep, D. (2020). Thailand - Data Protection Overview. Retrieved 31 December 2020, from https://www.dataguidance.com/notes/thailand-data-protection-overview

Synovitz, R., & Mitevska, M. (2020). 'Fake News' Sites In North Macedonia Pose As American Conservatives Ahead Of U.S. Election. Retrieved 4 December 2020, from https://www.rferl.org/a/macedonia-fake-news-sites-us-election-conservatives/30906884.html

Tamarkin, E. (2015). The AU's cybercrime response A positive start, but substantial challenges ahead. Retrieved 11 July 2020, from https://media.africaportal.org/documents/PolBrief73_cybercrime.pdf

Tamon, M. (2015). IPv4 Exhaustion, 5 Implications for Africa Running out Last. Retrieved 17 February 2020, from https://circleid.com/posts/20150713_ipv4_exhaustion_5_implications_for_africa_running_out_last

Tang, F. (2020). China central bank stresses central role in sovereign digital currency. Retrieved 18 November 2020, from https://www.scmp.com/economy/global-economy/article/3101657/chinas-central-bank-stresses-its-central-role-new-sovereign

Tapper, J. (2015). Obama administration spied on German media, government - CNNPolitics. Retrieved 21 September 2020, from https://edition.cnn.com/2015/07/03/politics/germany-media-spying-obama-administration/index.html

Taranovich, S. (2018). Planet Analog - How do electronic systems react at high altitudes?. Retrieved 14 October 2020, from https://www.planetanalog.com/how-do-electronic-systems-react-at-high-altitudes

Abdullin, A., Davletgildeev, R., & Kostin, S. (2020). Organization for Defense and Cooperation in the Field of Collective Cyber Security in Europe. Retrieved 2 December 2020, from https://www.redalyc.org/journal/279/27965040013/html/

Taylor, E., & Hoffmann, S. (2019). How is the EU–US Relationship on Internet Governance Working?. Retrieved 19 July 2020, from https://www.chathamhouse.org/2019/11/eu-us-relations-internet-governance-0/3-how-eu-us-relationship-internet-governance-working

Tharoor, I. (2021). The 'free world' keeps shrinking. Retrieved 17 March 2021, from https://www.washingtonpost.com/world/2021/03/03/democracy-declining-freedom-house-report/

Thierer, A. (2012). 15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm. Retrieved 18 January 2021, from https://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm/?sh=6d3837507170

Tidy, J. (2021). Gang behind huge cyber-attack demands $70m in Bitcoin. Retrieved 6 July 2021, from https://www.bbc.com/news/technology-57719820

Tladi, M. (2021). What Is Logic Bomb Malware and How Can You Prevent It?. Retrieved 25 April 2021, from https://www.makeuseof.com/what-is-logic-bomb-malware-and-how-can-you-prevent-it/

Tredger, C. (2020). China Telecom Global links with Angola Cables to extend global reach. Retrieved 7 October 2020, from https://itweb.africa/content/nWJadvbeXolqbjO1

Treed ·, 2020, A. [@disastrid]. (2020, March 12). *I love switching between VPNs and seeing how media outlets tailor their headlines depending on who they think the audience* [Tweet]. Twitter. https://twitter.com/disastrid/status/1238098196183777282?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1238098196183777282&ref_url=https%3A%2F%2Fpublish.twitter.com%2F%3Fquery%3Dhttps%253A%252F%252Ftwitter.com%252Fdisastrid%252Fstatus%252F1238098196183777282%26widget%3DTweet

Tsz Yan, Y. (2019). Smart Cities or Surveillance? Huawei in Central Asia. Retrieved 6 May 2020, from https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/

Tung, L. (2021). Ransomware: We need a new strategy to tackle 'exponential' growth, says Interpol | ZDNet. Retrieved 20 July 2021, from https://www.zdnet.com/article/ransomware-we-need-a-new-strategy-to-tackle-exponential-growth-says-interpol/

