

**THE EUROPEAN UNION AND THE UNITED
STATES APPROACH TO CYBER SECURITY:
A COMPARATIVE STUDY, 2001-2013**

*Thesis submitted to Jawaharlal Nehru University
for the award of the degree of*

DOCTOR OF PHILOSOPHY

JAYADEV PARIDA



**CENTRE FOR EUROPEAN STUDIES
SCHOOL OF INTERNATIONAL STUDIES
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI - 110067
2019**

Date: 22.01.2019

DECLARATION

I declare that the thesis entitled "The European Union and the United States Approach to Cyber Security: A Comparative Study, 2001-2013" submitted by me for the award of the degree of DOCTOR OF PHILOSOPHY of Jawaharlal Nehru University, is my own work. This thesis has not been submitted for any other degree of this University or any other university.


Jayadev Parida

Mr. Jayadev Parida


CERTIFICATE

We recommend that this thesis be placed before the examiners for evaluation.

Ummu Salma Bava
Prof. Ummu Salma Bava
(Chairperson, CES)


Prof. Ummu Salma Bava
Chairperson
Centre for European Studies
School of International Studies
Jawaharlal Nehru University
New Delhi-110067, India

Ummu Salma Bava
Prof. Ummu Salma Bava
(Supervisor)


Prof. Ummu Salma Bava
Chairperson
Centre for European Studies
School of International Studies
Jawaharlal Nehru University
New Delhi-110067, India

Date:

DECLARATION

I declare that the thesis entitled “**The European Union and the United States Approach to Cyber Security: A Comparative Study, 2001-2013**” submitted by me for the award of the degree of **DOCTOR OF PHILOSOPHY** of Jawaharlal Nehru University, is my own work. This thesis has not been submitted for any other degree of this University or any other university.

Mr. Jayadev Parida

CERTIFICATE

We recommend that this thesis be placed before the examiners for evaluation.

Prof. Ummu Salma Bava
(Chairperson, CES)

Prof. Ummu Salma Bava
(Supervisor)

Dedicated To,

Four Women

My Grandmother, Mother, Ph.D. Supervisor and my Wife

Acknowledgements

A good 'Guru' can inspire hope, ignite the hidden knowledge and encourage a love of research. No piece of research can be undertaken in isolation. As I completed my work of Ph.D. thesis, first and foremost I owe my deepest gratitude to my supervisor **Prof. Ummu Salma Bava** for her continuous moral support and enduring guidance in different research matters during my M.Phil. and starting from my discussion of the idea of synopsis, research structure and formation of this work and other academic endeavours as well as non-academic suggestions. Her immense patience, guidance, motivation, inspiring words and in-depth knowledge in research methodology, European studies, international relations and security studies have enlightened me exceptionally to accomplish this work. Moreover, she also taught me the worth of hard work, discipline, dedication, management and value of time in life.

I also express my profound thanks to all faculty members of the Centre for European Studies, Prof. Rajendra K. Jain, Prof. Gulshan Sachdeva, Prof. Bhaswati Sarkar, Dr. Sheetal Sharma and Dr. Teiborlang T. Kharsyntiew. I also express my heartiest thanks to my research committee members Prof. Srabani Roy Choudhury and Prof. Jayati Srivastava. I am thankful to the staffs (special thanks to Sheeshpal Ji) of Centre for European Studies (CES), JNU, and Rembrandt Library of the Centre for European Studies which helped a lot in providing specific books for my research. I would also like to express my thanks to the Dr. B. R. Ambedkar Central Library for large online resources which helped me to complete this work.

I also extend my gratefulness to Dr. Ingo Peters, Otto-Suhr-Institute for Political Science Center for Transnational Relations, Freie Universität Berlin, for hosting me at the Freie Universität Berlin to complete my research work as well as guiding me to enrich my academic credentials. I am also thankful to Dr. Myriam Dunn Cavelty and Dr. Robert Scott Dewar, Center for Security Studies, ETH Zurich; Dr. Roxana Radu, Geneva Internet Platform, Geneva; Prof. Dr. Volker Roth, Institute of Computer Science, FU Berlin; Dr. Sandro Gaycken and Ms. Isabel Skierka, the Digital Society Institute at ESMT, Berlin; Dr. Ben Wagner, Dr. Annegret Bendiek and Dr. Matthias Schulze, SWP (German Institute for International and Security Affairs), Berlin; Dr. Julia Pohle, WZB, Berlin; Dr. Hannes Ebert, German Institute of Global and Area

Studies, Berlin; Mr. Alexander Klimburg, the Hague Centre for Strategic Studies, The Hague; Mr. Mirko Hohmann, Global Public Policy Institute, Berlin; Ms. Gail Kent, Facebook, UK; Mr. Ahlefeldt Johanne, PKGr, SPD, Berlin, for their resourcefulness and hospitality made my field work in Germany immensely productive.

I also express my heartiest thanks to the Konrad-Adenauer-Stiftung, Berlin, for scholarship that to support my very productive research stay in Berlin (November 2016-April 2017). I also thank Mr. Amos Helms, Mr. Dear Henri and KAS India office staffs for their support. I would like to thank Indo-German Partnership Project, co-funded by the DAAD and the UGC and Project Director, Prof. Ummu Salma Bava for the financial support to my research trip to Berlin, Germany (May 2017-July 2017). I also express my gratitude to the Indian Council of Social Science Research, New Delhi for awarding a Doctoral Fellowship and the University Grants Commission for giving me fellowship that helped in my research work.

I also extend my thanks to Dr. Samir Saran, Mr. Arun Mohan Sukumar and Brig. R K Sharma, Observer Research Foundation, for giving me the opportunity to gain both professional and research experience on cyber security issues. I would also like to thank Prof. Satish Kumar for giving me the first opportunity to work at FNSR, New Delhi.

I am extremely indebted to my grandparents, father, mother, my younger brother Appu, Big B Himhansu, for standing with me throughout my life. This is the result of their immense support and care that I have reached so far, words cannot substitute my feelings towards them. I would like to thank my second family Nana, Maa, Babuni Kakei, Khudi, Sanju nani, Udyanath piusa, Maju nani, Rudra piusa, Ranju nani and Pitabas piusa, Mamuni, Bapi bhaina, Pinka bhaina, Kanhu, Jitun, Jipun, Muni, and Badi for believing on me.

I also convey my heartfelt thanks to my wife Bineeta for her continuous moral support, encouragement, belief, sacrifice and for standing with me as a true friend, philosopher and partner to complete this work.

Last but not the least, my heartiest thanks to my friends – Bailochan, , Rajnish, Chandan, Arvind, Rakesh, Niraj, Mandeep, Deva, Vidya, Subhendra, Mathew and Joerg Wolf. I would like to express my special thanks to Deepak bhai, Binayak bhai, Mohan, Vineet, Manas, Subrat, Jogendra, Tilka, Rishu, Vaibhav, Pavul Raj and Shashi for their affectionate support in JNU. I would also like to express my thanks to Sonam Di for her sisterly affection and help during my work. I would like thank my classmates for the time spent with them during the research work. I also want to thank Anee, Ankita, Chhua, Chagulikaka, Dugu Didi, Lopa, Lilly, and Nirmal Bhai, Bhauja, Lata Dei, Kabi didi, Babuli bhai, Rohit and Auysh for their direct and indirect support and encouragement during the work.

Above all, I thank the Almighty for His kindness and blessings for enabling me to complete this work in time.

New Delhi

Mr. Jayadev Parida

Date: 22.01.2019

CONTENTS

	Page No.
<i>List of Figures and Tables</i>	<i>i-ii</i>
<i>List of Acronyms</i>	<i>iii-vii</i>
<i>Preface</i>	<i>viii-x</i>
CHAPTER 1: INTRODUCTION	1-33
Background: Situating Security in International Politics	
Traditional Threats to Security	
Non-Traditional Threats to Security	
Emerging Security Landscape and Actor Matrix	
The EU's Actorness and Security Dynamics in Europe	
The US and the Changing Security Landscape	
Security in a Digital Age	
<i>Data as Risk and new Threat</i>	
<i>Data as Business opportunity</i>	
<i>Data as a Regulated Area</i>	
The EU and Cyber Threats	
The US and Cyber Threats	
The EU and US: Cyber Preparedness and the Issue of Data Protection	
Research Framework	
CHAPTER 2: CYBERSPACE: TECHNOLOGY, STATE AND SECURITY	34-61
Introduction	
Territory, Technology and Transformation	
Evolution of the Internet and Impact on State, Economy and Society	
Cyberspace - Data: As a Multidimensional Factor	
Cyberspace: A Challenge to Sovereignty	
Cyber Threats and Growing Vulnerabilities	
Cyberspace: Security and Governance	
Conclusion	
CHAPTER 3: THE EUROPEAN UNION'S APPROACH TO CYBER SECURITY	62-105
Introduction	
The Emerging Security Landscape of Europe from, 1990-2001	
The Evolution of the European Union as a Security Actor	
The European Union and Cyberspace: Digital Connectivity, Vulnerability and Regulation	
The Cyber Attack on Estonia, 2007	
The European Union and Cyber Threats: Issue of Data Protection	
The European Union's Approach to Cyber Security	
<i>Cyber Security Strategy of the Union, 2013</i>	
Conclusion	

**CHAPTER 4: THE UNITED STATES APPROACH TO
CYBER SECURITY**

106-137

Introduction

The United States and Emerging Security Landscape, 1990-2001

The 9/11 and Impact on American Security: Rise of Non-Traditional Threats

The United States and Cyberspace: Digital Connectivity,

Vulnerability and Regulation

The United States and Cyber Threats: Issue of Data Protection

The United States Approach to Cyber Security

The US and Third Country Cyber Relations

US and Digital Privacy

Conclusion

**CHAPTER 5: THE EUROPEAN UNION AND THE UNITED STATES
APPROACH TO CYBER SECURITY**

138-185

Introduction

The EU's Cyber-preparedness

The US's Cyber-preparedness

The European Union's Approach to Data Protection

The United State's Approach to Data Protection

Convergence and Divergence in the EU and the US Data Protection
Approaches

Convergence and Divergence: The EU and the US Data Protection Policy

Conclusion

CHAPTER 6: CONCLUSION

186-197

The European Union and the United States Approach to Data Protection:
Divergence versus Convergence

Convergence in Data Protection Approach

Divergence in Data Protection Approach

Summary of the Research Findings

References

198-246

Annexure:

Annex 1: List of Experts Interviewed and Institutions visited during the Field
Work from 01 November 2016 – 19 July 2017

LIST OF FIGURES AND TABLES

Figures

Figure 2.1: Complex Connectivity and overarching influence of technology on State, Business and Society	35
Figure 2.2: Evolution of Internet	41
Figure 2.3 the complex interface of science, technology and national security	43
Figure 2.4: Offensive Cyber Capabilities	44
Figure 2.5: Complex Cyber Interconnectedness	53
Figure 3.1: Internet Users in the EU – June 2017	80
Figure 3.2: European Union Internet Penetration - June 2017	80
Figure 3.3: European Union – EU 27 (and UK) Top 10 Internet Countries – June 2017	81
Figure 3.4: Individuals - frequency of internet use	82
Figure 3.5: Ranking of the ten European Union countries with the highest malware encounter rates as of January 2017	83
Figure 3.6: Attack Distribution Data for 2016 and 2017	87
Figure 3.7: Data Created in every 60 seconds in 2016	90
Figure 3.8: Cyber Security, Cybercrime and Data Protection	91
Figure 3.9: Coordination between NIS competent authorities/CERTs, law enforcement and defence	100
Figure 4.1: Cyber security incident reports by federal agencies in the United States	121
Figure 4.2: Cost of Cyber Crime	121
Figure 4.3: Digital Economy Real Value Added and Total Economy Real Gross Domestic Product: Percentage from Previous Year	123
Figure 4.4: The US: Significant Cyber Incidents	124
Figure 4.5: US and Data Creation in every Minute, 2018	126
Figure 5.1: US Cyber Structure	149

Tables

Table 2.1: List of Major Cyber Attacks 1988-2018	49
Table 2.2: Cyber Threats Structure	54
Table 3.1: The EU and Security Actorness	67
Table 3.2: EU Member States and US's Percentage of Individuals using the Internet	78
Table 3.3: Evolution of the EU's Cybersecurity Approach	92
Table 3.4: Evolution of the EU's Data Protection Regime	102
Table 4.1: The US as a Security Actor	108
Table 4.2: US's Percentage of Individuals using the Internet	118
Table 4.3: Evolution of the US Approach to Cyber Security	128
Table 4.4: The US and Data Protection	135
Table 5.1: Data Protection Policy Convergence and Divergence between the EU and the US	166

List of Abbreviations and Acronyms

AFSJ	Area of Freedom, Security and Justice
ARPA	Advance Research Projects Agency
ARPANET	Advance Research Projects Agency Network
B2C	Business to Consumer
BEA	Bureau of Economic Analysis
BiZ	Bosnia and Herzegovina
C*CAT	Cyber-Crime Advisory Tool
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CAGR	Compounded Annual Growth rate
CEE/S	Central Eastern European States
CEO	Chief Executive Officer
CERN	European Organisation for Nuclear Research
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIA	Central Intelligence Agency
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CFSP	Common Foreign and Security Policy
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CSIS	Center for Strategic and International Studies
CSSG	Cyber Security Strategy for Germany
CSSSEU	Cyber Security Strategy of the European Union
CSSSUK	Cyber Security Strategy of United Kingdom
CTOSE	the EU Cyber Tools On-Line Search for Evidence
CYBERCOM	Cyber Command
DAE	Digital Agenda for Europe
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DDoSA	Distributed Denial of Service Attack
DoS attack	Denial of Service Attack
DHS	Department of Homeland Security

DNS	Domain Name System
DoD	Department of Defense
DoDSOC	Department of Defense Strategy for Operating in Cyberspace
DRC	Democratic Republic of Congo
DSCI	Data Security Council of India
DSPs	Digital Service Providers
EC	European Commission
EC	European Community
EC3	European Cybercrime Centre
ECHR	European Convention on Human Rights
ECPA	Electronic Communications Privacy Act
ECSC	European Coal and Steel Community
ECSM	European Cyber Security Month
ECSS	Estonia Cyber Security Strategy
ECU	European Currency Unit
ECJ/ CJEU	European Court of Justice
EEC	European Economic Community
EEAS	European External Action Service
EFTA	European Free Trade Area
ENISA	European Network and Information Security Agency
ENP	European Neighbourhood Policy
EP	European Parliament
EP3R	European Public-Private Partnership for Resilience
EPC	European Political Community
EPIC	Electronic Privacy Information Center
ESDP	European Security and Defence Policy
ESS	European Security Strategy
EU	European Union
EU CERT	Computer Emergency Response Team for the EU
EUCTS	European Union Counter Terrorism Strategy
EUGS	European Union Global Strategy
EUISS	EU Internal Security Strategy
EUMS	European Union Member States
EURid	European Registry for Internet Domains

EUROPOL	European Police Office
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FWPDNC	The French White Paper on Defence and National Security
FTC	Federal Trade Commission
G8	Group of Eight
GB	Gigabytes
GCHQ	Government Communications Headquarters
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
gTLDs	Generic Top Level Domains
HTCC	High Tech Crime Centre
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IGF	Internet Governance Forum
IMPACT	International Multilateral Partnership Against Cyber Threats
IP	Internet protocol
IP address	Internet protocol address
IPE	International Political Economy
IR	International Relations
ISDSS	Information Systems Defence and Security Strategy of France
IST	Information Society Technologies
IT	Information Technology
ITU	International Telecommunications Union
JHA	Justice and Home Affairs
JRC	The European Commission's Joint Research Centre
LEA	Law Enforcement Agency
MAT	Mobile Assistance Team
MIT	Massachusetts Institute of Technology
MLAT	Mutual Legal Assistance Treaty
MS	Member States
NASA	National Aeronautics Space and Administrations

NATO	North Atlantic Treaty Organisation
NCSAs	National Cyber Security Agencies
NGO	Non-governmental Organisations
NIS	Network and Information Security
NSCIP	National Strategy for Critical Infrastructure Protection
NSA	National Security Agency
NSISS	National Strategy for Information Sharing and Safeguarding
NSS	National Security Strategy
NSSC	National Strategy to Secure Cyberspace
NTIA	National Telecommunications and Information Administration
NTS	Non-traditional Security
NTT	Non-traditional Threats
OECD	Organisation for Economic Co-operation and Development
OES	Operators of Essential Services
OPM	Office of Personnel Management
PII	Personally Identifiable Information
P3R	Prevent Protect Pursue and Respond
P-5	Five Permanent Members
PC	Personal Computer
PCS	Personal Communications Services
PDD	Presidential Decision Directive
PESCO	Permanent Structured Cooperation
PPP/P3	Public Private Partnership
SCA	Stored Communications Act
SCADA	Supervisory Control and Data Acquisition
SGDSN	General Secretariat for Defence and National Security
SID	Safer Internet Day
SIP	Safer Internet Programme
TLDs	Top Level Domains
TTIP	Transatlantic Trade and Investment Partnership
UKNSS	United Kingdom National Security Strategy
UN	United Nations
UNESCO	UN Educational Scientific and Cultural Organisation
UNODC	United Nation Office on Drugs and Crimes

UN-GGE	UN Group of Governmental Experts on Developments
US/USA	United States/ United States of America
USB	Universal Serial Bus
USNSS	United States National Security Strategy
USSR	Union of Soviet Socialist Republics
WCIT	World Conference on International Telecommunications
WMD	Weapons of Mass Destruction
WMDisruption	Weapon of Mass Disruption
WSIS	World Summit on the Information Society
WWW	World Wide Web
XML	Extensible Markup Language

PREFACE

In the Westphalian order, traditional threats impact the essential elements of modern state security- sovereignty, territorial integrity and autonomy. During the Cold War the nature of threats was identifiable, predictable and a action could be reciprocated. In the post-Cold War period, the rise in intrastate conflicts, non-traditional threats have challenged many aspects of state security. The dramatic 9/11 terrorist attacks on the US highlighted the unpredictability and vulnerability associated with the non traditional threats. The increased role of the non state actor further added to the security challenges to the changing security landscape.

This expansion in the security vocabulary and the growing unpredictability has multiplied the impact of non-traditional threats on the political, economic, security, social and individual level. In addition, the rapid adoption of information communication technologies (ICT) such as the Internet and computer technologies in different aspects of everyday life has further enhanced the impact of non-traditional threats to security. The technological revolutions – ICT and the internet are changing the power equation between individual and state, within the states and between states, creating a different kind of a technological divide. For example the Guttenberg Press, steam engine, gun powder have transformed the printing industry, travel, and conduct warfare. In other words, revolutions and innovation in science (research and development) and technological advancement have significantly influenced on politics, economics and security of the state, businesses and society.

The Internet and cyber technology which brings in opportunities to drive state and economic growth also brings in new vulnerabilities, as fifth domain has yet not been fully secured. Anonymity and inability to locate the origin of a attack in the cyber domain makes it a part of non-traditional threats due to the unpredictability and vulnerability. For example, an unknown individual from an unknown place empowered with cyber technologies today has the potential to bring down the most powerful country of the world by writing and releasing malicious software into the cyberspace. Given that digital economy has grown worldwide and internet has linked people, businesses and states into a tight network of connections, cyber threats pose unprecedented cost at the political, financial and personal level.

Given that the cyberspace transcends geographical limitations, different actors have responded in multiple ways to the opportunities and challenges in the fifth domain, it is to be noted that – land, water, air and space are other four domains and the cyberspace is the new fifth domain. With the arrival of the information age, the EU approach was confined to provide widespread affordable access to the information infrastructure, products and reliable services, over a secure, easy-to-use-technologies and high-end telecommunications networks to its citizens. In addition, the Union also had to respond to the cyber security risks which posed a new threat to citizen business and the political structure. The Union aimed to implement a coherent regulatory structure, a favourable business environment, and pushed to expand the digital economy. However, in the post-Estonian cyber attack in 2007, the EU was confronted with cyber security challenges and thus, enhanced its cyber security actorness by framing strategies and norms to address the new cyber threats. The EU adopted a comprehensive cyber security strategy in February 2013 that proposed harmonisation of three sectors – infrastructure (EU and national level), law enforcement (both in national and EU level) defence (national and EU level). Moreover, the adoption of the Network and Information Security Directive in 2016, cyber-diplomacy tool box mechanisms 2017, Permanent Structured Cooperation 2018 and Digital Agenda for Europe have been transforming the EU as a digital union to play a decisive role in global cyber security and diplomacy.

The US conceptualised the Internet through the Department of Defense as a disruptive component to military doctrine as well as an instrument for national security. The launch of the Soviet Sputnik and the Cuban Missile crisis were two significant historical events that pushed for revolution in military affairs of the US. It is in this backdrop, information security has been considered as the core to national security issues in the US strategic thinking. With the growth of the cyber domain in America, the US national security strategies incorporated cyber security from the Bush administration to the present.

Although, both the EU and the US use similar approaches in cyber preparedness and in enhancing their cyber security capabilities, but on the issue of data protection both convergence and divergence can be seen in their policy approaches. The EU pursues a

regulatory and unified approach to data protection and considers data as a core part of individual privacy. On the other hand, the US which lacks a unified regulation, perceives data protection issues through the prism of national security thereby privileging the state and not the individual, which significantly undermines the individual privacy both in physical and digital world.

In order to examine how the EU and the US approach cyber security and the issue of data protection the thesis, examines the changing nature of security and distinction traditional and non-traditional threats in the global security landscape. Furthermore, it analyses how security issues have expanded since the end of Cold War till the 9/11 attacks and thereafter, especially drawing attention to the impact of technology and rise of cyberspace and cyber security. There after the thesis describes the nature of the cyberspace and then explains how revolutions in science and technology influenced the national security and how various issues in the cyberspace are challenging businesses, individual, society, state and security. After that, the thesis explores the evolution of the EU as a security actor in the global security landscape and the EU's mechanism, policies and programmes to address the issues related to cyber security and freedom of expression and privacy especially with respect to data protection. Furthermore the thesis situates the US's as security actor and analyses response to non-traditional threats in the global security landscape and the US's mechanism, policies and programmes to respond to the issues of cyber security and how national security agenda played a decisive role in the context of individual privacy and data protection. The thesis analyses the EU and the US approaches to cyber security, and examined the convergence and divergence in their approaches to data protection. The concluding chapter presents the finding of the research and also draws attention to the latest developments at the EU and the US level, which have implications for cyber security both at regional and global level.

CHAPTER 1

INTRODUCTION

“Just as modernization dissolved the structure of feudal society in the nineteenth century and produced the industrial society, modernization today is dissolving industrial society and modernity is coming into being”

(Ulrich Beck 1992)

BACKGROUND: SITUATING SECURITY IN INTERNATIONAL POLITICS

Cyber technologies have created a new and unique world order that has animated with abundant opportunities, seamless connectivity, and ubiquitous mobility of ideas that impact the knowledge, information, power, and economy. As good and evil coexist, similarly the cyber world is also a source of asymmetric security threats to the nation states, society, business corporations and Individuals data. In a networked world, security cannot be seen merely as a binary and the world needs a cyberspace governance framework which can regulate and oversee that the core values of cyberspace - secure, neutral, open and accessible to all and not compromised.

A secure cyberspace will bring openness to the state, businesses and social, political, cultural, ideational and economic engagements. These open engagements would translate traditional values of human relations into a global chain system. And this chain system would create a network of world order wherein nation states could trade, manipulate with diplomatic abilities, manoeuvre with digital and technological capabilities, or engage to demonstrate their cyber power. All these could be only possible through the custody of data. Metaphorically, if cyberspace is a world, internet will be the information vessels and ‘data’ will be currency. Data is at the core of all cyber activities and has issues of privacy, protection and power.

In other words, data is critical to the entire cyberspace and thus the country or organisation or individual that holds control over data acquires digital power in the cyber world. For instance, the Domo’s Data Never Sleeps 5.0 report stated that “every day, netizens generate 2.5 quintillion bytes of data – 90 per cent of the data in the world has been created in the last two years alone” (Marr 2018). Each online activity generates data or sets of data: “from sensors used to gather climate information, individual posts to social media sites, digital pictures and videos, online transaction records, cell phone GPS signals to name a few, all generate data” (Wieczorkowski and

Polak 2014: 184). These data are core assets to the state, businesses, industries, economies and non-state actors.

Cyberspace is complex and a complicated ecosystem made of human and networks (Cavelty 2017)¹. Much “like natural ecosystems, the cyber ecosystem comprises a variety of diverse participants – private firms, non-profits, governments, individuals, processes, and cyber devices (computers, software, and communications technologies) – that interact for multiple purposes” (United States Department of Homeland Security 2011: 2). This digital environment weaves all natural “environments together as never before. Yet, much like these other natural environments”, it cannot realistically be controlled (Bryant and Mahrira 2012: 8). The digital revolution has created an interconnected cyber-physical-social ecosystem (Hsu and Marinucci 2015: 13). In this complex, complicated and interconnected ecosystem, where those who consume data also generate it, everyone is a stakeholder (Hsu and Marinucci 2015: 13). The complexity and widespread networks often lead to information leakage due to internal glitches (bugs) or external intrusions that is potentially catastrophic when it comes to individual privacy and data protection in the cyber ecosystem.

Moreover, large amounts of data packets² that float in the cyber world are highly vulnerable and insecure, because hardware, software and data cables that are physically located, can be accessed by actors like state, businesses and individuals. When the Internet technology was created in the United States of America (USA) in the 1980s, it was fundamentally for use in the military arena. Thanks to Tim Berners-Lee, a British computer scientist, who invented the World Wide Web, at the end of the Cold War, when the US emerged as the only superpower, that the internet went public and entered the civilian domain and this would have a revolutionary impact on world politics due to the rise of the Information Communication Technologies (ICT).

¹ This point was mentioned by Dr. Myriam Dunn Cavelty, Senior Lecturer for security studies, ETH Zurich, in a Skype interview with the researcher on 13 March 2017.

² “A data packet is a unit of data made into a single package that travels along a given network path. Data packets are used in Internet Protocol (IP) transmissions for data that navigates the Web, and in other kinds of networks” (Techopedia 2019)

The impact of this technology is global and as a result in January 2019, there are more than 4.1 billion (and counting) connected to the internet in the world, 2.3 billion (and counting) Facebook user, more than 639 million people actively using Twitter (Live Internet Stats 2019), similarly YouTube has over billion users and YouTube claims that netizen can navigate its sites in a total of 80 different languages, that covers 95 percent of the Internet population (YouTube 2019) and all this is growing exponentially. For the first time in human history, time and space have been shrunk by the innovations and revolutions in ICT that has created a truly networked and interconnected world of human and machine interactions. Each user generates a new set of data and as a consequence it creates an unprecedented amount of data that hold all kinds of information. This data can be mined for different kinds of information, which can be used for benign and illegal and criminal activities.

Cyberspace is currently an ungoverned terrain which needs to be secured, governed and open to all and abided by laws. Is it possible to replicate real world structure into the cyber world? Could it be possible to implement traditional legal boundaries to cyberspace? Who will provide security to 'individual data' - state or corporations? Can existing laws be applicable to data protection? Is there any security in the cyber world? Before analysing the nature of security in the digital world, there is a need to examined and understand the meaning of security in the as currently used in international politics.

'Security' is essentially a contested concept in international politics that is most commonly associated with states and the alleviation of threats. Since the 1648 Westphalian Peace Treaty, security in the classical sense refers to the survival of 'the state'. According to Caveltly and Mauer (2010: 48) "security is about the identification of *threats* to a particular *referent*, and the formulation of policy responses to those *threats*". However, the concept of security has expanded over time from the, the World War I, the World War II, the Cold War and the 9/11 attacks on America.

The Cold War security paradigm was fundamentally understood as one state action against another state and the threat was seen to impact 'territoriality, state sovereignty and state autonomy'. The emergence of those threats can be largely articulated in

three major clusters viz. *symmetrical security threats; security dilemma and arms race*, which was an outcome of the East and West rivalries between the US and the USSR.