Tunji, S. (2021). World Bank, partners create new global fund for cybersecurity. Retrieved 17 August 2021, from https://punchng.com/world-bank-partners-create-new-global-fund-for-cybersecurity/

Vacarelu, F. (2018). Transforming Diplomacy with Emerging Technologies and Approaches • UN Global Pulse. Retrieved 17 May 2019, from https://www.unglobalpulse.org/2018/07/transforming-diplomacy-with-emerging-technologies-and-approaches

Vailshery, L. (2021). Number of connected devices worldwide 2030 | Statista. Retrieved 8 February 2021, from https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology

Verton, D. (2003). *Black Ice: The invisible threat of cyber terrorism* (pp. 135-164). Madrid: McGraw-Hill.

Vincent, J. (2017). Putin says the nation that leads in AI ‘will be the ruler of the world’.

Retrieved 18 September 2020, from https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world

Vinuesa, R., Azizpour, H., Leite, I., Balaam, M., Dignum, V., & Domisch, S. et al. (2020). The role of artificial intelligence in achieving the Sustainable Development Goals. Nature Communications, 11(1). doi: 10.1038/s41467-019-14108-y

von Solms, S. (2015). A maturity model for part of the African Union Convention on Cyber Security. 2015 Science And Information Conference (SAI). doi: 10.1109/sai.2015.7237313

Vonau, M. (2020). Google has removed almost all Cheetah Mobile apps from the Play Store. Retrieved 5 November 2020, from https://www.androidpolice.com/2020/02/27/cheetah-mobile-apps-disappeared-play-store

Walker, S. (2019). CYBER-INSECURITIES? A guide to the UN cybercrime debate. Retrieved 1 May 2021, from https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf

Walt, S. (1985). Alliance Formation and the Balance of World Power. *International Security*, *9*(4), 3-43. doi: 10.2307/2538540

Wamala, F. (2011). THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE (pp. 13-23). Geneva, Geneva: International Telecommunication Union (ITU).

Wang, C. (2021). China slaps Alibaba with $2.8 billion fine in anti-monopoly probe. Retrieved 10 April 2021, from https://www.cnbc.com/2021/04/09/china-fines-alibaba-in-anti-monopoly-probe.html

Ward, A. (2020). China and Australia are in a nasty diplomatic spat over a fake tweet — and real war crimes. Retrieved 3 February 2021, from https://www.vox.com/22021226/australia-china-afghanistan-tweet

Waterson, J. (2019). Facebook refuses to delete fake Pelosi video spread by Trump supporters. Retrieved 2 December 2019, from https://www.theguardian.com/technology/2019/may/24/facebook-leaves-fake-nancy-pelosi-video-on-site

Weinberger, S. (2010). What Is SIPRNet?. Retrieved 15 November 2020, from https://www.popularmechanics.com/technology/security/how-to/a6426/what-is-siprnet-and-wikileaks-4085507

Wendt, A. (1992). Anarchy is what states make of it: the social construction of power

politics. *International Organization*, *46*(2), 391-425. Retrieved from http://www.jstor.org/stable/2706858

Weston, G. (2014). CSEC used airport Wi-Fi to track Canadian travellers: Snowden documents | CBC News. Retrieved 10 September 2020, from https://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881

Wickrematunge, R. (2018). Building resilience: Responding to cyber-bullying in Sri Lanka - Firstpost. Retrieved 13 November 2020, from https://www.firstpost.com/long-reads/building-resilience-responding-to-cyber-bullying-in-sri-lanka-4776511.html

Wildon, J. (2020). WhatsApp security flaw: Over 60,000 groups still accessible online | DW. Retrieved 2 November 2020, from https://www.dw.com/en/whatsapp-security-flaw-over-60000-groups-still-accessible-online/a-52543414

Williams, M. (2010). All Eyes Are on Los Angeles as City Deploys Cloud-Based E-Mail. Retrieved 23 April 2019, from https://www.govtech.com/pcio/All-Eyes-Are-on-Los-Angeles.html

Williams, M. (2015). A peek inside North Korea's intranet. Retrieved 17 October 2019, from https://www.northkoreatech.org/2015/07/06/a-peek-inside-north-koreas-intranet

Williscroft, R. (2019). *Operation Ivy Bells* (2nd ed., pp. 150-160). Alabama: Fresh Ink Group.