The preoccupation during the early the Cold War rivalry on the state as the prime source of threat, gave way to an expansion of the concept of security with the introduction of human security in international politics. However, in 1970s, the Copenhagen School of thought pushed the concept of human security which was later endorsed by the UN. Thus, from the late 1980s security has two components state and human security. The fall of the Iron Curtain (1989) and the dissolution of the Soviet Union (1991) brought to an end the existential Cold War rivalry. However, the conflict did not recede in the post cold war period and there were many conflicts - the emergence of the Balkan conflict and disintegration of Yugoslavia following the civil crisis viz. Slovenia (1991), Croatia (1992-1993), Bosnia (1992-1995), Kosovo (1999); the Oil-Crisis (1990) and the Gulf War-I (1991), which created turmoil on the international security landscape as all these events happened simultaneously.

The United Nations Human Development Report-1994 not only contributed to the concept of human security but also widened the discourse between military and non-military threats. In essence, in the post-Cold War world, the realm of military security was significantly diluted by the emphasis on human security till the events of 9/11. During the Cold War, new advanced technologies (Nuclear, Space and Internet) emerged and became a tangible element of national security. An amalgamation of computational, nuclear and space technology had a transformative role in the creation of global-(in)-security. While the process of globalisation and rapid digitisation has paved the way for greater connectivity, but on the other hand, this new environment brought new threats and vulnerability to both national and human security.

The September 11, 2001 terrorist attacks on the US impacted the security landscape by showing the power of non state actor to jeopardise peace, stability and prosperity on their terms. The Post 9/11 world order experienced a mushrooming of enormous challenges at the regional and the international level such as global terrorism, Weapons of Mass Destruction (WMD), climate change, fragile state, organised crime and more diffusely cyber-threats and the role of non state actors. National security

thus had been redefined in the post-Cold War period beyond the border and had to address the new threats. 2001 is one of the benchmark years, in which the concept and discourse of security widened and deepened in international politics.

TRADITIONAL THREATS TO SECURITY

In international politics, traditional threats target the fundamental principles of state security- territorial integrity, sovereignty and autonomy, and thus the nature of threats were identifiable, predictable and response could be calculated. Thus, in the traditional security paradigm a state could measure, analyse, measured, and comprehend the threat and could come with reasonable response. By analysing the threat perceptions, the state can also create a mitigation strategy to minimise the impact the threat and costs of the war any.

In international politics, state behaviour has significant implications for the rise of (in)security- creating the security dilemma for the other states. Security dilemma was created because of big ambitions to rule larger geographies had witnessed the emergence and fall of traditional territorial security structure e.g. British Empire, Mongol Empire and Russian Empire (were the three biggest empires of the history as per the land area it controlled). The territorial ambitions were complimented with Sea powers, it is quite understandable that who controls the land, controls the resources; who controls the water, controls the trade (economy). Prior to the two World Wars, armed forces were traditionally confined to exercise in land and water. The airspace emerged as third front of security structures later. States had witnessed a rapid technological advancement in aviation and in military affairs in early 20th century. This was seen during the World War I and more significantly a vital part of national power and used aggressively during the World War II. The airpower exhibited and scaled up the impact of global and means of future warfare. The impact of airpower was evident from the attack on Pearl Harbor on December 7 1941, in retaliation to that, the US's responses to it, became very crucial to the global and European security landscape and just after three years and seven months, the American attack on Japan through its mighty display of nuclear power by bombing Hiroshima and Nagasaki, on 6 August and 9 August 1945 respectively, would establish how technology would be a game changer in relations between states in the coming century. Moreover, the idea of threat to state and to preserving sovereignty creates dilemma, thus, the security

conditioned the mutual survival and safety of states. In other words, security dilemma led to arms race and to the traditional idea of the enemy being identifiable.

The end of World War II and new technological underpinning made a tectonic shift in the global security architecture and as a result the US and the USSR emerged as the two power blocs of the security evolving landscape. On the other hand, the war also brought to an end to the European balance of system and paved the way for balance of power structure. For the first time in global politics the power has moved away from Europe landmass to beyond the Atlantic Ocean and the US acquired supremacy in political, economic, and military moreover in technological knowhow than any other countries.

E. H. Carr's significant work "*The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations*" published in 1939 and Hans Morgenthau's well known book "*Politics Among Nations: The Struggle for Power and Peace*" published in 1948, provide a comprehensive and systematic analysis of the power struggle and security debates in international politics at that time. The power is not static and the balance of power can change over a span of time, with the impact of technology, it can also transform the outcomes and which state can be a leader in the international politics. In the early 1950s technology as a critical factor for national security as well as for economy growth, this is where America overtook both the Europe and USSR by investment on research and development. The revolutions in the area of science and technology have influenced the security of the state and this also lead to the revolutions in the military affairs, how the states could conduct on based their military apparatus. Thus, to address the threats to national security, military solutions influenced the security apparatus (Ullman 1983: 129).

In fact, in the span of a decade the USSR equalised with the US's military technological superiority by becoming a nuclear power in 1949 and overtook it became the first Space power with the launch of *Sputnik 1* in 1957. Hereafter, the two new technologies i.e. Nuclear and Space got integrated to national security apparatus of major global powers. Gradually nuclear weapons have become part of conventional weapons and incorporated into the Land, Water and Air power force structure. Throughout the history, revolutions in technological knowhow have transformed how

states used military forces – the shifts from men and animals (soldiers and cavalry) to men and machines (soldiers and mechanised infantry, aircrafts, conventional and nuclear weapons).

Till the end of the Cold War in 1990, military forces were fundamental to state security. This aspect underwent a change in 1990, with the inclusion of the idea of non-traditional threats to security. Prior to the 9/11 terror attacks on the US, IR pundits had also been able to redefine the changing nature of threats. Moreover, in 1989, prior to the end of the Cold War, Foreign Affairs published an article by Jessica Tuchman Mathews, an American peace activist, 'Redefining Security', she argued that 'the 1990s will demand a redefinition of what constitutes national security' (Mathews 1989: 162). It would take another 10 years for expanding the vocabulary of non traditional threats to security at the European and the American level. Terrorism as a global threat was recognised only after the 9/11 attacks on the US.

NON-TRADITIONAL THREATS TO SECURITY

The end of the Cold War which had also produced the longest peace in Europe was also marked by the return to war to European landmass nearly after a gap of half a century. On the other hand, in some parts of Asia, Africa and South America witnessed a rise in interstate and intrastate conflicts. The 'unipolar moment' (Krauthammer 1990) or the period of America hegemony (McCormick 1997) did not last long, as the 9/11 terrorist attacks on America, that became the defining moment for global security landscape, showed the indisputable rise of non state actor and the rise of asymmetric warfare. It can be argued a paradigm shift was taking place on national security and military level and state would have to reconfigure their security based on this phenomenon of non state actor and changing means of warfare. The 9/11 showed states were confronted with new vulnerabilities, risks and threats to which it was not easy to create a strategy or response.

Keohane and Nye in their structural analysis of the international system have focused on non-traditional threats and they have emphasised three factors: "*multiple channels*" - various ways for the movement of threats, *absence of hierarchy among issues* – only military security does not consistently dominate the agenda, '*minor role of military*

force' - there are many other ways to address the threats due to diversity of the threats" (Keohane and Nye 2001: 20). Certainly, the metaphor of security in the Post-Cold War period has changed.

Given that the non-traditional threats are unpredictable, it has become extremely difficult to the state to address the challenge policy and response. Since non-traditional threats have emerged the news issues can be categorised into five sectors of security: "*political, military, economic, societal and environmental*" (Buzan 1991: 433). The political and military security is a interplay between the defensive and offensive capabilities, intentions of states against other states, which is further linked to the organisational stability, legitimacy and government system of states. It requires greater and significant balance between the political and military aspects of security. Other three security aspects are fundamentally concerned for a sustainable future in which different facets of economy, society and environment of the states are interlinked. Moreover, "those five sectors do not operate in isolation from each other. Each defined a focal point within the security *problematique*, and a way of ordering priorities, but all are woven together in a strong web of linkages" (Buzan 1991: 38).

Within a short span of time, global security has faced two major events- '11/9 (1989) shifted from the Cold War predictability to unpredictability of power equation and 9/11 (2001) showed how the level of unpredictability had increased due to the role of non state actors' (Booth 2007: 2) that have impacted the. Issues such as climate change, terrorism, civil wars, ethnic violence, political instability, cyber-threats have emerged as new threats now and are further enhanced the unpredictability. Although, the state remains the key actor to address both traditional and non-traditional threats, the roles of international organisations, multinational and regional organisations, NGOs, have also gradually transformed with respect to international security.

Growing unpredictability increases the impact on the political, economic, security and human level, because it is not possible to calculate the cost of the threat. In addition to this, it also underlined the fact that technology that enables a state to become a superpower, the very same technology also helps others to challenge its supremacy. In other words, technology empowers all and importantly has challenged the territorial supremacy of a state and it empowers groups, organisation, and people. Given the

high level of unpredictability posed by non-traditional threats, the level of vulnerability has also increased. This period had also witnessed the synergy between the information communication technology and non-traditional threats to state security. After the worldwide socialisation of the cyber technologies in 1991, such as internet, computer and networks has produced huge opportunities as well as expanded challenges to national security.

With the advent of cyber technologies, the risk factors have also multiplied with it, for example in a digital age new attacks could be carried out easily by non-state actors. Undeniably the incremental assimilation of terrorist groups in the cyberspace is increasing day by day and the internet provides a medium for anonymity, communication and a platform for attack (Wilkinson 2010: 134). The new millennium is influenced by the quick growth of fast-cum-soft technology (i.e. internet and computers). This prime mode of communication is highly interlinked with the virtual world. Thus, the growing infiltration into the cyberspace has been making state and human security more vulnerable.

EMERGING SECURITY LANDSCAPE AND ACTOR MATRIX

The security landscape is always dynamic as the equation between the states, nature of threats and vulnerabilities are constantly changing. The European Union (EU) as an actor is the unique outcome of two war(s) in Europe. The end of the World War II had altered the centuries old power structure of Europe, which led to the power shift on its two flanks. The rise of the United States of America (USA) and the Union of Soviet Socialist Republics (USSR) scripted the future narratives of global politics that was the 'Cold War' from 1945 till 1990.

The aftermath of the World War II had left Europe with a political, economic, social turmoil. The economy had collapsed in many countries [Germany, Italy, France and many Central and East Europe (CEE)], there were millions dead and a large part of the most important cities were destroyed. Undeniably, the untold miseries and high unemployment rates were at the extremes of the 20th century in many countries. However, unlike the post WWI period, the US did not retreat a policy of isolationism and continue to be engaged with the Europe the most visible action came through the Marshall Plan or the European Economic Recovery Plan (1948) that was aimed the

European reconstruction. Since the USSR, prevented the CEE countries to receiving any aid, The Marshall Plan served two purpose - economic rebuilding in the Western Europe and the expansion of the US foreign policy influence over the landmass.

During the Cold War, ideologically and politically the world was divided into two parts. In addition to this, the Western Europeans were engaged in different ways to keep peace, development, and containment of Germany. Indeed, two major events have played a significant role to achieve this: the reconciliation between France and Germany would to lead the European Coal and Steel Community (ECSC) and the European Economic Community (EEC) the first step towards regional cooperation and the Trans-Atlantic collective defense mechanism (i.e. NATO 1949). The EEC would solely expand from six countries to other West European states led the foundation for the emergence of a new actor – the EEC and later after 1992 this transformed in to the EU. Simultaneously the West Europeans made all efforts to bring peace back to the Europe, the ‘widening and deepening’ process of the EU, in the post Cold War period has reached a different paradigm. The European unity and peace projects which started in the post -war period got its real worth only after the end of the Cold War, i.e. the Maastricht Treaty 1992 and the growth of EU to take in CEE countries.

According to Cooper (2000) “in 1989 the political systems of three centuries came to an end in Europe: the balance of power and the imperial age. That year marked not just the end of the Cold War, but also, and more significantly, the end of a state system in Europe which dated from the thirty years of war” (Cooper 2000: 15). The Cold War had given a period of partial peace to Europe, in which the states did not engage in any kind of direct war. The end of Cold War brought war back to the heartland. The end of Cold War paved the way for the rise of the US as a hegemonic actor and on the post Maastricht Treaty 1992, the EU emerged as supranational actor.

THE EU’S ACTORNESS AND SECURITY DYNAMICS IN EUROPE

The predecessor of the EU, the European Coal and Steel Community (ECSC), was formally established in 1951 aiming to bring about the cooperation between two critical industries (Coal and Steel) and it was expected to have a spill over effect of economic growth. Gradually, the EU has been elevated from a mere economic

organisation to a political actor (Ginsberg and Smith 2007) and to a global security actor (Kauert and Zwolski 2013). But, the dilemma of the globalised world and with multi-level governance within the EU, this has brought worrisome challenges to the Union in the 21st century.

The crises in the heartland - the emergence of the Balkan Crisis, the fall of communism in CEE after the disintegration of the USSR had entailed that the EU should create its own mechanism to fight against non-traditional threats, because they had to respond to these new threats and could not depend only on NATO to address these issues. On the other hand, the US unilateral retaliation against the 9/11 attacks had urged the Union to address the newly emerging threats with new set of approach and values. The convergence seen between the EU and the US aftermath of the 9/11 attacks was replaced by the divergence on the matter of the presence of WMD in Iraq in 2003. In this backdrop, the European Union's adoption of the European Security Strategy (ESS) in 2003 made it more active in the field of security and crisis management, as for the first time the Union has identified five non traditional threats. However, this also led to many questions arising on the nature of the EU and the kind of actor it is. Endorsing the effective multilateralism as a way forward, the ESS underlined that in a globalised world, a single state will not be able to address the threats alone due to the vagueness and unidentified nature of such a threat. Thus, the 2008 reviews of the ESS would include cyber security.

The last decade of the 20th century has shown pragmatic changes in the security dimension of the EU and role of its '*actorness*' (Greicevci 2011). Nevertheless, certain conditions have to fulfilled to become an actor, thus, the question is, how is the European Union conceptualised as a security actor, it is not a state nor having any sovereignty, rather is it a unique organisation in which 27 countries have given sovereignty and delegated their different areas in power to a mutual authority.

In fact, the EU first devised a mechanism for ensuring security, developed decision making procedures, and created an institutionalisation of the security domain. Gradually, it increases the stake in European security by extending an area of security, freedom and justice in Europe. The European Union's role in international security affairs has also evolved substantially in recent years. In essence, its developing

security portfolio includes the processes of state-building, conflict management, crisis management and peacekeeping missions. The security role of the EU develops at four levels: an institutionalised security domain (i.e. the CFSP); diplomatic ability (i.e. EEAS); an ‘external anchor’ for the periphery (i.e. ENP); direct military capacity (i.e. ESDP). The Maastricht Treaty 1992, Petersberg Tasks 1992, followed by Treaty of Amsterdam 1997 and the “Cologne European Council meeting in June 1999 developed the ESDP as part of the CFSP. During this process it was clear that the Member States have given a strong consensus that the Union must have the capacity for autonomous action backed by credible military force, ... and the readiness to act in order to respond to international crisis” (Greicevci 2011: 284). All these developments positioned the EU as a security actor, although traditionalists have not considered the EU as a composite international actor due to definitional deficits.

According to Sjostedt (1977:16) actor’s capability is a “capacity to behave actively and deliberately in relation to other actors in the international system [and that this] capacity primarily is a function of internal and internal cohesion”. Furthermore, Bretherton and Vogler (2006:2) have stated that actorness is “constructed through the interplay of both internal and external factors”. According to Rieker (2009: 703-719), an analysis of “the EU as a security actor can be done if the concept of capabilities is elaborated”. March and Olsen (1995) in their seminal work distinguishes four broad types of capabilities: “1. *Rights and authorities* – rights and authorities are the capabilities that are supposed be enshrined in formal rules. 2. *Resources*: by resources they mean the assets that make it possible to achieve the objectives viz. money, property, time, information, facilities and equipment, and have both individual and institutional attributes. 3. *Competencies and knowledge* on the part of individuals, professions and institutions. 4. *Organising capacity* – in fact this capacity is dependent on the availability of the other capabilities; it is also a condition for making effective use of them” (March and Olsen 1995: 95). They further elaborated that “without organisational talents, experience, and understanding, the other capabilities are likely to be lost in problems of coordination and control” (March and Olsen 1995: 95).

As Cooper (2000) argues that “the postmodern system in which [we] Europeans live does not rely on balance; nor does it emphasise sovereignty or the separation of domestic and foreign affairs. The European Union has become a highly developed system for mutual interference in each other’s domestic affairs, right down to beer and sausages” (Cooper 2000:19-20). But, “if the EU is becoming an increasingly more important actor, European [we] expect to find these capabilities exist, that they are of a certain size and that they increase over time” (Rieker 2009: 703). According to Rieker (2007: 11), “if the EU is indeed a security actor, [we] would expect to find (1) that rights and authorities have been developed for the CFSP and ESDP; (2) that resources in terms of budget, staff and equipment are allocated to the CFSP and ESDP; (3) that the CFSP and ESDP staff possess the necessary expertise and experience in this field; and (4) that the EU has the organising capacity to make effective use of its formal rights, resources and competencies”.

Over the period, the Union has developed a set of formal and legal rights (the Charter of Fundamental Rights of the European Union), institutions (the EU, the EC etc.) and rules to regulate this policy area (data protection), and that these have increased over time. Second, with the regard to resources (budget, staff and equipment), the EU has resources in this sphere and influence on its MS. In addition to that, the Lisbon Treaty 2009, the EU Global Strategy 2016 and The Permanent Structured Cooperation (PESCO) have enhanced and elevated the EU role as a security actor in the global security landscape. The EU that took a baby steps through the ESS to address the security issues of the Union, has taken a big stride by announcing the EUGS 2016, that seeks to address the emerging threat issues in global security landscape.

THE US AND GLOBAL SECURITY DYNAMICS

The US perused a policy of isolationism until the World War II. The attack on ‘Pearl Harbor’ and an increase in rivalries and tensions in and after 1945 produced a new international vocabulary – Cold War. The Cold War period remains as a hotspot in realpolitik from 1945-1990. After the demise of the Soviet sphere of influence, the US was often called the sole superpower in the world (Ikenberry 2005).

The US perceives global security through the prisms of national security and this plays an important role for its global foreign and security engagements. “The National

Security Act of 1947” created a legitimate national security structure and that was again concretised through “the Goldwater–Nichols Department of Defense Reorganization Act of 1986”. During the Cold War period from 1945-1990, the United State (US) was one of the key superpowers, along with the Soviet Union. The US identified its security interest at a much larger and global level and thus it had identified both national interest and response at national security from this perspective. Charles Krauthammer an American political columnist wrote the famous essay ‘The Unipolar Moment’ 1990, in The Washington Post, canvassed the end of Cold War indicating the rise of the US supremacy in global politics in the post Cold War period. The ‘moment’, was dramatically challenged by the terrorist attacks on the US in 2001.

Precisely, the terrorist attack in 2001 on the US made a radical change in the geostrategic approach to non-traditional threats and led to a structural makeover by the Bush administration via enactment of the Homeland Security Act 2002. The Act created United States Department of Homeland Security (DHS) and it was the largest and the most significant development in national security apparatus since National Security Act 1947, that created the Department of Defence (DoD). Since its inception, the DHS has been dealing with plethora of issues ranging from terrorism to disaster management. By default, the DHS was kept away from FBI, CIA and DoD, this design often collide with international laws. In fact, to stop future occurrences of such type of critical attacks, the Bush administration came up with a new National Security Strategy (NSS) 2002, which emphasised unilateralism, hard power politics and contentious strategy of ‘pre-emptive’ war (and it continued to remain as the vital part to US foreign policy).

The NSS adopted in 2002 identified that “the gravest danger our Nation faces lies at the crossroads of radicalism and technology” (NSS 2002). For the first time the US govt identified the technology as a disrupter for state security. In the ‘National Security Strategy 2006’, the Bush government envisaged that “disruptive challenges from state and non-state actors who employ technologies and capabilities (such as biotechnology, cyber and space operations, or directed energy weapons) in new ways to counter military advantages the United States currently enjoys” (NSS 2006: 44). Moreover, the Bush administration pursued the unilateralist foreign and security

approach to deal with the non-traditional threats. The successors of the Bush administration have more or less followed the similar strategic approach to deal with non-traditional threats to security.

The US had to lookout for resurgent Russia guided by Putin as well as rise of China and unfolding of new engagements between them, which poses potential challenges to the US global aspirations. The NATO and allies have been spending billions of money from Kosovo to Libya to Sudan to achieve peace and international security, although there were more failure than successes. However, the increase of new risks and vulnerabilities viz. malicious cyber activities have altered the security landscape and also manipulated the matrix of international actor. In the Cold War, security landscape threats were identifiable (known), however, the post Cold War security landscape, with the advent of cyberspace and technologies, they have changed the threat perceptions. It is nearly impossible to locate the origin of the attack in real time. Thus, the known became unknown, unpredictable and unidentifiable that emanates from unseen risks and vulnerabilities to the government, business, society and individual. This 'unknown-unknown' factor posed serious challenges to the actor matrix in global security landscape.

SECURITY IN A DIGITAL AGE

Security in the digital age is impacting everything and anything which is connected to this ecosystem - government, businesses, society and individual. In fact, cyber-threats not only affect the national security, but affect private security, security of critical infrastructures, personal security equally and fundamental freedoms are also hampered. Although, the debate on cyber security began more than three decades back, but it has now come into prominence in the traditional and non-traditional security realm. Cyberspace is becoming more vulnerable due the proliferations of new devices. Thus, the issues of cyber security have to be addressed in a rational way. Unidentifiable threats are already hiding behind the screen and on the other hand both public and private sectors have to cooperate in addressing this new threat. Above all, international organisations along with non-state actors (Industries, Civil liberty groups) would have to work actively in this field to ensure cyberspace does come under the jurisdiction of the international law while maintaining its core - free and open place to assemble.

Swiftly, these modern revolutions through the ICT have created a virtual platform for the emergence of new threats. In the realm of the digital age, both the internet and computer technology creates a virtual reality, that is, denoted as 'cyberspace'. William Gibson in his 1982 short science fiction story, 'Burning Chrome' used the word 'cyberspace'; however, the term became popular in 1984, after its use in his novel *Neuromancer* and gained more universal currency. Etymologically, cyberspace is a fusion term and the source of the first word 'cyber' is derived from the Greek word *kybernetes*, which means a pilot, governor, and ruler. The root 'cyber' is also related to 'cyborg' - that illustrates a human-machine interactions resulting by connecting the human body to advanced high-tech devices.

Perhaps, the increasing complex interdependency in cyberspace makes it more vulnerable because of its soft nature, easy accessibility, and this makes it even difficult in identifying where the threats to it originate - a state or non-state actor (business, individual). Over the decades, the cyber-ecosystem has largely been used by both state and non-state actors and individuals to accomplish their goals. Although, the cyber-vulnerability may not as dangerous as Weapons of Mass Destruction, but it is mostly used for soft targets and can be used as a *Weapon of Mass Disruption*³.

The exponential growth in the adoption and use of the cyber technologies for the both personal and business purposes have put vast amounts of information to be prone to attack. This is not limited to geographical demarcations, rather has global implications, because information transferred around the globe quickly and efficiently via the Internet (Griffin 1998: 135). According to Roth, a cyber threat to security is a pertinent issue to human security. To ensure a digitally resilient society, government and law enforcement agencies play a pivotal role in protecting individual privacy from being exploited via big businesses. The idea to be expressed here is that big business can be expected to exert pressure to create legal and political conditions that benefit their interest, in particular when it comes to profiting excessively from their ability to collect and monetise troves of information online from unwitting individuals. There is a need for 'fair exchange'. A fair exchange requires that

³ The concept is developed by the researcher, explained in the Chapter -2 of the thesis.

individuals are informed and that they can walk away from a negotiation if they do not agree to the exchange. However, walking away from public life in a world that increasingly moves online is certainly not an option. A take it or leave it proposition put forward by a business cannot be in the best interest of a society. Neither is a situation where individuals are coerced into agreeing to blanket transfers of rights to their data possibly buried in pages of corporate legalese. The bottom line is that fair exchanges in an information economy became possible only if keeping information private becomes possible without harm to one's public and private life (Roth 2017)⁴. In essence, the advancement of the cyber technologies has created a complex-hyper-interconnected digital age.

In this complex-hyper-interconnected digital age breach of security is a frequent occurrence therefore the notion of security is different from the real world. Cavelti (2007:87) has argued that "what has changed significantly due to the particularities of the digital age, however, are some condition so securing ...security is a momentarily static conditions, securing... includes the act of making something (cyberspace) safe or secure and this of actively thwarting possible threats to any given referent object of security, implying actors, politics and policies". Moreover, security in the digital age "has an additional dimension, namely, the humans as potential targets of cyber attacks or even unknowingly participating in a cyber attack. This additional dimension has ethical implications for society as a whole, since the protection of certain vulnerable groups, for example children, could be seen as a societal responsibility" (Solms and Niekerk 2013: 97). On the other hand, socialisation of the Internet and explosive use social networking platforms allows every individual to share information across the globe that creates a virtual repository without adequate legal, political and technological security.

However, for instance, the Morris worm 1988, the Estonian cyber-attacks 2007, Georgian cyber-attack 2008, emergence of 'Stuxnet' 2010, Sony Hack 2014, cyber attack on the Ukrainian Power Grid 2015, 2016, WannaCry 2017, Google+ breach 2018 and Wikileaks, Edward Snowden revelations about NSA spying and Panama Papers all are underlined the significance of cyber-(in)-security. In addition, cyber

⁴ This point was mentioned by the Prof. (Dr) Volker Roth, Institute of Computer Science, Freie Universität Berlin, Germany in a personal interview on 3 March 2017 in Berlin.

security is also interlinked with such issues as the right to privacy, freedom of expression at the individual level, the security of Critical (information) Infrastructure for both state and corporate sector and 'data protection' for individual, state and corporate sector. The complex interconnectedness, high dependency and new risk factors always put question marks on cyber security apparatus.

The gap remains under-examined due to inadequate policy formulation, a lacuna in technological know-how, new and unpredictable nature of threats. However, addressing cyber security issues is the need of the hour through a broad array of means. Because, the ungoverned terrain of cyberspace has become a critical issue for a superpower (US), middle power (India) (Paul and Hall 1999), resurgent power (Russia) (Garrard and Garrard 2008), rising power (China) (Dellios 2004-05) (Ikenberry 2008) (Rosen 2015) and potential superpower (EU) (Leonard 2005).

All through the World War II, the Cold War and beyond, indeed, transatlantic states had maintained close proximity in economic, political, and security affairs, which could be called as 'Cooperation among Democracies' (Risse-Kappen 1997). What stood out was that 'the US enjoyed undisputed economic and military supremacy in the alliance, likewise the European influence[ed] on decision making process in Washington worked through "three mechanisms: norms prescribing timely consultations among allies, use of domestic pressures for leverage in transatlantic interactions, and transnational and trans-governmental coalitions among societal and bureaucratic actors"' (Risse-Kappen 1997). At the advent of World Wide Web to navigate greater trade proximities and data flows both the power had adopted the 'safe harbour' policy in 2000, but the 9/11 terrorist attacks on the US and rise of cyber attacks on government and businesses infrastructures had gained the major focus both from the EU and US, although EU treated both data protection and cyber security in equal parameters.

In 2001, the EU came up with the "Network and Information Security: Proposal for a European Policy Approach", and on the other hand, the Council of Europe adopted the 'Convention on Cyber Crime', both emphasises the criticality and dynamic impact of the cyberspace. To address the non-traditional aspects of security, the EU laid out explicitly the strategy through the 2003 European Security Strategy (ESS), which

essentially identified the major non-traditional threats, viz. “terrorism, the proliferation of weapons of mass destruction, regional conflicts, state failure and organised crime”. The ESS is considered as a starting point of addressing non-traditional threat, in this document, it is stated that no single nation is capable of tackling the threats due to the complexity of the threats. To understand the nature of cyber-threats, the EU created an agency to fight against cyber crime and information security in 2004 i.e. the European Network and Information Security Agency (ENISA) (fully established since September 1, 2005).