Willmer, G. (2016). How NGOs can work with big Internet firms to overcome the digital divide. Retrieved 15 July 2019, from https://www.devex.com/news/how-ngos-can-work-with-big-internet-firms-to-overcome-the-digital-divide-87493

Wilson, S., Hamilton, D., & Stallbaum, S. (2020). The Unaddressed Gap in Cybersecurity: Human Performance. Retrieved 19 January 2021, from https://sloanreview.mit.edu/article/the-unaddressed-gap-in-cybersecurity-human-performance/

Winck, B. (2020). Major tech firms have a 'fundamental responsibility' to protect US elections, Microsoft's president says. Retrieved 9 January 2021, from https://www.businessinsider.in/stock-market/news/major-tech-firms-have-a-fundamental-responsibility-to-protect-us-elections-microsofts-president-says/articleshow/74165224.cms

Winther, M. (2006).Tier 1 ISPs : What They Are and Why They Are Important. Retrieved 15 April 2020, from https://www.gin.ntt.net/wp-content/uploads/2020/01/IDC_Tier1_ISPs.pdf

Wong, A. (2018). The Kaspersky Global Transparency Initiative Explained! | Tech ARP. Retrieved 14 October 2020, from https://www.techarp.com/internet/kaspersky-global-

transparency-initiative/

Woo, S., & Hinshaw, D. (2021). WSJ News Exclusive | U.S. Fight Against Chinese 5G Efforts Shifts From Threats to Incentives. Retrieved 17 June 2021, from https://www.wsj.com/articles/u-s-fight-against-chinese-5g-efforts-shifts-from-threats-to-incentives-11623663252

Woodhams, S. (2019). Huawei, Africa and the global reach of surveillance technology | DW. Retrieved 1 July 2020, from https://www.dw.com/en/huawei-africa-and-the-global-reach-of-surveillance-technology/a-50398869

Xu, Y. (2016). Internet Censorship Around the World. Retrieved 21 November 2020, from https://www.thousandeyes.com/blog/internet-censorship-around-the-world

Yeo, P. (2021). Opinion: How should the US respond to China at the UN?. Retrieved 25 July 2021, from https://www.devex.com/news/opinion-how-should-the-us-respond-to-china-at-the-un-100378

Yeung, R. (2020). *China's Trump Card :Cryptocurrency and Its Game-Changing Role in Sino-US Trade* (1st ed., pp. 252-254). New Jersey: Wiley.

Yunker, J. (2011). A URL in Any Language: Getting to know the next generation of URLs | UX Magazine. Retrieved 16 September 2019, from https://uxmag.com/articles/a-url-in-any-language

Zaki, Y. (2018). 11 dangerous games on the internet that could kill or seriously injure. Retrieved 23 July 2019, from https://gulfnews.com/lifestyle/11-dangerous-games-on-the-internet-that-could-kill-or-seriously-injure-1.2252866

Zeevi, Y. (2020). Facebook introduces Discover: Exploring new ways to support connectivity. Retrieved 1 August 2020, from https://tech.fb.com/discover/

Zetter, K. (2015). A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever. Retrieved 17 December 2020, from https://www.wired.com/2015/01/german-steel-mill-hack-destruction

Zimmermann, H. (1980). OSI Reference Model--The ISO Model of Architecture for Open Systems Interconnection. IEEE Transactions On Communications, 28(4), 425-432. doi: 10.1109/tcom.1980.1094702