Following the Estonian cyber attack, the ENISA became more visible in working as an active institution for securing cyberspace and standardising cyber security architecture of Pan-EU networks. According to Klimburg it has a very limited operational component, the EU CERT is only responsible for defending EU institutions. There is no way that ENISA would assume responsibility for incident coordination across national networks, let alone government networks⁵. Over the years the EU has taken significant steps to address the cyber security issues, at national level, Union level and global level. Moreover, in 2013, the EU promulgated its cyber strategy i.e. the “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013” to address the pressing issue of the hour viz. cyber security, both internally and globally.

Beyond the Atlantic Ocean, the United States is also experiencing the similar and robust challenges of the 21st century. The dramatic attacks, on the US in 2001, brought to the forefront the significance of non-traditional threats, which prompted President George W Bush to outline that ‘vast oceans no longer protect us from danger’. This signified that new threats could bypass the importance of geopolitics, strategic location and also the natural flanks which were seen as no longer secure. The US is a major target of cyber-threats that forced the Pentagon to build its cyber-command and strategy to address the cyber security especially in the context of ‘national security’ and ‘national interest’. Therefore, in 2003, the Bush administration first adopted “the National Strategy to Secure Cyberspace” and subsequently, the Obama administration adopted the “International Strategy for Cyberspace: Prosperity, Security, and

⁵ This point was mentioned by Dr. Alexander Klimburg, Director, The Hague Centre for Strategic Studies, The Hague in a email interview with the researcher on 28 February 2017.

Openness in a Networked World 2011”, these two strategies provide a wider perspective to address the cyber issues. However, President Obama has acknowledged that “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity” (The White House 2011b).

To address the newly emerging threats from the cyberspace, the EU-US reached consensus in the 2010 Summit in Lisbon, and discussed various issues, such as global economy, terrorism, energy security, environmental issues and bilateral ties inter alia with cyber security. In the discussion, they identified cyber-attacks as a global threat which cannot be addressed single headedly. For the first time, the Transatlantic forum came up to address cyber security issues. In fact, non-traditional threats have become more intense over a period of time, and in the domain of virtual world, these threats have made it more vulnerable and simultaneously challenge the fundamental rights. In the realm of the digital age both the internet and cyberspace have emerged as the prime means of communication as well as a new domain for the activities of the state and non-state actors.

But a cyber skirmish had erupted after the Snowden revelations in 2013 about the National Security Agency (NSA) surveillance, which raised the issues of individual privacy and data protection. This intrusive act by the US put a question mark on many issues between the both sides of the Atlantic – the relations between the EU and US, the role of data custodian, limits of national sovereignty that emerged as major concerns among the EU Member States as well as at the global level.

The EU immediately felt that the custodian of data should be based on the new rules and regulations that would have the same temper to adapt to technological changes in a digital world. The government has to play a significant role to make and bring out rules, implement new laws and adopt new regulations so that human society peacefully sustained inside a digital world without compromising privacy and security of the individuals. The issues of privacy, security and data protection debate between the EU and the US has become prolonged issues after the Austrian student Max Schrems attempted a lawsuit against Facebook over its privacy policies and adequate level data protection measures for the European citizens and the data sharing

agreements between the US companies and the Law Enforcement Agencies. The European Court of Justice found that there is clear violation of the data protection 1995 Directive, thus the in judgement on October 6, 2015 the Court revoked the 'Safe Harbour Privacy Principles' to halt the cross border data flows between the EU and the US. This was the biggest setback to the transatlantic data flows since the commencement of 'Safe Harbour' agreement between EU and US since 2000. However, after one year of long regulatory consultations, legal developments and diplomatic settlements between both the parties have agreed upon a new agreement viz. 'Privacy Shield', the future of data flow between the two global power is lot more dependent on the success of this agreement.

All data generated by cyber activities can be divided into two parts – personal sensitive data largely – “racial or ethnic origin; political opinions; religious beliefs; Trade Union membership or financial information; physical and mental health; sexual life and criminal offences and court proceedings considered as sensitive data” (EC 2016b: 38). While the second type of data is commercial data that is generated from everyday online activities and that could be used to track expenditure, preferences, choices, political views and misused to make a profit out of it. In view of this, to protect the European values in the digital age at global level, the European Union formally implemented the General Data Protection Regulation (GDPR) on May 25, 2018. The GDPR is creating a new benchmark for individual privacy and data protection in the digital world. Because the use and misuse of data can pose both threat and opportunity that there needs to be regulations for data collection, storage and use. Based on this data, three specific sets of interactions can be visualised that have different implications.

Data as Risk and New Threat

Data can be used by the private military industries to make revolutionary research on 'Internet of Things', 'Artificial Intelligence', 'Robotic Technology' and Unmanned Technology etcetera that can be used both positively and negatively. An authoritarian state or an undemocratic government could use the same data to digital profile the population, ignite ethnic violence and create conflicts to gain political mileage. Similarly, healthcare industries could use vitals of genetic data to create new drugs that can be highly priced; or even manipulate genetic codes of the population. An

even greater risk or threat is posed by Non- state actors including hacker groups who could use the same data to create law and order problems or provoke violence or to fulfill their financial needs.

Data as Business Opportunity

Data is used by businesses and industries for E-commerce. The growing digitalisation of the economy will create the demand for more data and will also drive business. On the other hand, the growing use of the digital platform by the state and the government is also creating its own demand and supply. E-governance is no longer a buzz word as services are being pushed through the ICT platform. More recently, the Indian ‘Aadhar’ project has come into focus as it creates a unique identity data for every Indian with the intention of providing service. Based on intrusive biometric collection, the matter is under the consideration of the Supreme Court on how intrusive this is to privacy and the necessity to link all activities with the Aadhar. In the absence of proper checks and balances an Orwellian big brother can be very dangerous even to its own citizens.

Data as a Regulated Area

At an everyday level, given the volumes of data that is generated, there is a need to provide a framework to regulate how this data can be accessed, used and transacted. In other words, the digital world also needs a regulatory framework like the real world has rules and laws to enable interaction between people, businesses and states. The cyber world needs its own framing rules so that the rights and obligations of all parties can be clearly delineated. Given that individuals are extremely active along with businesses in creating applications, software and generating data, the regulatory framework needs an input from private players as well. Secondly, any globally applicable cyber law should not have the kind of problems of earlier regimes - that it was not inclusive in design and impact. In third, therefore, all data needs to be secured with adequate technology (encryption and code) and proper legal architecture that will enhance the core values of cyberspace.

The fact of the matter is that all three groups do not exist separately or exclusively. The reality is that they all coexist adding a complexity to everyday life and drawing attention to how ICT has transformed human behaviour, activity, and the role of

business and states. As every digital activity produces data, the challenge is multifold—from the secure storing of data, to the regulations that deal with how it can and should be stored, accessed and the risks associated with the misuse of data. This has added a new dimension to the understanding of security at multiple levels.

THE EU AND CYBER THREATS

Over the years, the Internet has transformed and transcends the traditional politics of world affairs. As the data underlines – internet penetration touched only a billion marks in 2005, inexplicably in January 2019 internet marshal in to connect over 4 billion users and now it has connected more than half of the world population. Remarkably, more than 60 percent internet users have been represented from developing world, similarly, the total number of internet users have increased and multifold from 1999 to 2019 (Live Internet Stats 2019). The *internet world stats*, figure shows that internet penetration levels are highest in the EU at 85.7 per cent and the US at 95.6 per cent as compared to any others regions. On the other hand, developing world has been adopting digital life much quicker than developed world that is why China (only 57.6 per cent of its total population) has highest number of internet users followed by India (only 34.1 per cent of its total population).

The end of balance of power system has led to the rise of new challenges at the last decade of the 20th century viz. state failure, regional conflict and mainly the rise of violent non-state actors. Thus, the EU has made a stand to fight against these issues through the ESS; on the other hand the Union experienced some alarming increase in cyber crime events. In view of this, then, the European Research Commissioner Philippe Busquin said that “cybercrime hides behind our computer screen and in the wires of global communication networks and services”. Therefore, to address the online threats “the EU Cyber Tools On-Line Search for Evidence (CTOSE) project was initiated and supported by the Commission's Information Society Technologies (IST) programme” (Leyden 2003). It was one of the successful projects which were jointly undertaken by “the computer security specialist from the UK, France, Germany, Belgium, and the US. The project has also developed the *Cyber-Crime Advisory Tool (C*CAT)*, as well as a *legal advisor*, an expert system which offers advice on the legal aspects of computer investigations, an *XML-based specification* for electronic evidence, and a *demonstrator* showing investigations of

realistic commercial situations involving simulated attacks from hacking and website defacement to organised fraud” (European Commission 2003).

According to Bendiek (2012: 5), “the gradually developing[ment of] European cyber security policy approach tries to establish minimum standards in all EU Member States with regard to prevention, resilience and international cooperation”. Moreover, the EU aims to foster national security without compromising democratic values or unduly violating individual privacy. Nevertheless, the 2007 Estonia cyber attacks unfolded significant policy and security debates in the European Union. Franco Frattini (2004-2008), the then European Commissioner responsible for Justice, Freedom and Security commented that “the changing nature of security threats requires a strong Public-Private Dialogue in security research and innovation” and in the 2008 review report of the ESS clearly mentioned the cyber security issues and preventive measures as well. Though, the ENISA was introduced before 2007, but it was not in a position for undertaking action. However, after the Estonian attacks, its importance has grown gradually and in 2010 it published a report titled ‘Cyber Europe 2010’, this report importantly revealed that “the EU’s capacity to react to cyber threats is compromised by the unclear distribution of competences within the Union as well as the lack of effective internal structures in the smaller member states” (Bendiek 2012: 21). On the other hand, such “internal problems can rapidly turn into external vulnerabilities. In other words, domestic politics are highly relevant to security policy. Insufficient domestic regulation has an immediate negative effect on the security of other states” (Bendiek 2012: 21).

The EU adopted its Cyber Security Strategy in 2013. Therefore, ‘implementation of the EU cyber security strategy brings together very different understandings of the appropriate balance between state and society, security and freedom, and between policy decisions shaped intergovernmentally and by parliaments (Bendiek 2014d: 3). Since 2003 various literatures have been produced to test the ‘*sui generis*’ quality of the EU, however being a soft power it is gradually obtaining an ‘actorness’ (Archer 2008: 132, Bretherton and Vogler 2006) and stature on the global security landscape. But in this digital age ‘to preserve a balance between a secure Internet and civil liberties, the EU must not stop at simply implementing its cyber security strategy, but rather adopt a comprehensive strategy for cyberspace via the community method

(Bendiek 2014d: 3). The ‘*Special Eurobarometer 371 on Internal Security*’, has outlined that the Europeans are worried about “the risk of terrorism and cybercrime, [which] becoming increasingly sophisticated. [They are neither] constrained by national borders, nor are they restricted to one section of European society, [rather] they have an impact both on individual countries and on the European Union as a whole” (EC 2011: 4). On the other hand, the *Euro Wire 2011* has argued that even though most of the Europeans believe that the “cybercrime and security of EU borders are important and many believe that they will grow in the next three years” (EuroWire 2011), the Union is slow to put together its cyber-security policies. Moreover, “cybercrime is seen as a challenge most likely to increase in the next three years” (Eurobarometer 2011: 8). However, Bendiek (2014d) argued that the EU cyber security strategy aims to step up cooperation between member states over the years ahead in the area of security technologies, yet a comprehensive EU strategy for cyberspace should include stronger legal and policy obligations with respect to exporters of information and communication technology (Bendiek 2014d: 4-5).

THE US AND CYBER THREATS

In contrast to the EU, the role of Science and Technology in national security apparatus has been a key determinant in the US’s power ambitions. According to *Internet Live Stats*, the US stands third behind China followed by India as far as internet users is concerned and also ‘in the top of threat list’ (Cavelty 2014: 702). Papp and Alberts (2000) argued that “as [we] enter the Information Age, information and knowledge related technologies are becoming increasingly important factors in the national security equation of the United States.... [And] move further into Information Age, the impact that these technologies will have on national security affairs will become even more important” (Alberts and Papp 2000: 1). The cyber threats debate originated in the US “in the late 1980s, gained great momentum in the mid-1990s, and spread to other countries in the late 1990s” (Cavelty 2008: 1-2, 2010: 181). Libicki (2007: 2) has argued that prior to the 9/11 incidents, in fact, it was difficult to “conceive of a strategic attack on the US homeland by non-state actors except through the medium of cyberspace”. He further stated that “such would be a bloodless attack from afar that left no traces but could cause the systems we rely on to crash mysteriously. The President’s Commission on Critical Infrastructure Protection argued in 1996 that the capability to launch such an attack did not yet exist – but

given five years (that is, by 2001), it very well might” (Libicki 2007: 2). In the post 9/11 threat environment has led to “a series of worldwide government responses towards net and information controls, such that net content was blocked and removed...The leading legislation was the U.S. Patriot Act, followed by U.N. Security Council Resolution 1373 designed to protect against terrorism” (Cavelty et al 2007: xii). Moreover various provisions of the Patriot Act alarmed “internet professionals who objected to the expansive classification of ‘protected computers’ to include machines located outside territorial borders. The legality of this expanded jurisdiction raised troubling implications for sovereignty issues” (Cavelty et al 2007: xii).

To address the issues of cyber security the US has adopted various strategies both at the national and international level. The September 11, 2001 attack proved to be the biggest failure of information sharing. Therefore, after 9/11, the US adopted “the National Strategy to Secure Cyberspace” (NSSC), which provides a “framework for protecting this infrastructure that is essential to ... economy, security, and way of life” (NSSC 2003). At the very outset the NSSC proved as a cornerstone for public-private partnership. It also documented various policies and programmes to address the cyber-threats. In 2011, the US initiated its “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World”, the aim of this strategy is to enhance international cooperation in information sharing and building international cooperation to address the openness of the cyberspace. In the post-Bush period, as the new government took charge in 2010, the Obama administration underlined in the NSS that

cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority, but our unclassified government networks are constantly probed by intruders. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale. The Internet and e-commerce are keys to our economic competitiveness, but cyber criminals have cost companies and consumers hundreds of millions of dollars and valuable intellectual property. The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states. Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient (NSS 2010: 27).

In 2012, to prevent the events like 9/11, the US adopted the “National Strategy for Information Sharing and Safeguarding(Strategy)” (NSISS). The NSISS aimed to “strike the proper balance between sharing information with those who need it to keep the country safe and safeguarding it from those who would do harm” (NSISS 2012). The Department of Homeland Security (DHS) is the prime organisation for security and surveillance, under the umbrella of DHS, the Office of Cybersecurity and Communications addresses the issues of cyber security within and outside of the US. In 2011, “the Department of Defense Strategy for Operating in Cyberspace” (DoDSOC) adopted and it provides five strategic initiatives to protect cyberspace -

- (i) Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace’s potential;
- (ii) Employ new defense operating concepts to protect DoD networks and systems;
- (iii) Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cyber security strategy;
- (iv) Build robust relationships with U.S. allies and international partners to strengthen collective cyber security;
- (v) Leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation (DoDSOC 2012).

In February 2015, the Obama administration gave top priority to cyber security in the ‘National Security Strategy 2015’. The NSS 2015 has articulated that “as the birthplace of the Internet, the United States has a special responsibility to lead a networked world. Prosperity and security increasingly depend on an open, interoperable, secure, and reliable Internet” (NSS 2015: 12). The strategy was public after the Snowden revelations, thus, the administrations shared their willingness to take the ‘special responsibility’ to lead the networked world but that was clear exhibition of national interest in the name of global moral obligations. The strategy furthers stated that “[Our] economy, safety, and health are linked through a networked infrastructure that is targeted by malicious government, criminal, and individual actors who try to avoid attribution. Drawing on the voluntary cybersecurity framework, [we] are securing Federal networks and working with the private sector, civil society, and other stakeholders to strengthen the security and resilience of US critical infrastructure. [We] will continue to work with the Congress to pursue a legislative framework that ensures high standards” (NSS 2015: 12-13). All these strong commitments were made to enhance the power of the Federal agencies to get access to individual data in the name of national security. Moreover, the NSS 2015 also underlined that “[We] will defend ourselves, consistent with US and international

law, against cyber attacks and impose costs on malicious cyber actors, including through prosecution of illegal cyber activity. [We] will assist other countries to develop laws that enable strong action against threats that originate from their infrastructure” (NSS 2015: 13). The US has developed and elevated its cyber offensive and defensive posture through significant technical, organisational and strategic measures. But the commitment towards helping other countries to develop cyber security apparatus is still very far from reality in the Trump administration.

The NSS 2015 has observed that “globally, cybersecurity requires that long-standing norms of international behaviour—to include protection of intellectual property, online freedom, and respect for civilian infrastructure—be upheld, and the Internet be managed as a shared responsibility between states and the private sector with civil society and Internet users as key stakeholders” (NSS 2015: 13). The Trump administration has also exhibited US’s strong intentions to lead the networked world, on the one hand by adopting “the National Security Strategy” 2017, “National Cyber Security Strategy 2018” (after gap a of 15 years), and “The Clarifying Lawful Overseas Use of Data Act” 2018, on the other hand elevating the position of Cyber Command as a fully independent and unified combatant command.

The US has shown strong intent to address the cyber issues. But ‘both the threat perception and the envisaged countermeasures were shaped by the US over the years, with only little variation in other countries. ... The US is also shaping the information revolution both technologically and intellectually, particularly by discussing its implications for International Relations and security...’ (Cavelty 2010: 181). On the other hand Chinese and Russian are more concerned about nationalised and closed cyber use. In contrast, the EU has been keen to promote cyber normative and ethical values that emphasised for a better digital relation.

THE EU AND US: CYBER PREPAREDNESS AND THE ISSUE OF DATA PROTECTION

The Transatlantic domain has become the cynosure of world’s cyber debates. From security to business, surveillance to openness, restriction to free flow of cross border data have shaken century old relationship and decades old cyber relationships. Therefore, in many European and North American countries, “cyber security

strategies have widely become viewed as increasingly important mechanisms for addressing these risks. However, the bodies in charge of leading or coordinating cyber-security policy across the countries vary from cabinet offices to interior ministries to defense or national security directorates — an unevenness that could hinder international cooperation” (Robinson 2013: 20). Apart from the security and regulations, the issue of governance is also a significant factor in cyberspace discourse. “The present mode of Internet regulation lopsidedly favours the United States and does not sufficiently integrate the emerging powers of Brazil, India, South Africa, China, and Russia” (Bendiek 2014b: 6). The fallout had emerged in the post Snowden era, but for cyber security researchers “the concept of ‘multi-stakeholder governance’ may rhetorically evoke egalitarian fairness, but in practice camouflages the fact that [the US] interests and [the US] corporations are *de facto* the most important agenda setters in Internet governance” (Bendiek 2014d: 4). However, the Obama administration has formally shifted the internet governance power to a non-profit multi-stakeholder entity, although, during the presidential campaign Trump opposed the move of the US government, but has not taken any new steps to undo the work after assuming the office.

The EU-US cooperation on cyber security dates back to the 2010 Lisbon summit, where leaders committed to the creation of a “Working Group on Cyber Security and Cybercrime. The Working Group has established a prominent basis for Transatlantic cyber engagements, with remarkable achievements in addressing transnational cybercrime and other cyber threats” (European Council 2010c: 3). Since then, cyber security and information sharing is a major concern for the Transatlantic partners. The Working Group is divided into four expert sub-groups that work on “(i) cyber incident management, (ii) public-private partnerships (including market access barriers), (iii) awareness raising, and (iv) cybercrime” (The White House 2014). In 2012, both the partners also launched “the Global Alliance against Sexual Abuse Online, the signature of an EU-US joint declaration on making the Internet a better place for children, and the work on enhancing the security of domain names and Internet Protocol addresses” (EUEA Fact Sheet 2014). Few studies also identified that ‘the EU and the US are strongly divergent with regard to their respective cyber security policies. While the Americans are increasingly relying on deterrence, the Europeans are pursuing a more police-based approach, aimed at

building up resistance. This difference is reflected in the different tasks and competencies assigned to the respective intelligence services, and a corresponding different treatment of fundamental civil rights such as the right to informational self-determination' (Bendiek 2014b: 6, 2014d: 4).

Nevertheless, the issues that were revealed by the former NSA contractor Edward Snowden created a larger debate within EU member states, mainly the big three economies- Germany, France and UK. Cyber security requires agreement among states, but the foundation for agreement is trust. As Reding (2014) underlined that, "the Commission took a firm stance from the first surveillance revelations, saying loud and clear that mass surveillance is unacceptable" (Reding 2014: 3). She further stated that "the steps [that] should be taken to rebuild trust in EU-US data flows" (Reding 2014). As far as data protection is concerned "there is a sharp contrast to the privacy and data protection policies in Europe and US. The US approach has been to provide specific and narrowly applicable legislation, in Europe there are unified *supra-national* policies for the region" (Stratford and Stratford 1998: 17). To address data protection issues and emerging divergence Reding (2014) further argued that "first, we must make Safe Harbour safer (Safe Harbour has to be strengthened or it will be suspended). Second [we] need a robust EU-US *data protection agreement* in the law enforcement sector (the so-called Umbrella Agreement) which ensures EU citizens keep their rights when their data is processed in the US. Third, we must ensure that European concerns are addressed in the reform of US surveillance programmes" (Reding 2014: 3-4).

However, when all the security vocabulary put together in a confined box, national security got the top priority. Though, both the partners have been using Public Private Platform to address the cyber security issues, it would be the best option to stick to one principle i.e. trust. As Benedik (2014d) argued that

to stop these differences turning into a massive conflict, both sides need to be much more willing to make concessions to each other. A key condition for successful cyber dialogue is that both sides should acknowledge as fact the domestic political limitations to the transatlantic willingness to compromise. Because of its role as a global enforcer, the United States cannot reduce its emphasis on the security aspects and hence the deterrent dimension of cyber policy, either now or in the future. It is equally true that the EU will continue to focus on

combating cybercrime and that data protection issues will remain of paramount importance. Only if both sides respect these limits to cooperation it will be possible to clear the way for mutually beneficial collaboration in global cyber policy (Benedik 2014d: 4).

However, changes in political structure and ‘proxy’ attacks also are few issues need to be addressed. Similarly, security, privacy, freedom of speech and economic growth all need to be reinforced for a better transatlantic data flows.

RESEARCH FRAMEWORK

In the prism of the digital age, both the Internet and computer technologies have emerged as a consequential mode of communication and simultaneously as a new domain for the activities of the state, non-state actors (businesses) and individuals. While, the process of globalisation and rapid digitisation have paved the way to greater connectivity, this manmade environment has brought new vulnerability and threats to both national and human security.

The post-Cold War security narrative is extensively interlinked with ‘new threats/risks’ that has created a threat cycle after the 9/11. The attacks made a significant impact on the issue of security in the West (the EU and the US) in particular and also at the global level. This made governments to rethink national security and reframe strategies accordingly. Due to inadequate policy formulation, lacuna in technological knowhow and the rise of new and unpredictable nature of threats get multiplied. The whole new sets of strategies that have emerged to address the issues and challenges of post-9/11 security landscape underpins the significance of unconventional threats like terrorism and cyber-threats. In the context of above, addressing cyber security issues have emerged as an area of critical concern given its ability to impact national and human security, economic wellbeing of state, business and individual. This study is a comparative analysis of the EU and the US approach to cyber security and has examined with the special reference to the issues of data protection policy, the ‘convergence and divergence’ between the EU and the US.

The study has evaluated the EU and the US approach to cyber security, focusing on the policies and programmes. The period of the study is from 2001 to 2013. The year 2001 was a benchmark year in international politics with the terrorist attack on

America that highlighted how the international security landscape had become unpredictable. Further, in 2001, the EU came with the “Network and Information Security: Proposal for a European Policy Approach” and on the other hand, the Council of Europe adopted the ‘Convention on Cyber Crime’. In 2011, the US also initiated its “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World”, the aim of this strategy being to enhance international cooperation in information sharing and building international cooperation to address the openness of the cyberspace. The research has examined the other major development of 2013, when the EU adopted the Cyber Security Strategy to address cyber security threats. The study has focused on policy analysis and not on the technological aspects of cyber security. The cyber security discourse is an evolving domain in international politics, thus, the study has expanded and drawn the conclusions on the basis of new developments till January 2019.

The study had examined six questions in detail: What is the difference between traditional and non-traditional security?; What kind of Non-traditional threats have emerged in the post 9/11 world order?; What is cyberspace and what is cyber security and what threat does it pose to national and human security?; What is the EU’s approach to addressing cyber security and specifically the issue of data protection?; How is the US responding to cyber security and what measures does it take for data protection?; In addressing issues of cyber security, especially dealing with data protection, what kind of convergence and divergence is seen in the transatlantic partnership?

The research had two hypotheses - the synergy between information communication technology and non-traditional threats makes the international security landscape more unpredictable while cyber security threats make national and human security more vulnerable. Second, although the European Union and United States are cooperating on different aspects of cyber-preparedness, the issue of data protection shows both convergence and divergence in their respective approaches.

The study has used deductive research methods and applied a realist perspective to use to examine the EU and US approach to cyber security. It has used both primary and secondary data sources. The primary data has been the official documents of the

EU and the US, especially the communications of ENISA, the European Parliament, the Commission, the Council and also the White House, the United States DoD and the DHS documents. In addition, the officially released paper of the UN, ITU, NATO, OECD, Council of Europe and any other Governmental agencies and interviews taken during the field research also included in primary sources. In addition, 9 months of field trip has done by the researcher to interact with policy makers, researchers and experts. The secondary sources have been based upon books and academic journal articles, media reports and think tank reports.

The thesis is divided into six chapters. The introductory chapter situates the research work and begins by examining the changing nature of the security and traditional and non-traditional threats in the global security landscape. Furthermore, it analyses how security issues have expanded since the end of Cold War till the 9/11 and thereafter, especially drawing attention to the impact of technology and rise of cyber security, then using the tenets of realism lays out the key issues to be discussed on cyber security and data protection with respect to the EU and the US. The second chapter describes the nature of the cyberspace and then explains how revolutions in science and technology influenced the national security and how various issues in the cyberspace are challenging businesses, individual, society, state and security. The third chapter examines the evolution of the EU as a security actor in the global security landscape. Furthermore, it evaluates the EU's mechanism, policies and programmes to address the issues related to cyber security and freedom of expression and privacy especially with respect to data protection. The fourth chapter situates the US's as security actor and analyses response to non-traditional threats in the global security landscape. It also examines the US's mechanism, policies and programmes to respond to the issues of cyber security and how national security agenda played a decisive role in the context of individual privacy and data protection. The fifth chapter analyses the EU and the US approaches to cyber security, and examined the convergence and divergence in their approaches to data protection. The concluding chapter presents the finding of the research on the basis of the hypotheses namely the EU and the US approach to cyber preparedness, with respects to threat and vulnerability and issues of convergence and divergence in their data protection approaches.

CHAPTER 2

CYBERSPACE: TECHNOLOGY, STATE AND SECURITY

“The cities that were formerly great have most of them become insignificant; and such as are at present powerful, were weak in old time. I shall therefore discourse equally of both, convinced that human happiness never continues long in one stay”

(Herodotus, 440 BC)

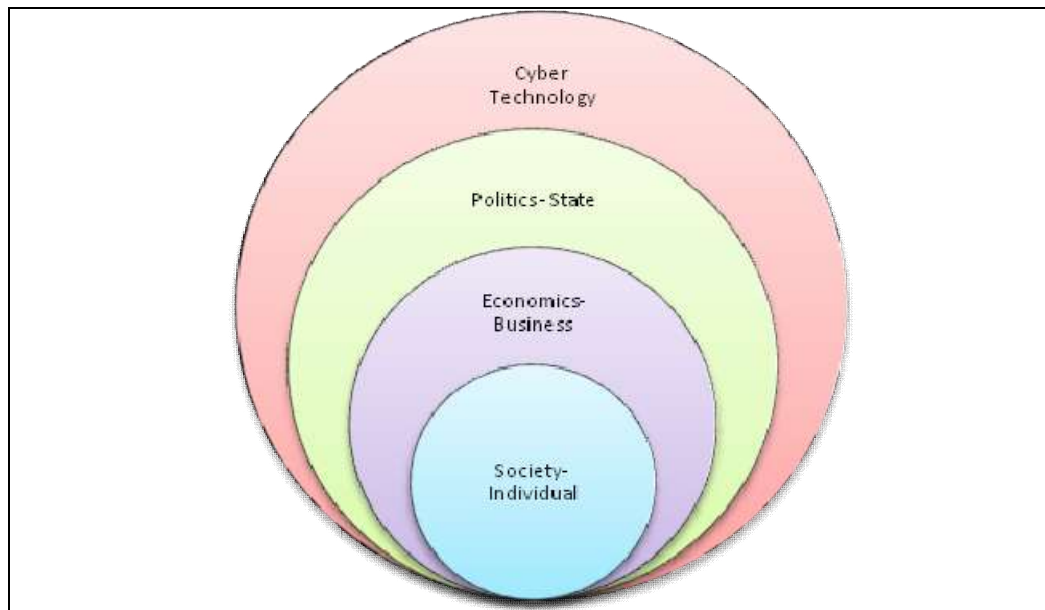
INTRODUCTION

What is cyberspace? Why does it need to be studied in International politics? What separates cyber-technologies from other technologies? How critical is it to understand today's adjacent technological revolutions? The technological growth has created another realm to human life and activity that impacts the individual, societal, political, economic, state and international security.

‘Today's science is tomorrow's technology’ to borrow Edward Teller's oft-quoted phrase. Similarly, today's idea is tomorrow's reality, in essence, some of the ideas of HG Wells and Jules Verne, George Orwell, and William Gibson to name a few. These ideas have impacted, be it state structure, narrative of threats and security, politics, social change, cultural movements, economy and trade. Furthermore, today's politics is tomorrow's history - the Peace Treaty of Westphalia to the first industrial revolution; the second Industrial Revolution (Engelman 2015) to the collapse of the Congress of Vienna (Sandvick and Ewhelan 2016); the First World War to the Cold War; Treaty of Paris to the fall of Iron Curtain; and then the Third Industrial Revolution (Rifkin 2011) and the Fourth Industrial Revolution (Schwab 2016). In these processes of changing power equations between states, technology has an overarching impact (see Figure 2.1) to unleash new avenues of human entrepreneurship.

Beyond this, technology has precisely unfolded a string of revolutions around the world. All of the new revolutions, from the time of Aristotle, up to the Fourth Industrial Revolution, have affected the territoriality of nations most radically and also led to shifts in social, political, economical, philosophical and more profoundly technological understandings.

Figure 2.1: Complex Connectivity and overarching influence of technology on State, Business and Society



Source: Author's work developed in consultation with Ph.D. supervisor

For example in case of the warfare, technological revolutions also challenged the state supremacy – gunpowder, fighter planes, conventional and nuclear weapons. Herz (1957) argued that “air warfare and nuclear warfare has brought the demise of the traditional impermeability of even the militarily most powerful states” (Herz 1957: 487). On the other hand, during the early phase of the Cold War, the role of Multinational Companies started to influence global security landscape.

Thus it becomes quickly apparent why multinational corporations have become important in world politics whether they wish it or not. Shifts away from the use of force are shifts away from the area of corporate weakness, and shifts toward greater prominence of economic welfare objectives are shifts in the direction of corporate strength (Nye 1974: 155).

The 1970's, was when today's leading technology giant started their venture in and around the Silicon Valley. For instance, Microsoft was started by Bill Gates and Paul Allen in April 1975 (The Guardian 2000). In essence, the 1970s laid the foundation to the expansion of cyber age one sees and encounters today.

The formation of cyber world has added another level of complexities and innovations the world is now living in a complex structure of cybernetics - the interaction between human and machines. The Human impute into the technological innovations –

computer, the Internet, World Wide Web, 3D printing, Robotics, Unmanned Aerial Vehicle, Big Data, Internet of Things (machine could speak to machine) and Artificial Intelligence (machine-human-machine interaction) has transformed the equation between physical and the virtual world.

The unprecedented augmentation of the ‘Information Technology or Information Communication Technologies (ICT)’ and its impact to constructing and transforming human-machine interactions have created an unprecedented global connectivity. The cyber technologies have shaped a matrix to connect all the dots around the world through the ‘Internet’. Likewise, the Internet is a network of networks, which translate and transcend each individual action to create universal human digital interactions. Even the pioneer of this technology would not have imagined that in less than 30 years more than half (50 per cent) of the world population would be able to connect to one medium that is the backbone to their everyday function. This ‘*civilisational*’ change has been propelled only by the disruptive diffusion of ICT or the Internet per se in day to day human life.

The impact of cyberspace through cyberisation⁶ followed by digitisation has rewritten the meaning of territoriality and is also transforming the Westphalian order. Robust and disruptive cyberisation has also diffused the power equation between the states, between state and society and between society and individual level. Technology can be considered as a factor in Nye (1990: 179) “the changing sources of power”. He further explained that in “assessing international power today, factors such as technology, education, and economic growth are becoming more important, whereas geography, population, and raw materials are becoming less important” Nye (1990: 179). But in recent times, states have been inclined to control emerging cyber technologies while counting it as a part of hard power linked to national security. Undoubtedly, cyberspace is a virtual space but it has geographical foundation because of computer networks, cables and satellites which are widely based in the physical world.

⁶ According to Ma (2016), Cyberization is the process of formation of the new cyber world and reformation of the present physical, social and mental worlds towards cyber-enabled hyper worlds.

TERRITORY, TECHNOLOGY AND TRANSFORMATION

The ‘impermeability’, or ‘impenetrability’ which was a characteristic of classical state system has been challenged by the technological revolutions – from aircraft to intercontinental ballistic missile and cyber age. For example, the US which was well protected from any external threats also suffered due to an aerial attack on Pearl Harbour in 1941. As Herz argued, “throughout history, that unit which affords protection and security to human beings has tended to become the basic political unit; people, in the long run, will recognise that authority, any authority, that possesses the power of protection” (Herz 1957: 474). Thus, over a period of time, the state has emerged as the political unit that could provide security to the people.

As the Weber points out state can “legitimately use the force” internally (Police) and externally (army) as it is part of the international law. Arguably, origin of state, authority and power politics are intertwined during the evolving process. In other words, state formation was a by-product of human centric action under specific conditions. As Robert L. Carneiro stated that:

The origin of the state was neither mysterious nor fortuitous. It was not the product of ‘genius’ or the result of chance, but the outcome of a regular and determinate cultural process. Moreover, it was not a unique event but a recurring phenomenon: states arose independently in different places and at different times, where the appropriate conditions existed, the state emerges (Carneiro 1970: 733)

The state formation is a nonlinear process; indeed, the processes that lead to the centralisation of sovereignty within a well defined territory. And these processes are not historically and geographically uniform and there is no single explanation or theory for them (Østerud 2011: 2507). However, the impact of technology on territory has challenged the existing notion of state sovereignty. In the post 1945 period, revolutions in the science and technology domain had a profound impact on states capability and capacity – political, economic, and military, which led to power differentiation between the states in international politics. For example, by 1964, the idea of the nuclear ‘P-5’ emerged after China’s nuclear test. The five countries (US, USSR, UK, France, and China) would create a distinct identity for themselves as a nuclear group and prevented anybody from acquiring this technology and joining the group. This would ultimately lead to the creation of Nuclear Non-Proliferation Treaty. In reality, science and technology have impacted the security landscape for state and

non state actors, business, corporations, organisations and people. However, “in the broader social science debate around science and technology, there are two conflicting narratives: *tale of hope* – advances in technology and science tend to make society better and *tale of pessimism* – new technologies and scientific advances have potentially negative or even disastrous consequences” (Mayer et.al. 2014: 3).

New and radical developments in the field of military technology – ‘the gunpowder revolution, killer robot and drones’ – has transformed the nature of warfare. As Storper and Walker (1989: 99) states, the trinity of ‘invention-innovation and adoption’ in technology is what results in massive transformation. History shows that two significant technological developments- gunpowder and printing press would have a revolutionary impact to borrow Wendell Phillips oft-quoted phrase “what gunpowder did for war the printing press has done for the mind”. J.F.C. Fuller (1954) wrote that “it (gunpowder) democratizes fighting”:

With the discovery of gunpowder war passed into its technological phase. Valour gave way to mechanical art: he who could wield the superior weapon was the more formidable foe, irrespective of his social status or his courage (Fuller 1954: 470).

The gunpowder revolution had also impacted the ‘warfare’ and ‘statecraft’ (Cassidy 2003). Similarly, “the printing press fostered knowledge and skills that were valuable in commerce” (Dittmar 2011: 1134-35). Technological revolution alters the power equation and also impacts the social, economic and political equations. Both gunpowder and Gutenberg press had very substantial effects on European society and politics. It changed the power equation between individuals and feudal lords; between feudal lords and kings; between kings and emperor. Similarly, in the present day world, in the same way, digital explosion is generating transformation unlike anything humankind has experienced before.

Digital technology has been able to bring down physical barriers and to unlock multiple opportunities of a cyber world. Is this revolution unique and does it possess magic to transform the equation between state, business and individual?

EVOLUTION OF THE INTERNET AND IMPACT ON STATE, ECONOMY AND SOCIETY

Present day, ICT has been transformed through the '*Midas touch*' of the Internet. The Internet itself was an invention of 1950s and 60s by the US as a response to a particular situation. A mix factors ranging from the Cold War tension, fear to push back through the technological innovation of the USSR, emergence of engineering, science and technology in national security architecture, radical modernisation of defence industry would all lead to the invention of the internet. The *raison d'être*, 1950s and 60s were the benchmark decades in international politics to validate the role of science and technology in national security projects.

Since the first industrial revolution, scientific revolutions and technological innovations have been chiefly associated with national power and security landscape. On way of looking of at the history of national security and warfare is to look at it as a history of technological inventions and innovations. This was also the case in the US and elsewhere, which led to heavy investment in science and technology during the 1940s. A significant and profound innovation has robust implications for national security with global implications. During the midst of the World War II, the US government launched the *Manhattan Project* in 1939 to produce the atomic bombs. The use of the atomic bombs on Hiroshima and Nagasaki on 6th and 9th August 1945 respectively not only fundamentally altered the end of war, also it established US as a super power, end of European balance of power, and firmly established the place of science, technology in national security. In the aftermath of the World War II, a victorious US was able to gain prominent place in global power politics enabled by nuclear science and atomic bombs to become sole nuclear super power for a short period. But the American summer did not last long, as the Soviet Union equalised with their bombs within a span of four years. The Soviet Union simultaneously reached the Space in 1957 by launching the first artificial Earth satellite *Sputnik – 1* to Earth's Orbit. Science fiction had become science fact, this two events (chiefly the Sputnik) had a significant impact and challenged the international image of the US.

The Sputnik effect further intensified the role of science and technology in national security affairs. Prior to this event, Dr. Vannevar Bush, director of the Office of Scientific Research and Development and a wartime advisor to Presidents Roosevelt

and Truman, wrote the legendary report “*Science: the Endless Frontier* in which he argued that scientific research and technological innovations, which proved essential to a successful wartime effort, would be vital to nation’s future peace and prosperity” (Bush 1945, Lane 2008: 248). The Sputnik moment was one of the benchmark events of an overall century of scientific achievement unlike anything seen in history. In response, the US Congress passed legislation formally to inaugurate the National Aeronautics Space and Administrations (NASA). The establishment of NASA clearly signalled the US intentions to join the ‘space race’ against the Soviets. “The Spuncticity of that period underlined that the technology and science would enable a nation to take the lead and high ground” (Tyson 2013). This entire gamut of debates created a complex relation among science, technology and national security that led to technological innovation that would gave birth to the Internet.

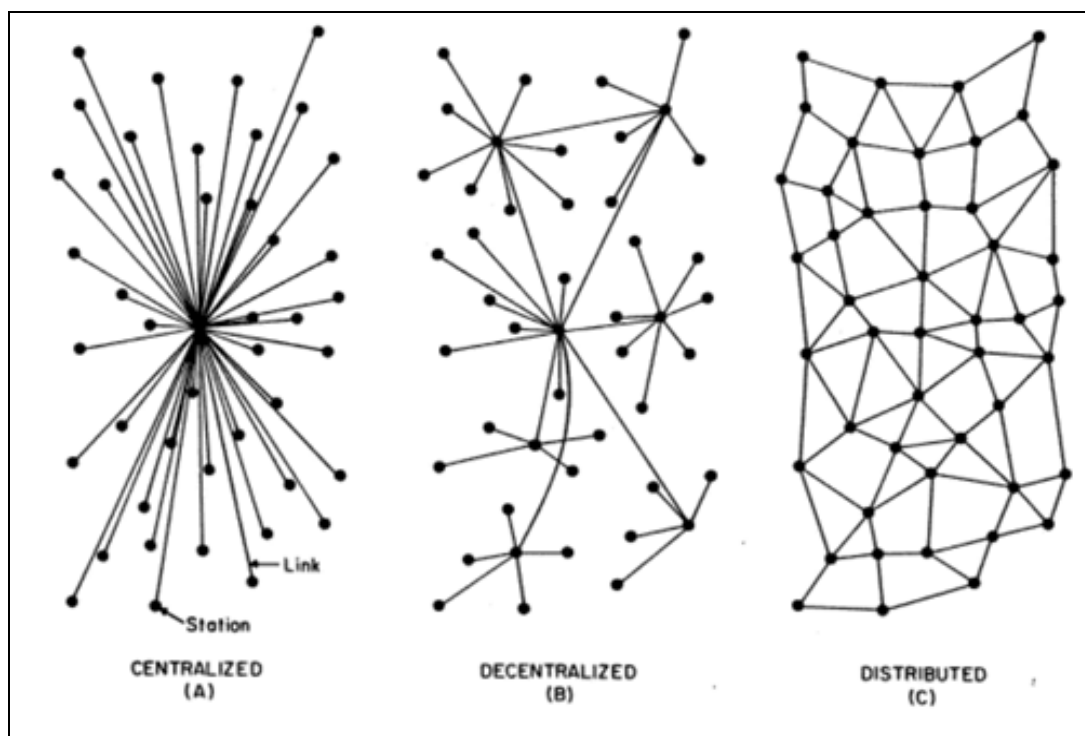
Sputnik Effect and the Evolution of the Internet

The Soviet *Sputnik – I* was “a traumatic experience of technological surprise in the first moments of the Space Age for the US” (Grantforward 2017). In the midst of most dramatic moments of technological history and to address the urgency of the time, a stunned America “became the second nation to place an object in the orbit when it successfully launched the *Explorer -I* satellite on 31 January 1958” (Grantforward 2017) and also established the Defense Advanced Research Projects Agency (DARPA) in February 1958 to address the already-accelerating pace of technology. Notably, this comfort of technological supremacy did not last long, as the “*Eyeball to Eyeball*” (Dobbs 2012) events in 1962 showed.

The hovering cloud of nuclear confrontation seemed imminent in 1962. As the USSR’s hasty and greedy process of building hair-trigger nuclear ballistic missile systems almost pushed both countries towards the brink of a nuclear confrontation. This became a paramount concern for the US authorities, because the older version of the communication architecture had been built upon a centralised communication structure that did not distinguished between the civilian and military systems. And any such attack in the foreseeable future could paralyse the entire US’s communication backbone.

To address such adverse scenarios, the US authorities measured ways to communicate in the aftermath of a nuclear attack. One step in that direction was – the United States Air Force Project to RAND Corporation, US, attempt to find the answer to – “how could any sort of ‘command and control network’ survive? And Paul Baran, a researcher at RAND, offered a solution: design a more robust communications network using ‘redundancy’ and ‘digital’ technology” (RAND 2009). The prime focus of the research was to create a “communication network which will allow several hundred major communications stations to talk with one another after an enemy attack” (Baran 1964: 1). Furthermore, the study had recommended decentralising the single central node of the communication structure to increase the survivability of the communication backbone. Last but not the least, the study also recommended that to increase the survivability, to address common user service for a wide range of users – the requirements of future is all-digital- data distributed network (Baran 1964). This was how modern World Wide Web first started taking shape.

Figure 2.2: Evolution of Internet



Sources: Baran (1964: 2)

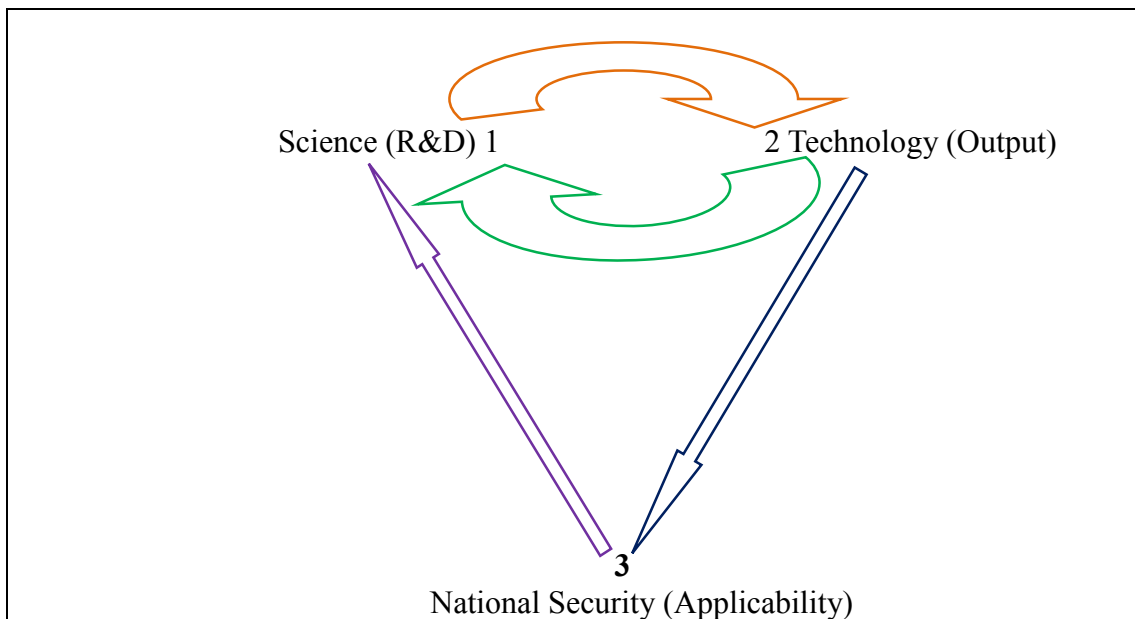
Thus, Figure 2.2 shows that the centralised communication infrastructure is less secure to decentralised and distributed communication architecture. On the basis of the RAND study, the US Department of Defense and the Defense Advanced Research

Projects Agency (DARPA), which deals with emerging technologies for the use by the US military, created the Advance Research Projects Agency Network (the ARPANET). It is this network that pioneered and eventually developed into the Internet. The initial design of the network was to protect the critical information infrastructure system, promote information revolution by sharing digital resources among technically and geographically separated computers. The formation of modern day Internet had two sets of goals at that time–

First Level Goals – “The top level goal for the DARPA Internet Architecture was to develop an effective technique for multiplexed utilization of existing interconnected networks” (Clark 1988: 1). *Second Level Goals* – “1- Internet communication must continue despite loss of networks or gateways. 2- The Internet must support multiple types of communications services. 3- The Internet architecture must accommodate a variety of networks. 4- The Internet architecture must permit distributed management of its resources. 5- The Internet architecture must be cost effective. 6- The Internet architecture must permit host attachment with a low level of effort. 7- The resources used in the internet architecture must be accountable” (Clark 1988: 2).

The prime goal of the architecture was that the Internet should continue and increase survivability and supply of the communications services even in critical failure in networks and gateways. As per the RAND Corporation recommendation, the internet protocols have been developed by Robert Khan and Vint Cerf. One of the Fathers of the modern Internet, Prof. Vint Cerf, always had an academic inclination and often claimed that the internet was created to exchange scientific and academic research among universities. Thereafter, the Internet became an integral part of the military innovations and modernisation (Cerf 2017). History of the Internet had many developments, but, indeed, the sputnik effect had a phenomenal impact on the invention of the internet in the US. The complex interface of science and technology with national security is described by the figure bellow.

Figure 2.3 the complex interface of science, technology and national security



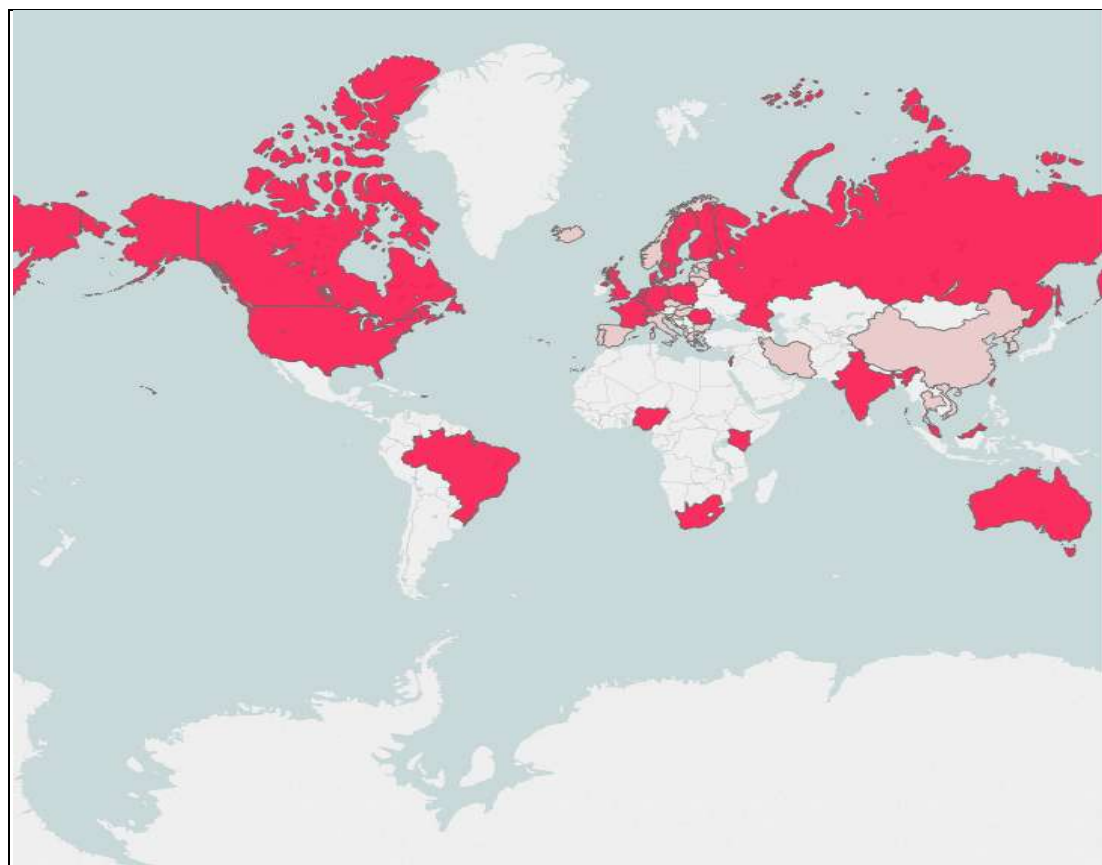
Source: Author's work developed in consultation with Ph.D. supervisor

Expansion of scientific knowledge leads to advances in technology (the flow from 1 to 2). For instance, Bertolotti (1983) did pioneering work on microwave radiation and this eventually led to the invention of the laser, compact disc and the automated supermarket checkout stand. Similarly, advances in technology lead to further research and development at the scientific level (the flow from 2 to 1). The Sputnik effect in the heat of the Cold War brought about intensive space race between two established super powers: US and USSR. Furthermore, the role of space technology in national security gained utmost importance wherein countries across the global start heavily investing in acquiring space technology. During the same period, there was a fear in the breakdown of communication networks. To address such pitfalls and challenges, the invention of packet switching as a new phenomena emerged and that revolutionised the impact of ICT on national security.

Technology affects national security in multiple ways (the flow from 2 to 3). According to Weiss "technology impacts national security - leads to direct technological competition among nation-states, national security affected by issue of the development of the capacity to manage technology, and ability to carry out technological innovation" (Weiss 2005: 298). Technological innovation in the field of internet and computer technology has enriched connectivity, capability for accessing

and sharing information at a faster speed towards a global inter-connected world. The spread of ICT has led to the diffusion of power of the state and empowered the individual to challenged authoritarian regimes (Arab Spring) through an effective and powerful use of social media. The growing vulnerabilities has moved beyond the physical borders and entered the virtual space wherein states are engaged in building offensive and defensive cyber capabilities – viruses and malwares which are the weapons of the cyberspace. This is similar to having tanks, missiles and fighter planes of the physical world. Leakages and risks involved in protecting state, business and individual data are posing multiple and diverse challenges to national security. Artificial intelligence and Internet of things rely heavily on data driven technological innovations. Thus, nation-states and businesses need to create, develop and upgrade on a continuous basis their technological frontiers and cyber preparedness to combat and protect their virtual world.

Figure 2.4: Offensive Cyber Capabilities



- Offensive capabilities (evidences) - 23 countries
- Offensive capabilities (indications) - 24 countries

Source: GIP Digital Watch, 2018

Conversely, national security has strong influence on science due to the continuous

demand for ungraded technologies (the flow from 3 to 1). Development in research and development and technology, has led to the securitising of the information age and the emergence of cyber technology has raised complex questions in regard to the territoriality, sovereignty, autonomy, security of the state. And on the other hand also presented challenges to the businesses.

CYBERSPACE - DATA: AS A MULTIDIMENSIONAL FACTOR

In a span of three decades, cyberspace has underlined and unfolded a different lifestyle that impacts all aspects of everyday life. Internet of Things, artificial intelligence, disruptive technologies are becoming a reality and also amplifying a “Cybered” (Demchak 2010)-life.

Every digital activity produces data. Data is a set of “information that is stored across various mediums – mobile, computer, physical and cloud servers. India’s, Personal Data Protection Bill, 2018 defines that data as a “means and includes a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means” (Meity 2018: 3).

Data can exist in different formats and platforms – as numbers or text in pieces of paper, bits and bytes stored in electronic memory. The data includes everything of a computerised human life – personal and private information of individuals, confidential and strategic documents of an organisation and critical information of a government. However, ‘data protection’ provides legal restrictions and guidelines on the use and misuse of data that is stored or collected by the service provider or data administrator.

Craig Mundie (2014) has argued that “ever since the Internet became a mass social phenomenon in the 1990s, people have worried about its effects on their privacy”.

Mundie further elaborated that, consumers around the world are enthusiastic to adopt a disruptive new technology - ‘use of credit card technology in middle of 20th century’. Now people are showing the same enthusiasm towards devices enabled with IoT and AI infrastructure, drones for personal uses. However, do not pay attention to the security aspect of the data that is produced due to the use of these devices. These

has given birth to the concept of privacy paradox in digital age as although the people are concerned about privacy in their everyday life, do not hesitate to share all detail on a digital platforms, and neither do they secure themselves adequately on digital networks, this leads to a privacy paradox. Interestingly, around the globe ‘personally identifiable information (PII) and data protection’ have become hotly debated topics in policy making while the ‘big data’ still remains unregulated.

“Data! Data! Data!” once cried Sherlock Holmes impatiently. “I can't make bricks without clay” (Doyle 1892). In the information age, data is the clay for all bricks. One cannot provide a solid output without data; the Government’s needs data to protect ‘national security’, corporate business runs through data and also a preferred destination for all cyber criminals. Data protection became a crucial issue specifically after the Snowden revelations in 2013 about the US NSA worldwide surveillance. The revelations provide three takeaways: first, human rights specifically the right to privacy needs a special attention by establishing new global standards or modifying the existing rules. Second, the door should open for other stakeholders for regulating the Internet ecosystem i.e. the multi-stakeholder approach. Third, the UN (by establishing a new agency or revamping the existing structure) should play a bigger role in international cyber security matters (Parida 2017: 96).

Data protection is primarily a subject matter of right to life and dignity, not just business or national security. It is necessary for all the stakeholders to sit together at a table to discuss the issue. For instance, the peace treaty of Westphalia or the Geneva conventions has a lot of binding principles on states. This is not the case in violation of human rights in the cyberspace. This invisible world has huge humanitarian implications and the right to privacy which is an integral part of every individual has also to be protected in the cyberspace.

CYBERSPACE: CHALLENGES TO STATE IN THE INTERCONNECTED WORLD

What is cyberspace? It is the most confusing yet prevalent word used in a globally digitised world. It is a space of nothing yet everything. Rebecca Bryant has sketched the cyberspace differently through the prism of “place, distance, size and route”. She argues:

Cyberspace. This word has stormed into our language and invaded our collective consciousness like no other. As the technology improves and ownership of home computers increases, we competently navigate our way around cyberspace, downloading information, reading and writing to newsgroups, and receiving and sending emails. Cyberspace represents the new medium of communication, electronic communication, which is fast outmoding, or even replacing, more traditional methods of communication (Bryant 2001).

Clark (2010) argues that the cyberspace has four layers “the physical layer, the logical layer, the information layer and the top layer - people”. He further explained that “it is not the computer that creates the phenomenon we call cyberspace, it is the interconnection that makes cyberspace – an interconnection that affects all the layers in our model” (Clark 2010). However, to understand the correlation between geography and cyberspace, and its impact on geographical enquiry, Dodge (1999) argued that “two particular dimensions of Cyberspace that will be of interest to geographers - understanding the geographical diffusion of Cyberspace by relating statistical measures of the Internet to real-space. Second, how Cyberspace can be mapped to help us begin to comprehend it. There are many other dimensions of this ‘new geography’ – cyber-geography - that require due consideration by geographers of all kinds” (Dodge 1999: 9). This could be the beginning of modern day Google mapping or GPS tagging.

Cyberspace is a metaphorical world that is based on the matrixes of computer algorithms. It provides enormous opportunities to connect entire human race into one strand yet it has been increasingly positioned as a platform for mass disruption. It would not be wrong to call it a weapon of mass disruption. Recently, the spread of fake news, disinformation, misinformation - via internet bot attacks; attack on health and banking sector – via malware and ransomware and misuse of Internet media and social networking- public and private spheres, have truly been able to deviate the core value of cyberspace and has fashioned it as a Weapon of Mass Disruption⁷ (here on WM-disruption). In strategic terms, Weapons of Mass Destructions are considered to be “chemical, biological, radiological, and nuclear weapons capable of a high order of

⁷ Russian interference in the US election in 2016, has created dramatic global disruption. It was the first instance when external forces could able to change the political preferences of American voters. The term is developed by the researcher.

destruction or causing mass casualties” (Carus 2012). Here the connotation of ‘WM-disruption’ would be linked to the flow of information as well disinformation on the Internet highways and its negative impact on businesses, governments and societies at large.

Scholars have been investigating decades-old linear trends and issues pertaining to WM-disruption, initially through the prism of military history, deterrence theory and security dilemma to study information war and cyberwar (Lamb 2002). Second, it was to link these debates into the misuse of the Internet by a terrorist (Bunker 2007) from the al-Qaeda to the current menace of the Islamic State. The cyber world has major implications for both the state and non-state actors. Cyber military preparedness has increasingly become a part of state security. Moreover, the prevailing security dilemma with respect to other’s capability (both state and non-state actors) has made cyber-deterrence ineffective in many ways for policy planning and strategy making.

Around the globe, 4.1 billion people (Internet Live Stats 2019), approximately 50 per cent of the world population have connected to the Internet, in contrast to 1995, which was less than 1 per cent. The more world is getting interconnected, the greater is the risks as there are more options for translating this risk into real threats. In the modern history of cyber attacks since 2007, the DDoS attack on Estonia to the recent outbreak of the ransomware ‘WannaCry’ in 2017, there has been a significant and notable amount of expertise, resources that have been invested to launch such attacks. As industries and governments invest more on human-machine and machine-machine and machine-human interaction to make the fourth industrial revolution a reality, here is a core matter to all cyber problems - how to identify who is behind a cyber attack? What kind of systems can be developed to build up cyber preparedness, security and governance? These questions are critical both for the state and business and need to be examined cautiously.

Table 2.1: List of Major Cyber Attacks 1988-2018

Year	Major Attacks	Origin	Target	Referent Object
1988	The Morris Worm	Robert Tapan Morris	UNIX system & US	State
2006	Unknown		NASA (US)	State
2007	DoS	Russia	Estonia	State
2008	Hacking	Russia	Georgia	State
2009	Hacking		Israel	State
2010	Iranian Cyber Army (Proxies)	Iran	China	State
2010	Stuxnet	US & Israel	Iran (World)	State
2012	Red October		World	Business*
2013	NSA	US & UK	World Wide	S.B.I.*
2014	Hacking and Data Breach	North Korea	Sony Pictures	Business
2015a	Data Breach	Hackers/proxies	Ashley Madison	Personal Data
2015b	Cyber Attack	Russian	Ukraine' power grid	State
2016	DNC Hack	Russian Proxies	US Election	State
2017a	Petya Malware	Russia	Ukraine's CII	State
2017b	WannaCry (ransomware)	Hackers	Health Industry	Personal Data (Health)
2017c	Equifax Breach	Hackers	Personal Data	Personal Data (Financial)
2017d	Ransomware 2.0	Hackers	Global Impact	Financial Data
2017e	BadRabbit	Hackers	Russia & Eurasia	S.B.I.
2018a	Hacking and Data Breach	Hackers	MyFitnessPal	Personal Data
2018b	exploitation of SWIFT	Hackers	Mexican banks	Financial Data
2018c	Hacking and Data Breach	Hackers	Exactis	Personal Data
2018d	Hacking and Data Breach	Hackers	SingHealth	Personal Data (Health)
2018e	Hacking and Data Breach	North Korean Hackers	Cosmos Bank, India	Financial Data
2018f	Hacking and Data Breach	Hackers	The Centers for Medicare and Medicaid Services	Personal Data (Health)
2018g	Data Breach	Software Bug	Google+	Personal Data

■ Benchmark cyber incidents

*S.B.I. – State, Business and Individual

* Business – Non-state actors

Source: data collected from various sources and compiled by the Author and developed in consultation with Ph.D. supervisor

In reality, the cyber ecosystem has changed with changes in people living in a natural ecosystem, operations of businesses, functions of governments and future of warfare. After 30 years of destructive war between Europeans, the Treaty of Westphalia was signed in 1648 to neutralise the conflicts. However, religion, commercial interests, territorial rivalries and power politics played a part in those 30 years of unrest. The Westphalia led to the creation of the present day political units recognised in international law - the state was recognised as having sovereignty over territory with full autonomy. In other words sovereignty is linked to territory. The creation of the cyberspace has challenged this classical understanding of state sovereignty as nobody has full power – individual, groups, business, or state in cyberspace. The rising risks in the cyberspace pose a question how this space will be managed?

The first cyber incident that had received the mainstream media attention was the Morris Worm that was created by the graduate student Tapan Morris to understand the extent of the Internet. In due course of time, state involvement and use of proxies has become a phenomenon e.g. 2007 to 2016 cyber incidents (see table 1). Similarly, in 2017 the phenomena had shifted to non-state actors involvements in cyber incidents. Likewise, personal data including financial and health information were frequently targeted by the hackers in 2018.

Technological advancements have questioned the assumption of state, jurisdiction and rules of the cyberspace. Since the emergence of the information age, internet and cyberspace, there is a growing competition between certain countries like US, Russia and China and EU and its Member States to dominant the cyberspace. However the UN has already taken an initiative to build rules for the cyberspace. The “United Nations Group of Governmental Experts on Developments (UN-GGE) in the Field of Information and Telecommunications in the Context of International Security - is a UN-mandated working group in the field of information security. Six working groups were established since 2004. The UN GGE can be credited with two major achievements: outlining the global cybersecurity agenda, and introducing the principle that international law applies to the digital space” (GIP Digital Watch 2018).

To promulgate a state centric oversight on the cyberspace, the Russia in 1998 first introduced a draft resolution in “the First Committee of the UN General Assembly (it was adopted without a vote)” (UNGA 1999). Since then it has been a customary annual report by the Secretary-General to the General Assembly with the views of UN Member States on the issue (UNODA 2017). Furthermore, the Golden Shield Project or the Great Firewall of China, the Chinese internet censorship project that potentially helps it to have cyber sovereignty became significantly a dominant global digital player. The rise of the Chinese internet giants are the example of the growing actors in the cyberspace.

The growing use of technology by people is leading to challenges for the traditional role of the state. Technology is breaking down hierarchies, chains of command and reducing the influence of the state, there by challenging its absolute authority. In the view of this, also the state losing authority in the cyberspace, strong internet censorship laws have come up in countries like North Korea, countries in the Middle East, Latin America, Africa, more recently in India (Indian Express 2016). Thus, states find it very difficult to regulate individual behaviour in the field of cyberspace. In many ways, the cyberspace has undercut both the territoriality and the sovereignty of the state, it is the networks which cut-across all borders and boundaries and including the authority of the state.

The risks in the cyberspace are growing from a simple cyber attack, to theft of digital identity, hacking and digital economic crimes, ransomware attacks, the spread of fake-news. The nature of the growing cyber attacks makes it difficult to immediately identify the perpetrator of such an attack, the gap between attack, identifying the attacker and the response, produces more vulnerability for all systems in a cyber age.

Apart from the financial implications of the cyber attack, there are other costs such as the credibility of the institution, political costs, security costs and military costs in the event of the attack on high profile government websites. Moreover, the financial costs of cyber threats are scaling up swiftly; for instance, cyber frauds in India costs of \$4 billion in 2013 (The Hindu 2013), the cyber attack on Sony studio cost \$100 million (Reuters 2014); the cyber attack on the Bangladesh Bank cost \$ 81 million (Zetter

2016); in 2017 the outbreak of WannaCry ransomware attack cost the world \$4

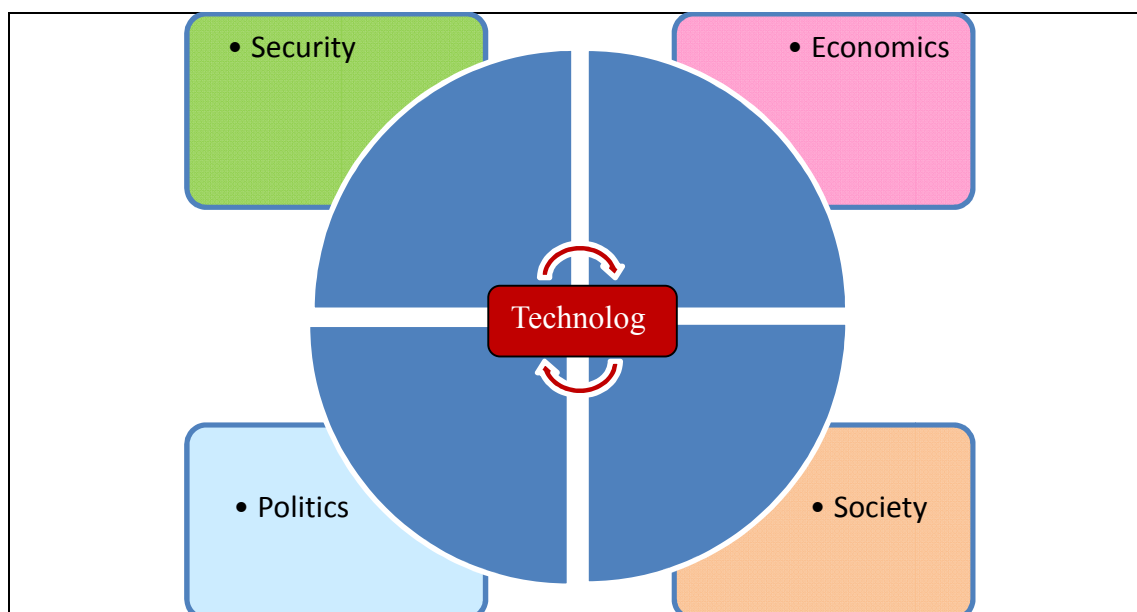
billion. An estimation shows that cybercrime costs the global economy \$450 billion in 2016 (CNBC 2017) and another estimation by Microsoft underlines that economic loss due to cyber crime would reach \$3 trillion by 2020. Thus, a cyber attack/crime has costs and impacts at the political, economic, security, social and individual levels. Cyber attacks/crime is already posing a significant risk to businesses, governments and societies. Given that cyberspace has multiple actors, all the stakeholders need to be brought together to keep the cyberspace stable, open and secure. Transparency, stability, security and openness are four major building blocks of cyberspace and that has to converge.

So far, online service providers and security researchers are able to identify some cyber attacks launched by states or state-proxies. However, more financial, technological investments and collaborations are needed to precisely identify the perpetrator of any cyber attack or crime. Thus, industries, governments and other stakeholders need to show strong commitments to make cyberspace safe, secure and open for all.

CYBER THREATS AND GROWING VULNERABILITIES

The Internet has become an essential and integral part of human life. This emerging complex interconnectedness (see figure 3) has compressed time, space, communication and connection like never before. Technology today transcends geographical frontiers and threats in cyberspace have become more asymmetric, unpredictable and unidentifiable.

Figure 1.5: Complex Cyber Interconnectedness



Source: Author's work developed in consultation with Ph.D. supervisor

Indeed, in the international security landscape for the first time a major cyber security incidents took place from November 2 1988 – May 5 1990 in the US (see table 2.1). Today, when technology has grown by leaps and bounds since the 1988 incident, cyber threats have become much more sophisticated than ever before which needs to be addressed on utmost priority. The act of cyber-criminals is not a soft-act, but in the present context it is [purely] an organised (and individual) act having some specific targets due to the *attractiveness of the target and weakness of defence mechanisms* (Kshetri 2010: 36). The illicit cyberspace users do so primarily to fulfil the economic temptation using such loopholes and gaps. Economic temptations are not the only fact behind these acts but there are some other aspects as well. However, such acts which started just to achieve the economic end, subsequently emerged as the biggest threats to the contemporary international system because of a variety of new modes of attacks, viz. viruses, spam-e-mails, worms, espionages, malwares and ransomwares.

With the advent of digital currency like Bitcoin, cyber criminals had shanged their techniques to target individuals and businesses. Cyber criminals use the dark web and the ransomwares - a type of malicious software to take control over a computer and in order to reasele the computer in return wants to get paid back. They threaten the users

to sell credentials in the dark deep web if they did not get paid.

Table 2.2: Cyber Threats Structure

Actor	Human Security	Economic Security	National Security	Motive	Impact
	Referent object – Individual	Referent object – Business	Referent object - State		
State	Data - Personally identifiable information	Data – Critical Business Information	Data – Strategic Information	Personal/Economical	Individual and Society
State - Business	Fundamental Rights	Information Protection	Critical Information Infrastructure	Financial and Personal/Community	Political and National - I
State - Business	Freedom of Expression	Employee Personal Information	Critical Infrastructure	Political, Technical, Economic and Security - I	Political and National - II
State - Business	Individual Privacy and Intellectual Property Rights	Intellectual Property Rights – innovations and patent rights	Military Information, Technology Transfer and Decision Making	Political, Technical, Economic and Security - II	Global

Source: Author’s work developed in consultation with Ph.D. supervisor

New cyber developments, new cyber risks are creating new fears within states, businesses and individuals. ‘*The cyber state of fear*⁸’ is the interplay between states, proxies and non-state actors and businesses and individual. In a simple explanation, attacking the Critical Information Infrastructure (CII) of another country and spreading disinformation to create violence and fear at the socio-political level can be called a cyber state of fear. Contemporary politics and society relies heavily on the functioning and security of critical infrastructures like water supply, electricity, telecommunications, energy, transport and especially the underlying ICT systems. However, defence networks rely upon different standards and structures, yet it is not free from cyber attacks. The disruption of any of these infrastructures may have serious consequences for the socio-economic and political well-being of the citizens and in a broader sense to the security of a state.

⁸ A term developed by the researcher

The convergence of cyberspace and terrorism is becoming a vital area of global concerns. The term cyber-terror or cyber-terrorism is a combination of two terms cyberspace and terrorism. Although both the terms have been defined already but more specifically cyberspace i.e. virtual world is the metaphoric representations of information in which computer programs function and data moves. On the other hand, the United State Department of State defines terrorism as ‘premeditated, politically motivated violence perpetrated against non-combatant targets by sub national groups or clandestine agents’ (Pollitt 1998).

Cyber-terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs and data which result in violence against non-combatant targets by sub national groups or clandestine agents (Pollitt 1998).

Pollitt (1998) has argued that “the modern thief can steal more with a computer than with a gun. Tomorrow’s terrorist may be able to cause more damage with a keyboard than with a bomb”. Simultaneously, “harmful attacks could be carried out in innumerable ways, potentially by anyone with a computer connected to the internet, and for purposes ranging from juvenile hacking to organised crime to political activism to strategic warfare. The new enemy was neither clearly identified nor associable to a particular state. Hacking tools could easily be downloaded and constantly become both more sophisticated and user-friendly. This diffuse threat-frame and the link to the fundament of society (critical infrastructure) opened the door for turning every small incident into a potential security issue of high urgency” Cavelti (2010: 182). The rise of vulnerability in the cyber domain could lead to a catastrophe across different areas impacting the - state, business, society and individual, therefore, cyberspace has to be secured.

*The cyber state of war*⁹ is based on two scenarios: first scenario (cyberspace is a battlefield) - dooms day imaginations - when fully automated (lethal) machine will takeover in all kinds of warfare. The way states are engaged in research and development to modernise military by using emerging technologies - unmanned systems (UAVs), robotics, autonomous weapon systems, automated disruptive

⁹ A term developed by the researcher

networks and other robust technologies that could potentially spur the future battle ground and warfare. Moreover, cyber manoeuvrability has become an integral part of research & development and policy planning of many states. The USA, the UK, China, Israeli, Russia, Iran, North Korea are among the front runners in this regard where as countries like India, Pakistan, Germany are also likely to join the cyber arms race (see Figure 2.4). For example, researchers have argued that the Estonian attack in 2007 (DDoS attack) and Stuxnet attack in 2010 were less sophisticated and advanced than the Russian cyber attacks on the Ukraine's critical infrastructure in 2015.

The second scenario (cyberspace as a medium) that entails that the future of warfare has already started by one means or the other. The USA and Israeli had used pre-emption cyber strategy in 2010 against the Iran's nuclear ambitions – the Stuxnet attack. The Stuxnet, such attacks have acquired a new dimension altogether, where it is the first instance recorded that the attack was generated from a sovereign state against another in peace time. The scholars termed this act as emergence of *cyber-war* or *cyber-warfare* in international politics. Richardson argued that “conflict in the cyberspace and conflation of all cyber conflict into the language of war poses dangers for the future of the internet” (Richardson 2011: 4). In fact, “after land, sea, air and space, warfare has entered the fifth domain: cyberspace” (The Economist 2010). The term cyber war/cyber-warfare was first used by the Richard A. Clarke in his famous book “*Cyber War*” published in 2010. Most of the scholars have reckoned that cyber-war is mainly a political action of one nation against another. Cyber-warfare is not totally different from information warfare. Information warfare is known to be fought on the fronts of ‘protected information’ e.g. the Wikileaks. On the other side, cyber-warfare is being linked by threats to politics, defence, economics, information systems and critical infrastructures. Both are supplementary and complementary to each other. In conventional warfare, the war normally has taken place in battlefields (i.e. land, water, air and space) but in cyber-warfare, it is not only fought at the virtual domain, but also in the physical domain. It totally changes the distinctions between the hard and soft targets.

International humanitarian law applies as far as conventional warfare is concerned. But in the cyber domain, the absence of policies and law enforcement mechanism at both on humanitarian and legal grounds poses greater challenges. Simultaneously,

there are still some differences between the public and the private stakeholders regarding the different aspects of cyber-warfare.

However, the fear of cyber technologies in future warfare is growing as one state intrudes into others virtual space. The World Economic Forum, a Swiss non-profit foundation has observed ten scenarios of future of warfare – “waging war may seem - “easier”; speed kills; fear and uncertainty increase risk; deterrence and pre-emption; the new arms race is harder to control; a wider cast of players; the grey zone; pushing the moral boundaries; expanding domains of conflict; what is physically possible becomes likely” (Kaspersen et.al 2016). By the means of cyber warfare, for example, an attack can achieve its political and strategic goals without any bloodshed as in a conventional warfare and thus, the security and governance of the cyberspace is becoming a paramount concern.

CYBERSPACE: SECURITY AND GOVERNANCE

“Cyber security, as a concept arrived in the post-Cold War agenda in response to a mixture of technological innovations and changing geopolitical conditions” (Hansen and Nissenbaum 2009: 1155). On the cusp of the fourth industrial revolutions, cyber security debates have taken a new shape. Emerging technologies such as IoT, Big Data, and AI are altering the traditional notion of cyber security. The impacts of new technologies are today challenging traditional doctrines and war strategy and the rules of engagement are changing between states and non-state actors. Cyber threats are located in the non-traditional threats landscape and states today have started to monopolise, manoeuvre, mechanise and control their digital space. In addition, with the growth of new emerging technologies and the rise of tech giants, there is a growing concern they can manipulate and are also lobbying to influence the international legal order.

Scholars have argued that the cyberspace is becoming more vulnerable because the domain itself is prone to threats. Lallana and Uy (2003: 29) opined: “cybersecurity is about combating threats and crimes in cyberspace. It includes passing appropriate laws and policies as well as developing capabilities and institutions to prevent fraud and fight threats”.

According to Hathaway, cyber security “tension is further exacerbated by the competition for resources, lagging policy implementation and an ill-defined technology roadmap to address security shortfalls as we adopt and embed the next-generation technology into our infrastructures and enterprises” (Hathaway 2012: 72). Nye (2011: 20) has elaborated that “the cyber-domain is a volatile manmade environment. [...] (the), “people built all the pieces,” but “the cyber-universe is complex; well beyond anyone’s understanding and exhibits a behaviour that no one predicted, and sometimes can’t even be explained well”. The very nature of cyber security entails two things - *unpredictability and vulnerability*.

Securing cyberspace has become a much needed element for individual well-being as well as for the state and business security. Tikk (2011) has argued that ten rules could be followed for cyber-security:

The Territoriality Rule - information infrastructure located within a state’s territory is subject to that state’s territorial sovereignty; *The Responsibility Rule* - the fact that a cyber-attack has been launched from an information system located in a state’s territory is evidence that the act is attributable to that state; *The Cooperation Rule* - the fact that a cyber-attack has been conducted via information systems located in a state’s territory creates a duty to cooperate with the victim state; *The Self-Defence Rule* - everyone has the right to self-defence; *The Data Protection Rule* - information infrastructure monitoring data are perceived as personal unless provided for otherwise; *The Duty of Care Rule* - everyone has the responsibility to implement a reasonable level of security in their information infrastructure; *The Early Warning Rule* - there is an obligation to notify potential victims about known, upcoming cyber-attacks; *The Access to Information Rule* - the public has a right to be informed about threats to their life, security and well-being; *The Criminality Rule* - every nation has the responsibility to include the most common cyber offences in its substantive criminal law; *The Mandate Rule* - an organisation’s capacity to act (and regulate) derives from its mandate (Tikk 2011: 121-129)

The cyber security threats are profoundly challenging both developed and developing countries. Thus, there is a need for comprehensive and “balanced view to recognise that there is a cyber-threat, but neither under-estimate nor over-hype the problem” (Giampaolo Di Paola 2012: 58) because, cyber security “requires coordination between governments, regional, and international organisations, the private sector and

civil society” (G8 summit 2011). In fact a comprehensive approach is needed to address the threats no matter how they emerged and through whatever source (economic or political or security or social reason). All these factors play a key role in cyber debates around the globe. Securing the cyberspace has to be done at different levels and also bringing in different approaches and having a large multistakeholder perspective. One can broadly divided in to four initiative – *State, Intergovernmental, Multilateral, Multistakeholder/Industry*:

State Initiative - Although, state has less control over most aspects of the cyberspace, it became customary for the state to issue and endorses various principles, to create a monopoly, impose sovereign rights to control digital space on their territory. Almost all major states are involved in cyber activities – US, Russia, France, UK, Germany, EU, China, Brazil, India, South Africa and Nigeria have put forward their respective cyber strategies and in investing in various programmes to secure their cyber space. While taking cautious note on new developments, the Chinese government’s Cyberspace Administration of China and People's Government of Zhejiang Province has been convening the World Internet Conference/ Wuzhen Summit since 2014. Similarly, in November 2018, the French government signalled for an overambitious agreement on cyberspace i.e. the Paris Call for Trust and Security in Cyberspace. It has received positive response from the EU and tech giants like Facebook and Microsoft, but countries like US, Russia and China have not shown willingness to sign it yet.

Intergovernmental Initiative – In the aftermath of the 2007 Estonian cyber attacks, NATO first created the Cooperative Cyber Defence Centre of Excellence (CCDCOE) 2008 in Tallinn. In addition, NATO also came out with the Tallinn Manual 2013 (Tallinn Manual on the International Law Applicable to Cyber Warfare) and Tallinn Manual 2.0, 2017. This Manual is based on the NATO convening an academic and non-binding study on *jus ad bellum* and how international law applies to cyber conflicts and cyber warfare. The Tallinn manual is based on the NATO

Multilateral Initiative – At the UN, for the first time in 1998, Russia took the lead to adopt a resolution on the role of ICT on international security. That was the first and one of the significant steps to shape cyber norms. Moreover, again in 2003, Russia

proposed the establishment of the UN – Group of Governmental Experts (UNGGE) to deal with information security and cyber norms. The UNGGE met several times between 2004 till the end of it in 2016/2017. In the final meeting, it left the international cyber norms debates unresolved. There are two reasons for this, first, the ideas proposed by Russia were never approved and endorsed by the US. Second, the US does not want to reduce its sphere of influence by letting multilateral forums like the UN to set or create cyber security norms.

Multistakeholder/Industry Initiative - In the last few years, Microsoft has shown keen interest to reaching out to promote its ambitious project i.e. the Digital Geneva Convention, to protect the cyberspace. The aim is to create a legally binding framework to ‘govern states behaviour’ in the cyberspace. Although it received positive appreciations from the western business communities, it failed to impress others. Historically, since states are the legitimate actors in who create international legal standards, fact remains to be seen how tech companies (Microsoft) led initiatives will replace or complement or supplement decisive role of the state in the area of international cyber regulation. In April 2018, technology giants came together to sign the ‘Cybersecurity Tech Accord’ led by Microsoft and Facebook, a non-partisan initiative by business and digital service providers to address cyber attacks while improving security, stability and resilience of the cyberspace.

However, data being a critical asset (security and governance) to the cyber ecosystem, there has been no effort to create a global binding treaty or convention on data protection to oversee the act of the states or businesses. Growing technical, political, economic, legal and social concerns over data protection necessitates a comprehensive approach from state, business and other stake holders.

CONCLUSION

Former US Federal Communications Commission Chairman, Julius Genachowski (2009-2013) once said that “if you shut down the Internet today you would shut down our economy”. That’s both the good news and the bad news”. In other words, the internet has become, the connecting link between the state business and people and that is why, coordination, cooperation, regulations, due diligence is the need of the hour.

Cyber-threats are asymmetric threats to national security, which can in innumerable ways impact the security landscape. Cyber-crime is closely associated with the economic and social aspects of the victim who would face digital financial and identity thefts. Cyber-warfare is an act motivated by political reasons in which the agents of cyber-warfare [like Stuxnet] are used to carry out the goals. Cyber-terrorism although is yet to make a radical geopolitical appearance, but undeniably, different terrorist organisations are converging in the cyber domain to fulfil their goals - recruitment, fund raising, online training and so on.

The issue related to the data protection in the cyberspace includes two way strategies: first, security of national and business assets and second, the safety of privacy and freedom of expression. In fact, the problem is not with the internet (cyberspace) but with the people, as the old saying goes 'you only get out what you put in'.

Cyberspace has an overarching influence on technology, state and security. Emerging technological innovations are purely data driven in which machine would overtake both the man and machine. Data biases required significant attention from the government and industries, pure data will lead to noble data driven cyber world. As the cyber technologies are also challenging the territorial limitations that further encourage the nation states to espouse the virtual space as theatre of their operational activities. Growing state engagement in the cyberspace (offensive and defensive) without legal and political restrictions is multiplying the vulnerabilities and also impacting the global security landscape. To address newly emerging threats all stakeholders in the cyber-domain, thus, need to have a proactive rather than a reactive approach.

Moving on from the examining the cyber domain, the next two chapters examines in detail the role of two significant actors - the EU and the US approach to cyber security.

CHAPTER 3

THE EUROPEAN UNION'S APPROACH TO CYBER SECURITY

“Data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well being of individuals”

(Directive 95/46/EC, Para. 2)

INTRODUCTION

As a prominent global economic power, the European Union has completed 60 years. The shadow of past and uncertainty of the future have often raised the prospects of imbalance to its quest for a peaceful world order.

There were the people in the past who had a vision for the future. In the Post-World War II period - three great men: notably first Chancellor of Federal Republic of Germany (West Germany) Konrad Adenauer, the Luxembourg-born, Christian Democratic French statesman Robert Schuman and the Italian Prime Minister, Alcide de Gasperi; three close friends: Belgium, Luxembourg and the Netherlands (Benelux); and the influential economist: Jean Monnet were able to overcome Europe's historical division to create a new European order, although only in the Western part. One of the greatest and finest diplomats of modern world international politics, Henry Kissinger narrated that “France and Germany, the two countries whose rivalry had been at the heart of every European war for three centuries, began the process of transcending European history by merging the key elements of their remaining economic power. In 1952, they formed the Coal and Steel Community as a first step toward an ‘*ever closer union*’ of Europe's constituent peoples and a keystone of a new European order” (Kissinger 2014: 88). Integration of coal and steel industries were meant to stop war machine to regain its power, because they had traditionally been the key drivers of national war machine (EC 2002).

From being at the centre of world politics, the European landmass had paid a heavy price to their ignoring history - the two devastating World Wars in a span of 20 years led to the demise of European power structure and transformed the global order. The end of the Second World War, 1945 also led to the process of regional integration in Western Europe. The birth of a peace process in Western Europe led to the genesis of

a new identity due to economic cooperation that resulted in a spill-over effect in all dimensions: social, political, security and cultural. The process of remaking Western Europe was done by subduing nationalism and moving beyond the principle of sovereignty and modernity to sharing sovereignty and post modernism. This would subsequently give birth to the EU as a post-modern actor.

These factors sought to create economic cooperation and to harmonise the war industry (i.e. Coal and Steel which had played a decisive role in the war), and to reconstruct peace in the western part of the continent. The economic cooperation further intensified in 1957 by the signing of the Treaty of Rome that led to the creation of the European Economic Community (EEC) – it was the documentation and creation of European values – “common values, common goals, common standards and common policies developed together, leading to the emergence of a stronger union between Europeans” (EU 2017b). By 1970, a new incremental growth took place in the institutional structure i.e. European Political Cooperation (EPC) which added the political agenda to the process. The end of the Cold War in 1990 with the reunification of Germany would lead to further vertical and horizontal integration and the growth in the members of the European Union.

The Maastricht Treaty 1992, Amsterdam Treaty 1997, Nice Treaty 2001 and eventually the Lisbon Treaty 2009 have ushered in a new actor at the European and global level. In 1992 the Maastricht treaty had entered into force and put in play a new paradigm in Europe. This emergence of the EU as a closer political union and its transformation as an actor in intentional politics captured by Bava (2008):

“the European Union emerged as a larger political actor in 1992 after the Treaty of Maastricht ... These efforts by the EU at further institutionalization and attempts to forge a common political voice are part of a series of endeavours aimed at shaping and strengthening its political identity. The EU is no longer merely a trading entity and regards itself increasingly as an important and significant political player at the global level. The process of creating a new identity in the EU is taking place at multiple levels – economic, political, strategic and legal” (Bava 2008: 233).

Thus the nature of the European peace project gradually changed over time and it took more than a decade for the EU to assume the status of a full-fledged security actor. The Amsterdam Treaty of 1997 brought many changes to the integration project this

can be grouped them into four areas: the free movement of persons; internal security; the external action of the EU; and the institutional issues (Piris and Maganza 1998: 36). The treaty initiated a process of ‘communitarising’ (Piris and Maganza 1998: 36) the Justice and Home Affairs (JHA) policy area, particularly in relation to the immigration and border control matters and simultaneously brought important innovations in the field of Common Foreign and Security Policy (CFSP). Subsequently, it recorded an unprecedented development in the field of security. The European Security and Defence Policy (ESDP) saw EU’s involvement in two small-scale operations in 2003 (in Macedonia and the Democratic Republic of Congo) and policing operations in Bosnia-Herzegovina (Bretherton and Vogler 2006) (Archer 2008: 91). The Lisbon Treaty further intensified the Union’s role in international affairs and global security issues – that is based on stronger multilateral cooperation and good global governance viz. addressing issues through ‘effective multilateralism’ (Lundin 2012: 26).

At the policy level, the European Security Strategy (ESS 2003) indeed had provided the Union with the needed roadmap to address the geopolitical turmoil. In the 2008 review, cyber-crime was added as an additional threat to national security. To have a comprehensive approach to address various issues of digital world and cyber threats, the Union in 2013, released its first ever Cyber Security Strategy. To make the digital world safe and secure and to protect the fundamental rights and personal freedom of any individual, in 2018, the EU adopted the General Data Protection Regulation (GDPR). The GDPR also intended to strengthen and unify data protection for all individuals, within the EU. By releasing EU Global Strategy in June 2016, the EU High Representative Federica Mogherini has indicated further its ability and intentions to address global threats in a complexly interconnected and multipolar world order. Before going into a detailed analysis of the EU’s policy on Cybersecurity, it is necessary to briefly outline the contexts and emergence of the EU as a security actor because that prepared the EU to take a proactive move in a new security landscape.

THE EMERGING SECURITY LANDSCAPE OF EUROPE, 1990-2001

Global geopolitics faced a major shift from 1990-2001. The end of the Cold War saw the disintegration of the USSR that created a new geopolitical and geo-economic landscape across the continent and Central Eastern Europe and in the former space of the Soviet Union. Simultaneously, the Balkan War in Europe and the First Gulf War in Asia unfolded a ‘threat of uncertainty’ (Kavalski 2005: 150), and the diffusion of threats brought attention towards the non-traditional dimensions of security and to rise of ‘new wars’ (Kaldor 2013) in the region. The ‘changing patterns of conflict’ (Newman 2004: 173-74) had brought in new threats along with the dissolution of Yugoslavia and the subsequent wars during 1991-1995, and “the Western Balkan states became Europe’s *Achilles’ heels*, revealing the EU’s inability to act decisively in periods of crisis” (Turhan 2011: 3). He further argued that the crises in the Western Balkans during the 1990s proved to be a catalyst for a plethora of changes within the EU. After those crises came to an end, there was a widespread belief even among the EU policy makers that Europe could do better (Turhan 2011: 3). This was the first instance after the Cold War wherein the Union was directly involved in crisis management. Lack of past experience and expertise brought handful of criticisms to the EU’s involvement particularly and NATO in general. During this period a huge amount debate and differences of opinions rose within the EU.

Chris Patten, the then EU Commissioner for External Relations:

Europe completely failed to get its act together in the 1990s on the policy for the Balkans. As Yugoslavia broke into bits, Europe was largely impotent because it was not united. Some member states wanted to keep Yugoslavia at all costs, some wanted to manage its break up, and others still felt we should stay out of the whole mess... We had to do better. A lot better (Patten 2004: 2).

Nevertheless, the EU had witnessed three major wars in the Balkan region in less than a decade. But, these geopolitical changes at its doorsteps had a spill-over effect on the structure of the Union. “New-threats with new trajectories had entered into the domain of the EU, with diffuse threats viz. migration influx, economic burdens” (Turhan 2011: 4). Thus, the end of balance of power system on the one hand created a power vacuum and on the other hand had altered the nature of threat assessments.

The power vacuum led to the emergence of ‘the unipolar moment’ (Krauthammer 1990a) in global power politics. This unipolar moment was crucial for future of global

security landscape. After the demise of the Soviet Union, the bipolar world was dead. The multipolar world was struggling to be born but the instant scenario was a moment of unipolarity (Krauthammer 1990a). During this particular period no other country had matched with the American pre-eminence in the “military, diplomatic, political and economic assets to be a decisive player in any conflict in whatever part of the world it chooses to involve itself” (Krauthammer 1990b). Likewise, the US involvement in the First Gulf War had revealed the huge gap between the military might, technological manoeuvrability and economic strength and that of other states. The significant influence of the US over global politics made the then Foreign Minister of France Hubert Vedrine to define it as a ‘hyperpower’ (NYT 1999).

During this period, there were also transformations in the Union, which would enlarge its borders and in that way added to a new security landscape for Brussels. On the one hand, with the collapse of communism across Central and Eastern Europe it paved the way for the EU enlargement and on the other hand it also brought the EU both on its Eastern and Southern flank closer to conflicts zones. The ‘Maastricht Treaty’ 1993 and the Treaty of Amsterdam 1999 paved the way for both horizontal and vertical changes within the Union. The formalisation of the European Single Market granted ‘four freedoms’- movement of goods, services, people and money. A true sense of Europe without frontiers emerged. In 1993, the Union has adopted the Copenhagen Criteria to add normative value articulation to the process of enlargement. It laid out the criteria that membership of the EU is open to any European country but it must satisfy – “*political criteria*: stability of institutions guaranteeing democracy, the rule of law, human rights and respect for and protection of minorities; *economic criteria*: a functioning market economy and the capacity to cope with competition and market forces; *administrative and institutional* capacity to effectively implement the *acquis*¹⁰ and ability to take on the obligations of membership” (EC 1993). In 1995 Austria, Finland and Sweden formally joined the Union, it now covered almost the whole of the Western Europe. Similarly, internet and mobile technologies also became a part of this transformation by changing the way millions of European youth communicate. The end of the Cold War had led the emergence of new threats in the Continent. Within the overarching Cold War framework, there was a *well-defined and*

¹⁰ The *acquis* is the body of common rights and obligations that is binding on all the EU member states (EC 1993).

identifiable threat to the European security landscape (Bava 2007: 99). Economic, social, environmental, cultural, political issues shaped the security discourse within the Union from 1990-2000. The 9/11, incidents impacted the US regional and global security landscape as terrorism became the top most threat to all countries. This critical scenario, both at the global and regional levels enabled the EU to manifest its own strategy to mitigate the wide variety of threats. However, divergence had originated between the Atlantic allies due to the overwhelming unilateral approach of the US towards Iraq in 2003.

THE EVOLUTION OF THE EUROPEAN UNION AS A SECURITY ACTOR

This horizontal and vertical makeover of the EU has been articulated by many academicians and researchers emphasising different policy aspects of the Union and also as a security actor. Robert Cooper (2003) opined that ‘the EU is a post-modern system’; and for Renard it is a ‘fledgling actor with limited capabilities and strategic clout’ (Renard 2014); and Rieker (2007: 5) argued that “If the EU is to be perceived as a credible security actor, it also needs a certain degree of political and administrative capabilities”. While assessing the EU’s norms and power, Zielonka (2008) argued that ‘the EU is a peculiar international actor’; and for Ian Manners ‘the EU is a Normative Power’ (Manners 2006), form a deepening and widening security studies perspectives “...the EU’s security actorness from a traditional perspective can lead to the conclusion that the EU is an underdeveloped security actor, considering its relatively weak military capabilities. A broader understanding of security, on the other hand, can help to better our understanding of the comprehensive nature of the EU’s security actorness” (Zwolski 2009: 92). The incident of 9/11 had demonstrated that “possession of the greatest military might on earth, including the most advanced technology, cannot by itself guarantee security” (Biscop 2004: 10). Thus, for a country to mitigate the *complex problems*, a greater cooperation with a good strategy is needed.

Table 3.1: The EU and Security Actorness

Year	EU Treaties and Events	Security Aspect	Outcomes
1992	The Maastricht Treaty	Creation of CFSP	Creation of the EU as a Security Actor
1992	Petersberg Tasks	Humanitarian and rescue tasks; Peacekeeping tasks;	Building of the security mandate of the EU

		Tasks of combat forces in crisis management, including peacemaking	
1995	Dayton Agreement	Peace and Stability in Bosnia and Herzegovina	End of Bosnian War
1997	The Amsterdam Treaty	High Representative (High. Rep.) of the Common Foreign and Security Policy	To represent the EU as a Security Actor at the global level
1998	The Saint-Malo Declaration	Anglo-French security capacity building	Building the EU capacity for autonomous decision making and use of military force
1999	The European Council meeting in Cologne	Consensus on to enhance capacity in autonomous action in order to respond to international crisis without prejudice	Javier Solana designated as the first High. Rep. of the CFSP
2000	Treaty of Nice	Amendments to Treaty on European Union	EU enlargement in 2004
2002	The Berlin Plus Agreement is signed between NATO and the European Union	NATO-EU security management – assets made available for the EU in crisis management operations	Capacity Building of the EU
2003	European Security Strategy	The EU identified five major non-traditional threats to security	Terrorism, Proliferation of Weapons of Mass Destruction, Regional Conflicts, State Failure and Organised Crime
2004	The European Defence Agency	Defence integration among Member States	European Defence
2008	Review of the ESS	Addition of New threats to NTS	Cyber Security and Climate Change
2009	Lisbon Treaty	Unified and Strong Union	Creation of the EEAS and the office of the High Representative
2016	EU Global Strategy: Council conclusions on security and defence	EU approach to global security	EU became a Global Actor
2017	The Permanent Structured Cooperation (PESCO)	Enhancing European defence cooperation	Common European Defence apparatus

Treaties,
 Strategies,
 Agency,
 Projects,
 Meeting and Agreements

Source: Author's work developed in consultation with Ph.D. supervisor

The beginning of the EU's actorness can be traced back from the Maastricht Treaty, and, the Anglo-French security declaration of 1998 was a milestone in the history of the construction of the Union's security actorness. This created a mandate to enhance the EU capacity for autonomous decision making and use of military force in the absence of NATO deployment. In 1999, the EU acquired a visible face to showcase its foreign and security policy of the EU, in the form of Javier Solana, who was designated as first High Representative of the CESP. Five years after the Dayton Agreement was signed in 1995, the EU was taking the first steps to become a security actor.

The 9/11 terrorist attack on the US would made a significant impact on global and regional security landscape. Ten years, after the end of the Cold War, worlds leading power was attacked by non-state-actor. It drew attention, to the rise and capabilities that terrorist groups had acquired. It also underlined the fact that, the non-state-actors were going to play a significant role on the security landscape and people, states and businesses are going to experience increasing vulnerability from these new kinds of threats. This requires leadership from, state and at the political level to respond to the new security challenges. It is in this backdrop that, the 2002, agreement was a step forward for the EU's own visibility as it could use NATO assets for Crisis Management Operations.

Simultaneously, the US came out with its National Security Strategy at the same time. However, 2003 saw lot of divergence between the EU and US on the issues of pre-emptive warfare in Iraq. France and Germany two major EU countries did not support the 2003 American intervention in Iraq. It is in this backdrop, Javier Solana was asked by the Council to develop a response to which would take the shape a European Security Strategy (ESS) that was adopted by the EU in December 2003. The ESS aimed at framing or structuring a pan-European mechanism with global applicability. The ESS stated that geopolitics in the 21st century is as critical as was before, whereupon "no single country is able to tackle today's complex problems on its own" (ESS, 2003: 1). Furthermore, it pointed out five key threats to security: "Terrorism, Proliferation of Weapons of Mass Destruction, Regional Conflicts, State Failure and Organised Crime" (ESS 2003).

A wide range of geopolitical turbulence, exogenous shocks (Kaunert and Leonard 2012) and incremental growths in the EU had led to new security paradigm for the region, which was clearly outlined in the 2003 security strategy - A Secure Europe in a Better World. The ESS underlined the fact that “the world is full of new dangers and opportunities” (ESS 2003: 14), and advocated using “effective multilateralism” to address new threats. The ESS briefly outlined three techniques to address the non-traditional threats: first, “identifying the threats; second, have a strategic objective of addressing the threats through the international order based on effective multilateralism, simultaneously building security in [our] neighbourhood (which was later manifested in the EU Neighbourhood Policy)” (ESS 2003). One could say that the EU as a security actor was putting forward through the ESS to become more active, capable actor which could respond to crises and threats in a coherent manner..

The ESS also emphasised the fact that “in an era of globalisation, distant threats may be as much a concern as those that are near at hand... the first line of defence will often be abroad... the new threats are dynamic... conflict prevention and threat prevention cannot start too early” (ESS 2003: 6). Thus the EU emphasised on the need to develop a “*strategic culture* that fosters early, rapid and when necessary, robust intervention” (ESS 2003: 11). Nearly a decade after the EU came into being and the post Cold War period experienced a shift in the security landscape in 2001, the Union launched its security strategy in 2003. For the first time, the EU had clearly identified the threats, indicated it would use a multilateral framework to address them along with global partnerships. This was another steps to the EU’s growth as a security actor.

But the strategy has been criticised both by scholars and practitioners. According to one criticism, “a strategy document is not the same as having a strategy” (Shapiro and Bindi 2010: 343). Second, the formulation of a security strategy is (or should be) “a political process, an effort to build consensus around a broad approach to securing a polity’s interests” (Shapiro and Bindi 2010: 343). Third, it is the result of a “political negotiation”, not the “impetus for a strategic change” (Shapiro and Bindi 2010: 343). Last, but not the least, the EU lacks the “institutional infrastructure to carry out such a process” (Shapiro and Bindi 2010: 343).

The scope of the EU as an actor was transformed due to the, the big bang enlargement of the Union in 2004 which added ten new members¹¹, majority of them being Central and East European countries¹². The new borders of the EU on the eastern side brought it closer to Russia as its immediate neighbour.

As consequences of the some of member states participating in US's War on Terror, there were repercussion on Europe as well with the terrorist attacks in Madrid (2004) and London (2005). The rise of terrorism and use of cyberspace for radicalisation did not become a part of the threat perspective immediately. Cybersecurity per se was not the pressing issue for the EU until the DDoS attack on the Estonian cyberspace 2007. During that period, EU's emphasis was on other issues like democratisation, peace building and economic stabilisation, and simultaneously preparedness for tackling terrorism, migration, organised crime (women trafficking, drug trafficking, arms trafficking and money laundering) and other crises were the prime areas of concern. The five threats identified by the EU were based on the preceding events, this is why, in the ESS review 2008 security became important given the enlargement of the EU and the changing threat perceptions both internally and externally at the regional and global level.

The review of the ESS was a response to the changing security landscape. The report on the implementation of the ESS in 2008 said that "globalisation has brought new opportunities [...] but (it) has also made threats more complex and interconnected". In addition, it identified more threats to Europe, viz. "illegal immigration, piracy, Information Security and ecological problems". Moreover, it gave specific place to cyber security, which was added to the security strategy for the first time:

Cyber security - Modern economies are heavily reliant on critical infrastructure including transport, communication and power supplies, and also on the Internet. The EU Strategy for a Secure Information Society adopted in 2006 addresses internet-based crimes. However, attacks against private or government IT systems in EU Member States have given this a new dimension, as a potential new economic, political and military weapon. More work is required in this area to explore a comprehensive EU approach, and to raise awareness and enhance international co-operation (Report on the implementation of the ESS 2008: 5).

¹¹ Cyprus, the Czech Republic, Estonia, Hungary, Malta, Latvia, Lithuania, Poland, Slovakia and Slovenia

¹² The Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Slovakia and Slovenia

It is quite obvious, that the EU added cyber-security in the agenda, because the review report came after the major attack on Estonia and equally after the Central and Eastern European enlargements of 2004 to 2007. The report underlined some important areas and mechanisms to fight against cyber-crime, viz. comprehensive EU approach, awareness both globally and locally, and international cooperation. Since 2008, the debate on cyber-security has been vigorous in the European countries. During 2007-2009 significant amount of statesmanship and diplomacy was involved to make the Lisbon Treaty happen, also on the backdrop there were debates held in Tampere, Hague and Stockholm to address the internal security issues. And “with the Lisbon Treaty in place, new provisions sketching out further ambitions and a ‘communautairization’ of internal security policymaking added to what could be categorized as a growing degree of strategic content in the area of EU internal security cooperation” (Bossong and Rhinard 2013: 46). The Lisbon Treaty further enhanced the EU's role in political, economic, military and security actor. After the failure of the constitutional convention the EU was back to building a stronger identity as an actor. It created greater visibility to for the office of the High Representative of the Union for Foreign Affairs and Security Policy who also had *double hatted functions* Vice President of the Commission and also created the EEAS. The first High Representative was Catherine Margaret Ashton and the currently the office is held by Federica Mogherini.

Simultaneously, the EU also launched its Internal Security Strategy (EUISS) in 2010 which identified “*organised crime, terrorism, cybercrime, border security and disasters*” (EC 2010b: 2) as new threats and it proposed specific action. The EUISS identified “five strategic objectives, with specific actions for each objective, for overcoming the most urgent challenges in order to make the EU more secure - “1. Disrupt international criminal networks; 2. Prevent terrorism and address radicalisation and recruitment; 3. Raise levels of security for citizens and businesses in cyberspace; 4. Strengthen security through border management; 5. Increase Europe’s resilience to crises and disasters” (EUISS 2010 in EC 2010b).

The fundamental aim of the strategy was to create a resilient internal security mechanism through “identification, prevention, securitisation of business and borders from transnational threats”. The EUISS has shown a desire to create ‘commonness’

within and among the Member States. It also symbolises the renewed interest of the Union both and established the link between the external and internal threats. Moreover, it has also strengthened the Area of Freedom, Security and Justice (AFSJ). The AFSJ is the significant internal security component to protect the borderless EU. It has the mandate to ensure security and free movement within the Union. It covers large policy areas – “management of EU’s external border, judicial cooperation in civil and criminal matters, police cooperation, asylum and immigration policies, fight against crime (terrorism, organised crime, cybercrime, sexual exploitation of children, human trafficking, illegal drugs etc)” (EC 2018b).

The period also witnessed global recognition to the EU’s normative power, which also shaped its global security actorness. By endorsing democracy as organising principles of politics, the EU has shown its normative approach to address the Arab Spring. Subsequently, the then President of the European Council, Herman Van Rompuy in his address to the United Nations General Assembly in 2011, spoke of the international community’s “responsibility to assist” Libya with political transition (EC 2011). The EU’s growth as a regional actor was recognised in 2012, by the award of the Nobel Peace Prize. The citation recognises the EU’s contribution over six decades “to the advancement of peace and reconciliation, democracy and human rights in Europe” (Nobel Prize 2012). However, the EU’s efforts to address the crisis in the neighbourhood did not draw much result during the 2014 Ukrainian crisis when Russia annexed Crimea. Rather this highlighted not only the EU but also the US were unwilling to take any military action against Russia and prefer using sanctions to target Moscow. The changing security landscape was addressed two years later in the European Union Global Strategy (EUGS) launched in 2016. The release of the 2016 EUGS came after the Brexit vote that has long term implications for the EU as a security actor, more so in a security terms as Britain exits would result in the loss of one the key permanent UNSC member and nuclear member as well. Federica Mogherini, High Representative of the Union for Foreign Affairs and Security Policy, Vice-President of the European Commission, while forwarding the EUGS 2016 said that the EU and World are at the crossroads of new challenges.

The crises within and beyond our borders are affecting directly our citizens’ lives... what our principles, our interests and our priorities are. This is no time for uncertainty: our Union needs a Strategy. We need a shared vision and common action (EC 2016c).

She has also underlined that “none of our countries has the strength or the resources to address these threats and seize the opportunities of our time alone” (EUGS 2016). A little over a decade, not only the EU had grown as an actor, but there was also a change in the security landscape. The 2016 EUGS also showcased that the EU was expanding its scope and area as a security actor from the regional to the global.

THE EUROPEAN UNION AND CYBERSPACE: DIGITAL CONNECTIVITY, VULNERABILITY AND REGULATION

The Maastricht Treaty 1991 enhanced the political cooperation and paved the way for the EU as a political, social, economic and security actor. At a fundamental level the EU has been a place of building peace, security, and prosperity. Similarly, economic activities have been crucial to the identity of the EU from 1957, Treaty of Rome. With the adoption of ICT and the growth of the digital economy, the adoption of the Digital Agenda for Europe in 2010 and Digital Single Market 2015 policy is now transforming the EU as a Digital Union. Cyberspace is not only changing the security landscape of states and business within the EU but also enhancing its influence in global security landscape. It is driving economic behaviours and altering the trading patterns. Unlike any other revolutions, which were influenced, concentrated, created on a particular geography in a linear way, the cyber-revolutions are ‘nonlinear revolutions’ which are not situated in a particular geography.

The EU has gradually enhanced its sphere of influence on – economy, politics, security, society and cyberspace. The socialisation of the Internet in early 1990s [here socialisation indicates the development of the World Wide Web (WWW) and its cornerstone Hypertext Markup Language (HTML) to create web pages and web applications and opening of the Internet for private companies and public usages] was originally started in Europe and that created various opportunities and challenges to the Union both in promoting new innovations and balancing individual privacy and national security debates of the Member States. That was the time when the Cold War tensions were high on the agenda and the formation of the EU was still in the process. However, the European Organisation for Nuclear Research (CERN) based in Switzerland developed the World Wide Web.

The digital image of Europe in 2000, was totally different from 1990, almost every Western European country has recorded 30 percent of individuals using internet by rapid internet penetration (see table 3.2). And by 2007 (one of the benchmark years for cyber security discourse), out of EU – 27 (and UK) only 6 countries (see table 3.2) have recorded less than 50 percent and less than 40 percent in 3 countries of individuals using internet, while in other countries the percentage was above 60 percent and the all of the Western European countries recorded just higher than the percentage of the US (see table 3.2). The figures for 2017, shows that out of 500 million population of the EU, 83 per cent of them (and counting) are internet users and about 48.8 percent Facebook subscribers (Internet Live Stats 2018). The rapid growth of digital technology has transformed life in all spheres from economic activity to social connectivity and political influence to military modernisation as well.

However, to secure the information age and to address the internet based crime issues, some kind of a *de facto* debate had taken place within the newly formed EU in 1992, but it was largely around the protection of E-commerce. A European Initiative on Electronic Commerce was adopted in 1997, which was formally implemented in 2000. It primarily puts stress on the growing importance of the Internet Business (i.e. the electronic commerce). It stated that, “the global electronic commerce market is growing extremely fast and Internet Commerce could be worth European Currency Unit 200 billion by the year 2000. 86 million people were connected to the Internet worldwide by the end of 1996, and by 2000, [it was] expected to reach 250 million individuals” (European Commission 1997). This was based on a four pronged agenda: “widespread affordable access to the infrastructure; coherent regulatory structure based on Single Market principles; skill promotion and awareness to create favourable business environment and compatible regulatory framework at the global level” (EC 1997). The EU’s has stood for a secure, open and regulated digital union.

All these debates of that period were heavily influenced by the disruptive technology – credit card – because “consumers around the world enthusiastically adopted [this] disruptive new technology to streamline commerce and made it possible for ordinary people to do things that, until then, only businesses and large organizations could do” (Mundie 2014: 29). It is the first instance of the diffusion of an “economic class

structure” by disruptive innovations. The rapid European, American and global adoption of cards (credit and debit) empowered the common people, produced large sets of data for the companies (use and misuse) and also allowed criminals to get benefit. With the advent of internet, all these information which is also called as data, are easily transported beyond the territorial jurisdiction of the EU and the MS.

Already in 1980, the Organization for Economic Cooperation and Development (OECD), outlined a set of comprehensive data protection and privacy guidelines for Europe and US. This was the first instance when the issues of ‘information/data protection, cross border data flow and individual privacy’ were discussed at the European policy level. The recommendations of the Council of Europe on Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data in 1981 “directed the companies on the proper way to collect and retain personal data, ensure its quality and security, and provide meaningful opportunities for individuals to consent to the collection and have access to the data collected about them” (Mundie 2014: 29). This move by the OECD also encouraged individual member states to create their own data protection regulations. However, after the formation of the EU, Brussels adopted a directive in 1995 (Directive 95/46/EC in 1995) on the protection of the individual privacy, data protection and free flow of cross border data within and outside the EU. This would be the first step by the EU to create a policy framework that addressed digital economy, connectivity, data protection, privacy and vulnerability with in a specific regulation.

For an economic actor like the EU to think in terms of economic security (data protection) and social security (individual privacy) in the realm of virtual world comes as no surprise. Due to easy accessibility and convenience, the adaption of the e-commerce had posed questions to international arbitration laws offline and virtual world (Biukovic 2002: 319-320).

In 2000, David Byrne, the then European Commissioner for the Health and Consumer Protection in his speech at the Kangaroo Group, Conference: Barrier in Cyberspace, 2000 emphasised that “B2C (business to consumer) [trust] is an important aspect in e-commerce. Thus, public policy needs to be very clear, and simultaneously, internet has to be secured because there are more citizens to be concerned about in the

cyberspace and their economic interests as consumers. ... We [the EU and companies] need to bear in mind the interests of citizens, notably in data protection, crime prevention and safe use of the Internet” (Byrne 2000: 2). In fact, e-commerce potentially has many advantages, such as lower price, greater choice and better information (Byrne 2000: 2, Colón-Fung 2007), but issues linked security and confidentiality creates vulnerability in the virtual domain. The cyberspace offers medium an easy environment for undertaking of fraud because of ‘its anonymity and easy access, the lack of risk awareness, the lack of cyber-security skills and complex legal prosecution process for low value cross-border transactions’ (Centeno 2002: 1). Thus, to address the vulnerabilities, the Commission has found out three solutions, viz. prevention of the problems; alternative disputes resolution system; and help of the courts which is the last resort (Byrne 2000: 3-6). To address such risks, companies also adopted ‘hard measures or technology-based security measures’ (Centeno 2002: 15) and ‘soft measures – awareness, education and cybercrime law’ and to address the human factor as well as the issues of ‘social engineering attacks’ (Schneier 2000) where secret information is obtained by talking to people rather than breaking into a core layers of computer, are often the most damaging of any attacks (Centeno 2002:16). The issues related to risk, reliance and trust emerged as the significant game changer between the governments, business and individual.

Given the costs of information security is significantly high, this required lot of policy coordination between the MS and the EU. The adoption of the “Network and Information Security: Proposal for A European Policy Approach 2001”, was one of the vital policy approaches to address the issue of information security. Weber has argued that “the jurisdictional problem of cybercrime manifests itself in three ways: lack of criminal statutes; lack of procedural powers; and lack of enforceable mutual assistance provisions with foreign states” (Weber 2003: 426). He further identified the limitations of the existing international law to address the new risks associated with cyber-crime. To address the cyber crime issues, at the European and global level, for the first time in 2001, *the Council of Europe Convention on Cyber Crime*, resulted as a treaty which emphasised the criticality of the un-governable aspect of cyberspace. It contains 48 articles on the subject of response to the jurisdictional issues posed by the socialisation of the Internet. The treaty has aimed to harmonize cybercrime laws and assure the existence of procedural mechanisms to assist in the successful prosecution

of cyber criminals (Weber 2003: 426).

The growing dependency on the ICT and emerging threats was not only critical to the European digital economy and the fabric of the society, but also at the political and security level. Thus, to address the newly emerging risks, the EU established the European Union Agency for Network and Information Security (ENISA) in 2004 that signified the Union's commitments towards information security (cybersecurity). Although the ENISA is working proactively at the EU level, even after 14 years it is not empowered enough to deal with all security related issues. According to Gaycken (2017), the ENISA has very limited budget, is under staffed and has limited influence compare the national bodies in the big counties like Germany and France. There is need to enhance the capabilities and elevate its capacities¹³.

Further, to strengthen the ICT aspect of the digital economy, the EU adopted the Strategy for a Secure Information Society 2006, to create a secure, reliable and single European information space. Parrale to these new developments in cyber policy and creation of institutional – ENISA, the cyber attack on Estonia 2007 would compel the EU to formally securitize the cyberspace in the review of the ESS which took place in 2008.

Table 3.1: EU Member States and US's Percentage of Individuals using the Internet

<i>Country Name</i>	Year					
	2000	2005	2007	2010	2015	2017
Austria	33.73	58	69.37	75.17	83.94	87.94
Belgium	29.43	55.82	64.44	75	85.05	87.68
Bulgaria	5.37	19.97	33.64	46.23	56.66	63.41
Croatia	6.64	33.14	41.44	56.55	69.8	67.10
Cyprus	15.26	32.81	40.77	52.99	71.72	80.74
CZ	9.78	35.27	51.93	68.82	75.67	78.72
Denmark	39.17	82.74	85.03	88.72	96.33	97.10
Estonia	28.58	61.45	66.19	74.1	88.41	88.10
Finland	37.25	74.48	80.78	86.89	86.42	87.47
France	14.31	42.87	66.09	77.28	84.69	80.50
Germany	30.22	68.71	75.16	82	87.59	84.40

¹³ This point was mentioned by Dr. Sandro Gaycken, Director Digital Society EMST Berlin, in a personal interview on 05 July 2017 in Berlin.

Greece	9.14	24	35.88	44.4	66.84	70.1
Hungary	7	38.97	53.3	65	72.83	76.75
Ireland	17.85	41.61	61.16	69.85	80.12	84.52
Italy	23.11	35	40.79	53.68	58.14	61.30
Latvia	6.32	46	59.17	68.42	79.2	81.32
Lithuania	6.43	36.22	49.9	62.12	71.38	77.62
Luxembourg	22.89	70	78.92	90.62	97.33	97.83
Malta	13.11	41.24	46.9	63	76.18	80.07
Netherlands	43.98	81	85.82	90.72	91.72	93.20
Poland	7.29	38.81	48.6	62.32	68	75.99
Portugal	16.43	34.99	42.09	53.3	68.63	73.79
Romania	3.61	21.5	28.3	39.93	55.76	63.75
Slovakia	9.43	55.19	61.8	75.71	77.63	81.63
Slovenia	15.11	46.81	56.74	70	73.1	78.89
Spain	13.62	47.88	55.11	65.8	78.69	84.60
Sweden	45.69	84.83	82.01	90	90.61	96.41
UK	26.82	70	75.09	85	92	94.7
US	43.08	67.97	75	71.69	74.55	95.6

Source: ITU Statistics, 2018 and Internet World Stats, 2018

■ The cyber attacks on Estonia 2007 were the benchmark year for global cyber security discourse.

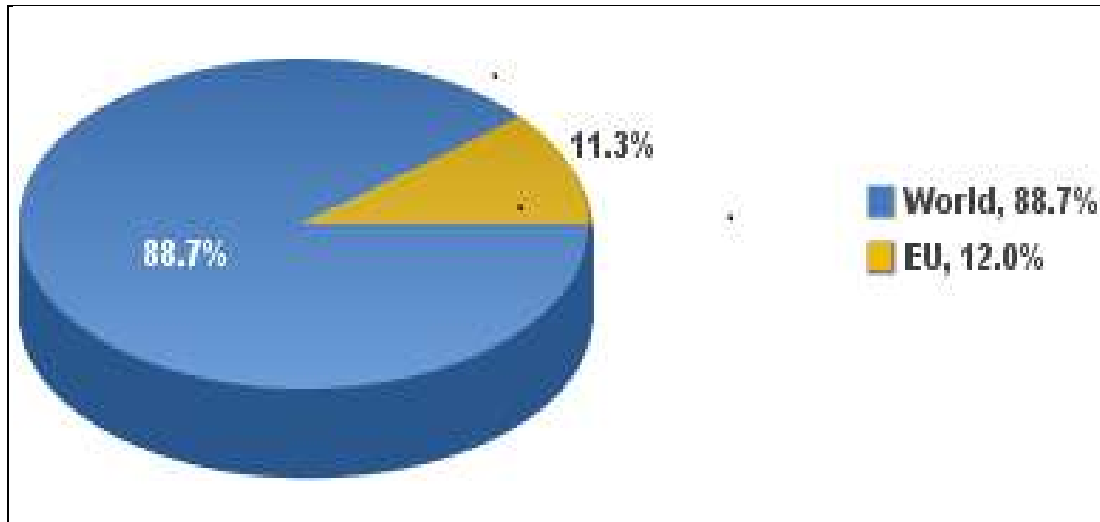
■ United States ■ Pre Brexit UK

After the 2007 crippling cyber attack on Estonia, the cyber security debates had become one of the vital topics and policy priorities for the Union. The reform of cyber security agencies like the ENISA, addition of cyber security and cyber crime into the review of the European Security Strategy in 2008 and EU Internal Security Strategy in 2010 have also emphasised the urgency of the matter and subsequent policy makeovers. Along with policy developments from 2007-2017, the use of the Internet has also grown exponentially. By end of 2017, out of EU- 27 (and in UK¹⁴), all countries were having more than 60 percent internet penetration and four countries (Bulgaria, Croatia, Italy and Romania) were having less than 70 percent of penetration. It can be easily understood that why the EU is called a ‘Wired Union’. However, its ranking globally is not so high.

¹⁴ Given the fact the Brexit war took place in 2016, the UK put it in the bracket as it is exiting the Union

The global figure shows that China tops the table in the Internet users followed by India, US, and Brazil. As per the latest facts and figures of the Internet *World Stats* – out of total internet users around the world, 12 percent internet users are only from EU-27 (and UK) (figure 3.1).

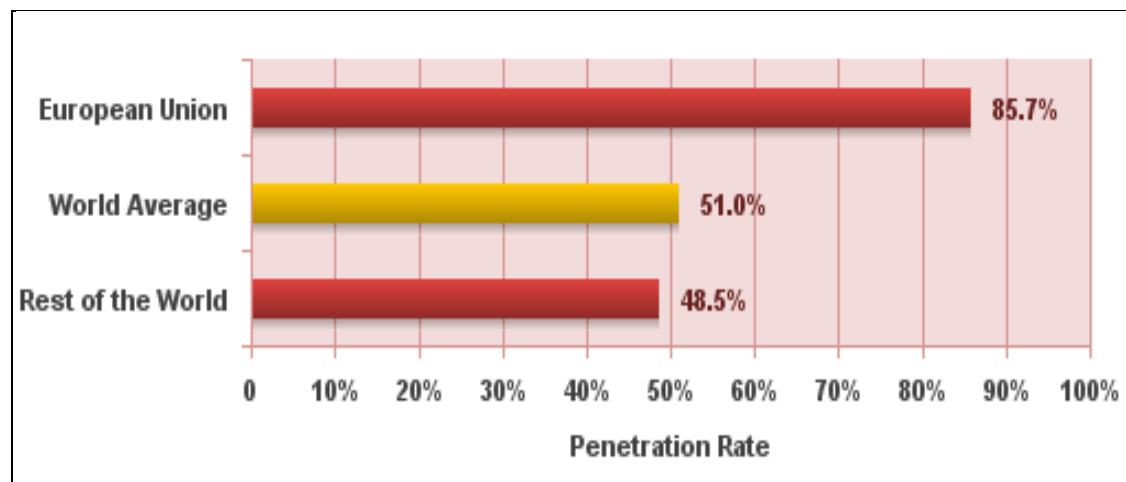
Figure 3.1: Internet Users in the EU – June 2017



Source: Internet World Stats, 2017

As per the Internet *World Stats, 2017* – only 51 percent of the world has been connected to the Internet while the EU-27 (and UK) has recorded one of the largest users with an average of 85.7 percent (figure 3.2) with a fastest network speed. However, South Korea and Japan are using the fastest internet network as far as the bandwidth is concerned.

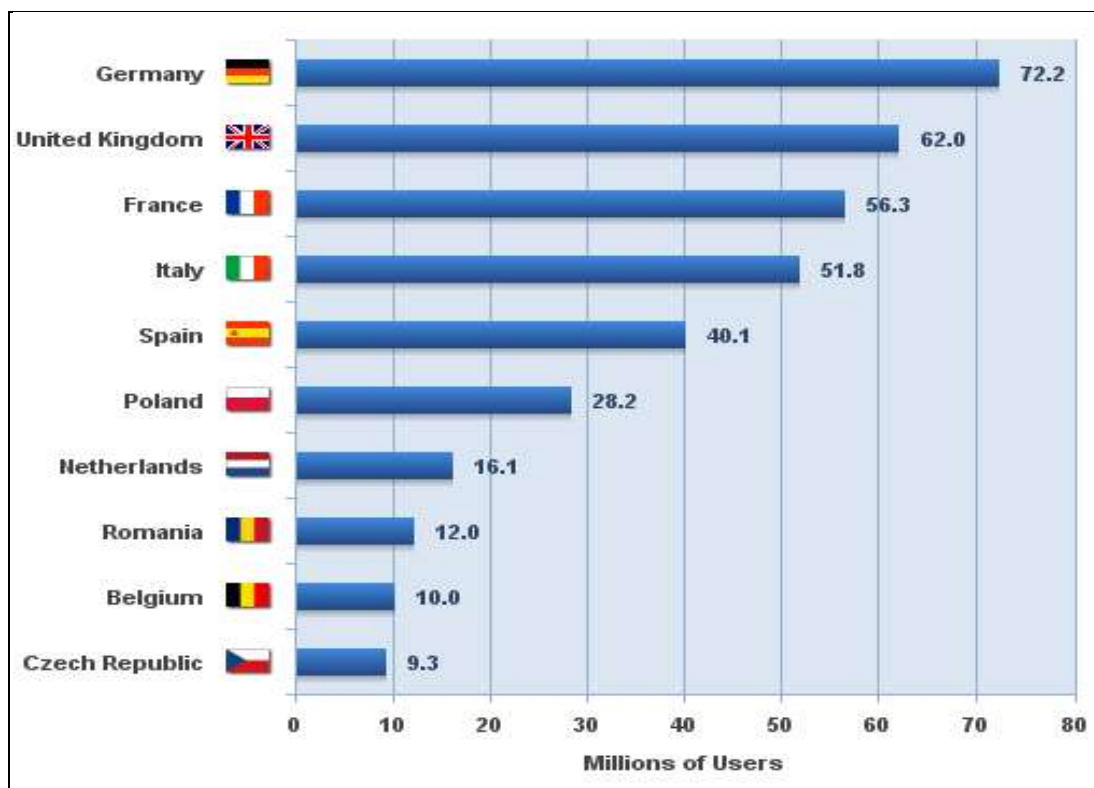
Figure 3.2: European Union Internet Penetration - June 2017



Source: Internet World Stats, 2017

Among EU-27 (and UK), Germany tops the table (figure – 3.3) as per internet user based, although it is in the 11th position compared to world internet based users. Among the top three in the EU-27 (and UK) table they have a very distinctive approach to cyber security discourse. Germany has given significant emphasis on the individual privacy, fundamental rights, rule of law and data protection in the digital age. While France and United Kingdom have brought a mixed approach of national and cyber security and kept data protection and privacy on the sideline. Being three major digital players in the EU, their different approaches bring in mixed-policy making to address the issues.

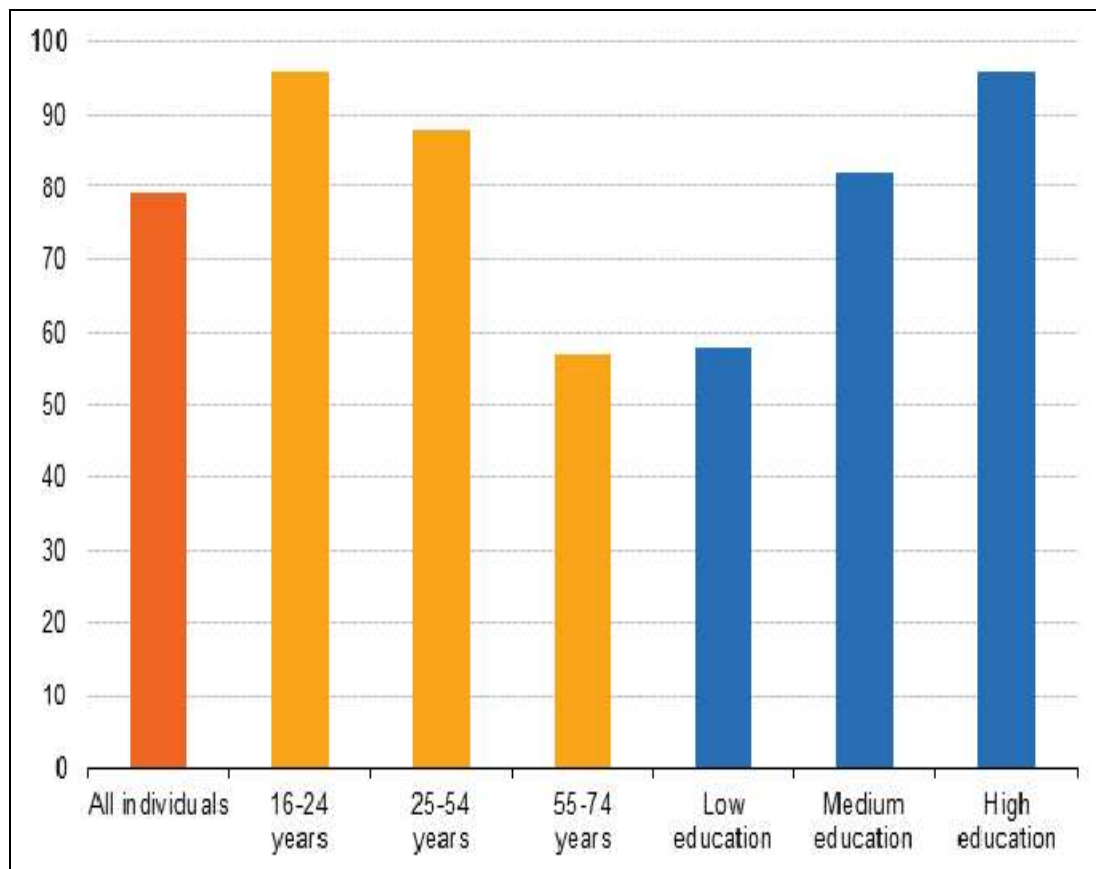
Figure 3.3: EU-27 (and UK) Top 10 Internet Countries – June 2017



Source: Internet World Stats, 2017

The International Telecommunication Union Facts and Figures, identified that young people are the prime consumers of the digital ecosystem, ‘the proportion of young people aged 15-24 using the Internet (71 per cent) is significantly higher than the proportion of the total population using the Internet (48 per cent)’ today (ITU 2017). Similarly, in the EU, more than 90 percent young people between the age of 16 and 24 are connected to the Internet and above 85 percent of individuals from the age group of 25-54 (figure 3.4). In a similar way individuals with higher education are more connected (90 percent and above) than the low and medium education.

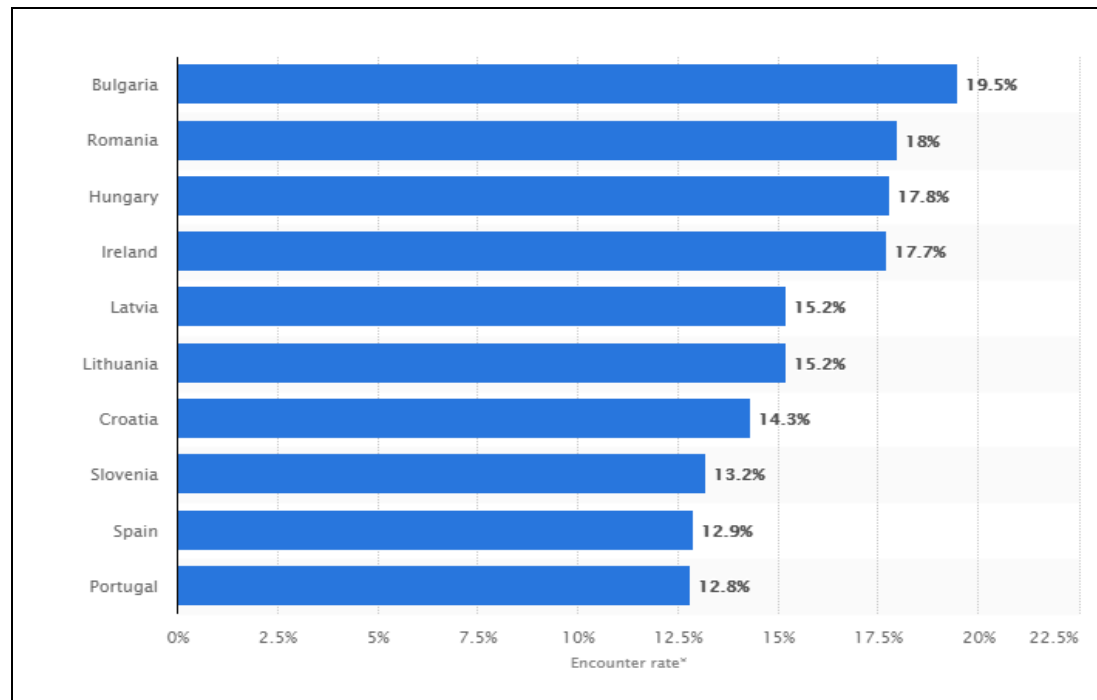
Figure 3.4: Individuals - frequency of internet use



Source: Eurostat, 2017

This indicates (figure 3.4) that the individuals with high education and young in age are more adaptable to the technological changes and disruptive developments. While older people and those with low educational background are not using the internet so much. This has also created a kind of digital divide among the digital users. According to the Eurostat, over 80 percent households in the EU-27 (and UK) are having access to both internet and broadband connection. That also shows the adaptability of a society and their preferences towards a digital world.

Figure 3.5: Ranking of the ten EU countries with the highest malware encounter rates as of January 2017



Source: Statista, 2017

The challenges to the EU's digital aspirations are huge both internally and externally. Internally, on the one hand it has to maintain balance between national security, fundamental rights, privacy and data protection issues and framing them into European commonness and on the other hand information sharing, capacity building, risk managing at the both national and EU level have to be also addressed. Externally, Russia, China, North Korea pose the prime threats to the EU's digital ecosystem. Moreover, Russia's hybrid warfare capacity, historical linkages, and frequent intrusion to EU's cyberspace make it one of the biggest threats. In addition, the rise of non-state actors and different organised syndicates also target the EUMS for various illicit use, cyber crime and financial gains. As per the (figure 3.5), the Central and Eastern European and Baltic countries have become the core targets of the new cyber geopolitics.

Coming back to the cyber-security matters, the Union has been working proactively after the Estonian incident. In fact, it is imperative to have a look at the cyber attacks on Estonia because it became an eye-opener for the EU to formulate and implement policies to mitigate security problems in the cyberspace.

THE CYBER ATTACK ON ESTONIA, 2007

Estonia which was an independent country before the outbreak of the World War I, was captured by the USSR in 1939, but after the Soviet disintegration, it declared its independence once again and subsequently joined the NATO and the EU. Estonia including other two Baltic republics has Russian speaking minority. In April 2007, Estonian Government moved the Bronze Soldier, a memorial commemorating the Soviet liberation of Estonia from the Nazis from the Tõnismägi Park in central Tallinn to the Tallinn Military Cemetery. This decision sparked rioting among the Russian-speaking community [which comprises around 26 percent of Estonia's population in 2007]. To ethnic Estonians, the Bronze Soldier symbolized Soviet oppression but to the Russian minorities its relocation represented further marginalization of their group. In retaliation, from 27 April to 18 May 2007, distributed denial-of-service (DDoS) and cyber-attacks targeted the country's infrastructure, shutting down the websites of all government ministries, two major banks and several political parties. At one point, the hackers even disabled the parliamentary e-mail server (Ruus 2008, Herzog 2011: 50-51, Michael 2012: 14). Later investigations have found some evidence that the cyber attacks originated in Russia.

After the crippling attack in 2007, the Estonian government came up with many preventive measures, such as Cyber Security Strategy, 2008–2013, Estonian Research and Development Strategy, 2007–2013 with the aimed to create Knowledge-based Estonia and the National Defence Development Plan, 2009–2018. They have mainly brought out a threefold classification of threats: cyber crime, cyber terrorism and cyber warfare. The Estonian Cyber Security Strategy (2007-2013) emphasised two things: “protection of national resources simultaneously with the accomplishment of taking the fight against cyber crime to the international/global level”.

Apart from the national strategies, the Estonia government had urged the EU and NATO to firmly respond to the new type of warfare. Moreover, at the 62nd session of the UN General Assembly in 2007, the then President of Estonia, Toomas Hendrik Ilves had also the raised the concerns that “cyber attacks are a clear example of contemporary asymmetrical threats to security. They make it possible to paralyse a society, with limited means, and at distance” (Ilves 2007: 3). The asymmetric and unpredictable nature of the cyber threats and the attack on Estonia got significant

European and global attentions. Due to lack of evidence after the attacks, immediate action was not taken against Russia. But the attacks were condemned by the EU, member states, NATO and the US (The Sydney Morning Herald 2007), while China treated it as an internal security dilemma of Estonia (Herzog 2011: 55). However, at the EU level, an asymmetric attack on the Estonian government created a spillover effect on policy formations of the Member States and the Union level. This would lead to the cyber threats coming into the ESS review 2008 and the EU international security strategy 2010.

Initially it was reflected in France, UK and Germany, the big three economies of the Union. In the same way, Germany mainly focused on the protection of critical infrastructure as a major concern of the cyber security mechanism. “Critical infrastructures (CI) are organizational and physical structures and facilities are of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences” (National Strategy for Critical Infrastructure Protection 2009: 4).

The UK government identified that, “the first duty of the Government remains: the security of our country” (UKNSS 2010: 3). Indeed, the nature of threats is that they are more open in nature, so for this reason, not a single country is fully secure from the threats. “(Britain) today is both more secure and vulnerable than most of her long history. More secure, in the sense that we do not currently face, as we have so often in our past, a conventional threat of attack on our territory by a hostile power. [...] more vulnerable, because we are [...] (the) open societies, in a world that is more networked than ever before” (UKNSS 2011: 4). Though the nature of cyber attacks is diffused, it poses challenges to the government, businesses and individual to protect the freedom, security and prosperity.

The French security strategy emphasised “(our) society is increasingly dependent on information systems and networks, particularly the Internet. A successful attack, on a French critical information system or the Internet could have serious human or economic consequences” (Information Systems Defence and Security Strategy 2011). Moreover, the EU MS have taken important steps along with the private sector to

address cyber security threats.

The attack on Estonia, would lead the NATO to establish in 2008 the Cooperative Cyber Defence Centre of Excellence, which is a cyber military headquarters in Tallinn to check Russia's incursion primarily on NATO member states. In addition, to strengthen both cyber resilience and to contain Russia in *lawfare*, NATO produced the first of its kind "Tallinn Manual on the International Law Applicable to Cyber Warfare" in 2013. The Tallinn Manual sees how international law applies to the cyber conflicts and cyber warfare and the Manual were prepared by an international group of experts invited by the NATO. In the Wales Summit 2014, the Heads of the State and Government of the member countries of NATO unanimously agreed on enhancement of cyber defence as cyber threats and cyber attacks were becoming more common and sophisticated. They also affirmed that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 was to be taken by the NATO on a case-by-case basis (NATO 2014). By releasing the Tallinn Manual 2.0 in February 2017, the NATO has once again reaffirmed its 'cyber containment policy' towards Russia.

A decade after the 2007 cyber attacks on Estonia, it has now become a 'digital republic' (Heller 2017) and spreading the success story of digital world both in the EU and worldwide. France and UK have been using an identical strategy to address cyber threats through the prism of national security. On the other hand, Germany has focused on data protection and privacy issues in the cyber realm. However, the EU data protection directive is a mirror of German data protection policy. At present, almost all of the EUMS have their national cyber security strategy in place. At the European level, the EU has emerged as a common platform for all stakeholders. The EU has been pursuing a 'carrot and stick' policy to make the 'digital single market' more secure, setting security standards, pursuing digital diplomacy, and developing stringent data protection policies to address various issues of cyberspace.

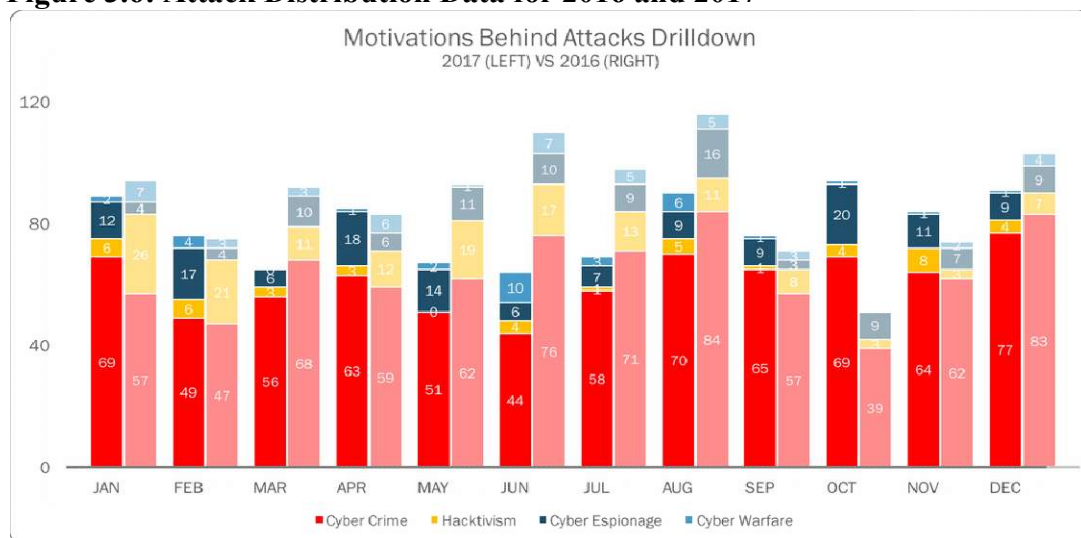
THE EUROPEAN UNION AND CYBER THREATS: ISSUE OF DATA PROTECTION

The EU in order to be a critical political, economic and security actor, it has to adapt to the changing environment, new and hybrid threats and the new emerging security challenges. Given that digital economy and digital connectedness are at the core of the economy, society, politics and security for the EU. All issues relating to cyberspace have become extremely important for the Union. This point was clearly point out ENISA 2012 document:

“The borders between virtual and real worlds are dissolving. New technologies, services and business models push existing concepts and regulation to their limits. The organizational structures and physical barriers that have stood for centuries are being severely put to the test by cyber threats that are continually evolving. ...The leading roles that information technologies play in modern society have made cyber security essential to the worldwide economy” (ENISA 2012: 4).

In essence, there is a greater possibility of being targeted by cyber attacks if the core of national growth depends on the Internet. Likewise, the same holds true for the EU in the recent period, the reason is its rising dependency and unpredictable nature of the cyberspace. However, the EU has emerged as a prominent actor in the cyber-domain in terms of e-commerce, connectivity, services, securitization, bandwidth. In addition, the Union is also well aware of the problems confronting the cyberspace. The digital world brings in new challenges, such as Cyber-Espionage, Cyber-warfare, Hacktivism, cyber-crime which are increasingly becoming the most talked about cyber security terms.

Figure 3.6: Attack Distribution Data for 2016 and 2017



Sources: hackmageddon, 2017

Figure 3.6 shows how different types of cyber attacks have evolved throughout 2016 and 2017. It is clear from this data that the majority of attacks fall into the category of cybercrime or hacktivism. The same trend is also observed in 2015 (Lohrmann 2017). The widely accepted definition of Hacktivism is, “the act of carrying out malicious cyber activity to promote a political agenda, religious belief, or social ideology, it could be state sponsored or conducted hacktivism” (Denning 2015) or self motivated. Cyber attackers (hackers) would attack for plethora of reasons, but the fundamental factor is to exploit the data. Those pieces of information or data could belong to people, government, and business.

The EU’s first approach to the cyberspace was focused on digital inclusion, to create a digital society where everybody could participate. To facilitate this, process one of the key steps was the launch of “.eu top-level domain” in December 2005 for Europeans with the aim to promote digital economy. Within a year after the launch in 2007, a huge number of cases of misuse of the domain that had been registered came to the fore front. That also shows how hacktivists and syndicates work promptly to pursue their illegal activities in the cyber age. This shows the need for the EU to develop strong policy for the cyber security, so as to complex nature of the cyber-attacks. The Union has indentified and defined various aspects related to cyber issues.

“**Cyber-security** - commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein” (CSSEU 2013: 3).

“**Cybercrime** - commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. online distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)”

(CSSEU 2013: 3).

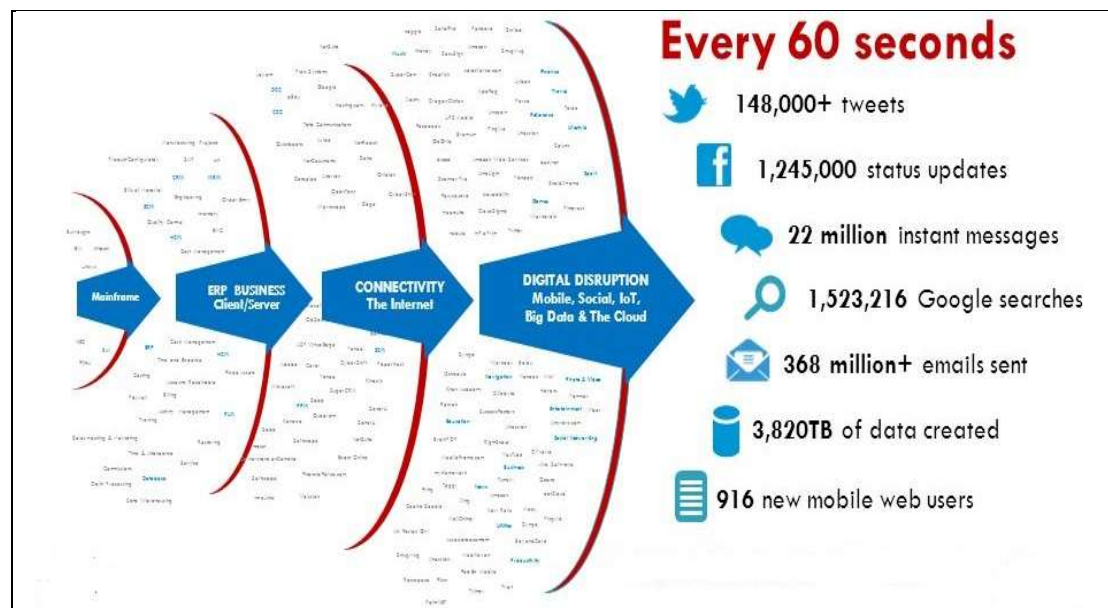
“*Cyber espionage* - is the act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers” (ENISA 2012: 6).

Cybersecurity has emerged as the prime agenda in the security landscape of the European Union. The domain which promoted the businesses in the Union has today acquired a security dimension. The European Research Commissioner Philippe Busquin (2003) rightly pointed out that, cyber threats ‘hides behind our computer screens and in the wires of global communication networks and services’. Various revolutions in the digital technologies have raised the concerns about the risks to data protection. The EU treated the issues of data protection and cyber security as both sides of the same coin. Since, the emergence of the digitization of human activities (money, machine and matter), the issue of data protection and individual privacy has been a subject of great concern.

In case of the EU, history plays a vital role in shaping up the approach to privacy in the digital age. On the contrary, the biggest pitfall is that the EU does not have strong internet industries and most powerful internet companies being based in either the US or China (Radu 2017)¹⁵. Although, America and Europe are part of the western world there is a differentiation in their value systems, this impacts the way data collected, stored and used.

¹⁵ This point was mentioned by Dr. Roxana Radu, Program Manager, the Geneva Internet Platform, in a Skype interview with the researcher on 13 March 2017.

Figure 3.7: Data Created in every 60 seconds in 2016



Source: SlidePlyer, 2018

The EU had adopted 1995 Directive data protection, furthermore it has been replaced by one of the most developed and robust regulations of digital world, the EU General Data Protection Regulations (GDPR) in 2018. The idea was to secure the European data in Europe and elsewhere.

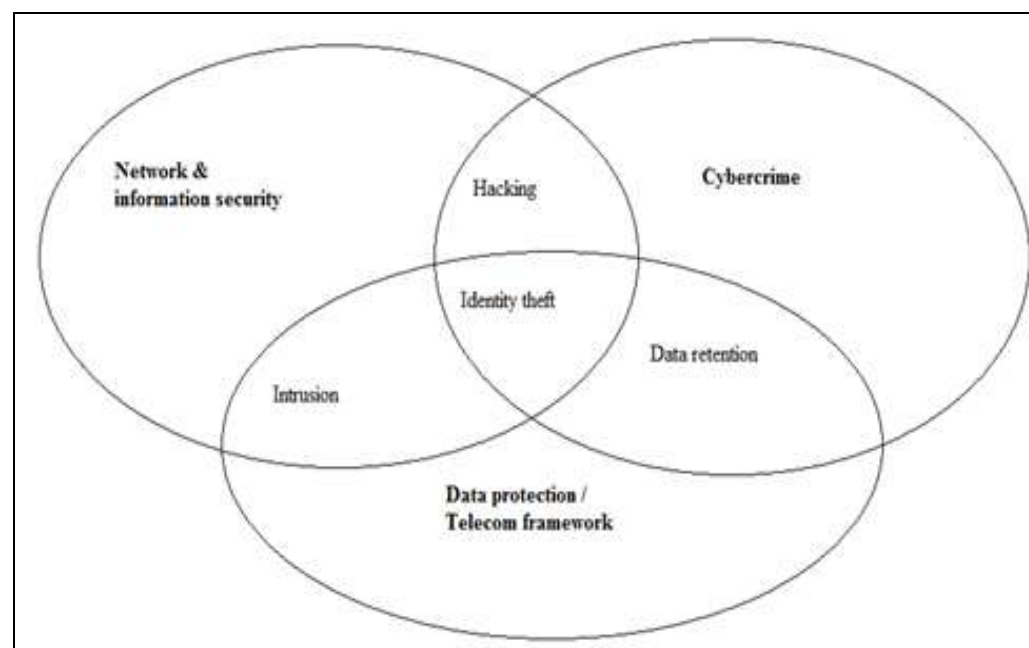
The diffusion of internet, computer, communication and mobile technology has resulted in data economy being the key to the EU’s current and future growth. Thus, data has emerged as “an essential resource for the EU’s economic growth, competitiveness, innovation, job creation and societal progress” (EC 2018a). In a data driven society, economy, polity and security dimension, the EU’s approach to cyber security and data protection regulations holds relevance to all these different aspects.

THE EUROPEAN UNION’S APPROACH TO CYBER SECURITY

The emergence of “information age in 1990s has fundamentally transformed the way in which the world operates” (Joyner and Lotrionte 2001: 826). Thus, the risks of information security and information warfare have gained the attentions of the governments as well as businesses in the EU. To protect the Internet-ecosystem and promote innovation, security, and to reduce threats in 2001, the Commission adopted a new policy to address the risks of the digital realm, i.e. “Network and Information

Security: Proposal for a European Policy Approach”. In fact, it outlined the importance of security for ICT and vice versa, and on other hand it also illustrated the correlation between the telecommunications, cyber-crime and data protection. The figure 3.8 shows the interrelation between the policy sectors of these three.

Figure 3.8: Cyber Security, Cybercrime and Data Protection



Sources: Commission of the European Communities 2001: 3.

The Commission has argued that security of the cyberspace is a key priority as well as a challenge for the policy makers. To address the newly emerging cyber threats, the Union has adopted soft measures - raising awareness; strengthening the cooperation between the Union and the MS to fight against cyber-risks and hard measures to enhance the credibility of the Computer Emergency Response Team (CERT), “which will be based on information sharing, technological support, standardisation and certification on the basis of market, creation of legal framework, security to government sector and promotion of international cooperation” (Commission of the European Communities 2001: 4). Dewar has argued that this policy was decisive for the development of the EU cyber security approach because it “laid out a detailed typology of threats from cyberspace; recommended specific technical measures to improve security provided a definition of NIS that would persist in EU policy in this sector until 2013; and formalised the placing of actor co-operation front and centre in the developing cyber security discourse” (Dewar 2017: 143).

Table 3.2: The EU’s Cybersecurity Policies and Strategies

Year	EU Policies and Strategies	Outcomes
2001	Network and Information Security: Proposal for A European Policy Approach	Recognising cyber vulnerabilities
2003	The European Security Strategy	Identified non traditional threats to security
2004	Creation of European Network and Information Security Agency (operational in 2005)	Institution building
2006	The EU Strategy for a Secure Information Society	Formation of Strategic approach to cyber security
2007	Cyber Attack on Estonia	Adoption of National Cyber Security Strategy by the EUMS
2008	Report on the Implementation of the European Security Strategy	Shift in approach – securitisation of cyberspace
2009	(a) The Critical Information Infrastructure Communication (b) Treaty of Lisbon	Stronger Union
2010	The Digital Agenda for Europe	Digital connectivity
2013	The EU Cyber Security Strategy	Strategic Approach to cyber security
2016	The Directive on security of network and information systems (the NIS Directive)	Creation of EU standards for information systems
2017	The cyber diplomacy toolbox	Sanction Regime
2017	Permanent Structured Cooperation (PESCO)	Cyber Defence mechanism

Source: Author’s work developed in consultation with Ph.D. supervisor

The EU established a “High Tech Crime Centre (HTCC) at Europol in 2002 (EC 2011b:60), for better coordination, analysis and training”, however, it does not have power to arrest. To address online scams, the European Commission also established a Joint Research Centre (JRC), a way of handling electronic information, to protect the rights of cyberspace users and guard against online deception. On the other hand, the EU Cyber Tools On-Line Search for Evidence (CTOSE) project helps to identify, secure, integrate and present electronic evidence on on-line criminal offences. However, in 2003, the Union has become the cyber Sherlock Holmes (European Commission 2003) to secure online transactions as well as guard against frauds during online buying. The new approach developed in this project enables investigators to use ‘computer forensic tools’ to gather evidence, which can stand up in courts or

tribunal proceedings throughout Europe. Four kinds of law enforcing mechanisms have been developed under CTOSE project – “Cyber-Crime Advisory Tool (C*CAT), legal advisor, XML-based specification and demonstrator for the protection of the cyber-ecosystem of the EU” (EC 2003).

In 2005 the Commission came with a new strategy, the ‘*2010 – A European Information Society for growth and employment*’. This policy has drawn a strategic roadmap for the Union and brings growth and security of ICT on to the centre stage. It is the successor of both the e-Europe 2002 and 2005, and an integral part of the Europe 2020. It contains three major objectives:

1: A Single European Information Space offering affordable and secure high bandwidth communications, rich and diverse content and digital services. 2: World class performance in research and innovation in ICT by closing the gap with Europe’s leading competitors. 3: An Information Society that is inclusive provides high quality public services and promotes quality of life (Commission of the European Communities 2005: 5-10).

Nonetheless, it has highlighted the need for a proactive policy approach to stimulate favourable market developments and the promotion of the knowledge society (e.g. lifelong learning, creativity and innovation), consumer protection and a healthy and safe European information society. In addition, it has ushered in the creation of a *Single European Information Space*, to address at the outset four main challenges posed by digital convergence: speed, rich content, interoperability and security.

It has elevated the position of the Lisbon Strategy 2000, to create a competitive and dynamic knowledge based society. In 2006, the Union formally came up with “A Strategy for a Secure Information Society – “Dialogue, partnership and empowerment”, an initiative for the Europe’s continent wide protection, private-public dialogue and global awareness. This document has emphasised the importance of PPP (Public Private Partnership) and the growing importance of ICT in the EU security threshold. It also encouraged creating a strategic partnership between the Member States, private sector and the research community which could bring transparency in the security landscape. This was one of the “incremental, linear” (Dewar 2017: 147) and significant developments in the EU approach to cyber security.

2007, turned out to be an evaluating period for the EU, with the massive cyber-problem in Estonia that pushed the Union to come out of its comfort zone and to take necessary steps to secure the cyberspace in a pragmatic manner. A large number of patch work initiatives were undertaken to enhance the capacities and capabilities through - allocation of fund for freedom, justice and security for the time period 2007-2013.

The European Union transformed from a reactive to resilient actor after the Estonian cyber attack. In 2007, the Union drew significant attention towards the threats and vulnerabilities of the cyberspace in a more vigilant and lucid manner. To assess the situation, on November 15-16, 2007, the EC organised an EU level expert meeting to fight against cyber-crime. The main objective of this gathering was to adopt a common policy on the fight against cyber crime and simultaneously engage key law enforcement and private sector representatives in discussions to identify concrete actions which can be undertaken at the EU level. As a result, it has identified that combating cyber crime actions required improved “*cross-border law enforcement cooperation*, common principles of public private cooperation and coordination to address various issues ranging from online sexual abuse of children and attacks against information systems” (European Commission 2007c). The Commission also identified eight major areas of problems such as, “rising vulnerability and risks of cybercrime; lack of coherent EU-level legislation; lack internal and cross-border law enforcement cooperation; lack of public private partnerships; lack of technical competence; unclear system of responsibilities and liabilities for the security applications and lack of public awareness” (Commission of the European Communities 2007: 2). However, the meeting did not highlight the issues of data protection which is vital to all cyber activity.

The Union had formulated many policies since 1997, without experiencing any large scale attacks and vulnerability, but in 2007-08 a series of incidents - cyber-attack on Estonia 2007, Lithuania 2008, and Georgia 2008 - took place within, as well at the doorsteps of the EU which shifted the Union’s priority towards becoming more proactive, secure and resilient towards cybersecurity issues. As a result in 2008, the review of ESS included cybersecurity as a major threat in the globalised world.

In 2009, through the Connect with Respect (i.e. Safer Internet Day), a project that

includes 30 European countries, which is co-funded by the European Union and celebrated in more than 70 countries, the Union brought a new policy for the protection of the child rights in cyberspace. The main aim was to empower and make aware teenagers to deal with potential risks they may face while they are online, such as cyber-bullying, revealing of personal information, etc. The growing influence of the social networking has turned into a social and economic phenomenon, attracting huge regular users in EU, and changing the way people interact with each other in the cyberspace. Thus, the Union set the guidelines to prevent the underage child, i.e. below the age of 13 to have access to social networking sites. On the other hand, it set standards to ensure that private profiles of below 18 users should not be searchable. It was one of the vital steps to protect information and privacy of children in the digital world.

In March 2009, The Commission adopted a resolution on Critical Information Infrastructure Protection (CII) which was also endorsed by the Council. It was aimed to protect EU's CII from large scale cyber-attacks and cyber disruptions and to enhance its preparedness to become more secure and resilient, to strengthen the security and resilience of vital ICT infrastructures, with the help of the Member States and EU institutions like ENISA. From 2009 onwards, the Commission proactively started to emphasise upon 'secure Europe' to protect from cyberattacks and disruptions. In this regard, the then Commissioner for Information Society and Media, Viviane Reding said:

Europe must be at the forefront in engaging citizens, businesses and public administrations to tackle the challenges of improving the security and resilience of Europe's critical information infrastructures. There must be no weak links in Europe's cybersecurity (European Commission 2009b).

She further argued that the reality of cyber-attacks is nowadays quite far from being a game or a proof of intelligence and curiosity. "Cyber-attacks have become a tool in the hands of organised crime, a means of blackmailing companies and organisations, of exploiting weaknesses of people, and also an instrument of foreign and military policy and a global challenge to democracy and economy" (Reding 2009: 1). In fact, one month long internet interruption in Europe or US would mean economic losses of at least 150 billion Euros (Reding 2009) and in 2014 the scenario was estimated that the world spent 1.2 million US dollar in each 30 seconds (Armbrecht 2016). That

scenario is just the tip of the ice berg, with the advent of Fourth Industrial Revolutions if the Internet went down for a day it would impose an unimaginable damage to economy, politics, security and society of the EU.

The Commissioner also urged to the Union to create a ‘*Mister Cybersecurity*’ like ‘*Mister Foreign Affairs*’, a security star with authority to act immediately if a cyber attack is underway, a cyber-cop in charge of the coordination of our forces and developing tactical plans to improve our levels of resilience (Reding 2009: 1), which is still far from the reality. Dewar (2017)¹⁶ has argued that UK was one of the key Member States that pushed the EU to enhance its cyber defence capabilities. Once the UK is out of the club, the agenda to enhance the cyber defence capabilities might be delayed at the EU level.

In 2010, the Union stimulated its mechanisms to secure Europeans through “*The Stockholm Programme- an Open and Secure Europe Serving and Protecting Citizens*”. It had three major priorities: Justice, Freedom and Security for the period of 2010-2014, through which it advocates for six primary pillars of security and stability of the region- “Europe of rights, justice, protects, access, solidarity and Europe in a globalised world” (European Council 2010b). This strategy was aimed to protect the rights and promote justice among the Europeans both vertically and horizontally¹⁷ on one hand, and on the other hand securitising Europe from various traditional and non-traditional threats (i.e. identified by the ESS and the Review report and others like economic crime, piracy, trafficking and sexual immorality¹⁸). This strategy also proposed to ratify the 2001 Council of Europe Convention on Cybercrime (European Council 2010b: 22) as soon as possible by the MS. At the same time it insisted that both the Union and the MS develop transparency in tackling the criticality of cybercrime.

¹⁶ The point was mentioned by the Dr. Robert Scott Dewar, Senior Researcher, the Center for Security Studies, ETH Zurich, in a Skype interview with the researcher on, 07 July 2017.

¹⁷Rights of the children, minority groups and victim of violence; simultaneously promotion of democracy and justice among the MS.

¹⁸ Sexual abuse, child pornography, sexual exploitation of children.

The EU enhanced its cyber-preparedness in 2010, by the adoption of the Digital Agenda for Europe (DAE), empowerment of ENISA (through cyber Europe exercise) and building an atmosphere of trust within and outside the EU to fight against cybercrime and security. “Digital Agenda for Europe aims to stimulate the accessibility and to make Europe a powerhouse of smart, sustainable and inclusive growth on the global stage” (European Commission 2010c: 5-6). The fundamental focus of the Agenda was to make the EU as a hub of data driven digital economy, with due protection of individual data and privacy. However, similar transformations are shaping now in the digital space of the EU. For the first time, the Union hosted the EU-US summit 2010 in Lisbon by taking cyber security issues to their bilateral forum.

In 2011, the Commission adopted and upgraded policy on “Critical Information Infrastructure Protection (CIIP)”. The main aim was to deal with the critical cyber threats on CIIP and secure the infrastructure from being attacked. The 2011 CIIP was the successor to the 2009 policy of the Commission. It also outlined the critical and global nature of cyber-threats that could “originate from anywhere in the world and due to global interconnectedness, impact any part of the world” (European Commission 2011a: 4). Therefore, a global understanding has to develop to mitigate and to manage the risks related to digital infrastructure. This report also “emphasised internal (pan European cyber-mechanism on the one side), and external (on the other side building strategic international partnership with US, G8 and other like minded countries) inter alia with the European coordinated efforts in the international forums and discussions on enhancing the security and resilience of internet” (European Commission 2011a: 6). To address the evolving threat scenario – cyber warfare and cyber terrorism – the Commission agreed to push global cyberspace norms creation and cooperation to address the issues that would bring security, stability and resilience to the Internet.

In 2011, the internal security as well as cyber threats became the major area of concern for the Union. Shortly before a major summit meeting in March 2011, the European Commission and the European External Action Service was hit by a major cyber attack (EUobserver 2011, Bendiek 2012: 9) which drew attention to the growing vulnerability and threats across cyber domain. These are stark reminders of the importance of taking actions to counter threats to internal security (European

Commission 2011c). To address the growing cyber threats, the Union launched a pilot project – Computer Emergency Response Team for the EU (CERT-EU/EU-CERT) in 2011 and after successful completion of a year, in 2012, the EU established a permanent body of IT experts to provide 24x7 security support to the EU institutions.

In November 2011, for the first time, transatlantic cooperation came in place specifically to accelerate their cyber preparedness through a cyber security exercise. With the support of “the EU’s cyber security Agency ENISA and the US Department of Homeland Security, a day-long table-top exercise, “Cyber Atlantic 2011, was held in Brussels” (European Commission 2011b). Simulated cyber-crisis scenarios were conducted to explore how the EU and the US would come together and cooperate in the event of a cyber-attack on their critical information infrastructures (ENISA 2011). It was one of the commitments on cyber security by the two Atlantic friends during the Lisbon summit in 2010, whereupon they had agreed to establish an EU-US working group on cybersecurity and cyber-crime. So far the developments in the field of cybersecurity were only within the EU, but for the first time it moved across to the other side of the Atlantic.

In 2012, The Commission strengthened the European Public Private Partnerships for Resilience (EP3R), which was a part of the 2009 strategy to protect critical information infrastructure. Its other core institutions and projects (those fighting for cyber-security and resilience) as a result the ENISA, EUCERT, EUROPOL and DAE were also fortified. On 30 January 2012, Neelie Kroes, the then Vice-President of the European Commission responsible for the Digital Agenda, in her speech in Brussels, emphasised that “transformative change in the digital realm had gone from promise to delivery; from a technical novelty to the backbone of the economy and society In fact, it will grow more, and in tomorrow's world, thus there is need to secure the Internet” (Kroes 2012a: 2). Moreover, threats to EU’s digital economy and ambitions are mushrooming in the backdrop of security, accessibility and openness of the cyberspace, but the private sector owns or controls the majority of cyber infrastructure as well as possesses the sophisticated expertise which made them a crucial actor in this domain. Thus, there is a need for comprehensive multistakeholder approach to address various issues related to cyberspace. The Union also realised the necessity to strengthen hand fortify the EP3R to enhance the information sharing about the cyber

incidents between the public and private sectors, by building a system of incentives, awareness and investment on innovation for security technologies.

Cyber Security Strategy of the Union, 2013

Cyber resilience became one of the prime concerns for the Union in 2012, and the EUROPOL was elevated to address cyber domain issues. In 2013, the EU established the European Cybercrime Centre (EC3). The EC3 has mandate to “strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from internet crime” (EUROPOL 2018). All these debates and the urgency over cyber security led EU release the “Cybersecurity Strategy of the European Union 2013” (CSSEU). The main aim of the strategy is “an open, safe and secure cyberspace” internally through cyber coordination and externally by cyber diplomacy.

The proliferations of digital technologies have underlined the fact that nation-states are living in a borderless and multi-layered, interconnected digital world and “the Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation” (EC 2013a: 3). Furthermore, a lack of governance and international regulations in the cyberspace makes it very high security risks area. The CSSEU underlined that the role of the private and civil society are critical to governance, regulations and security of the cyberspace (EC 2013a: 3). Therefore, the CSSEU clarifies the principles that should guide cybersecurity policy in the EU and internationally to build a comprehensive approach to cybersecurity discourse.

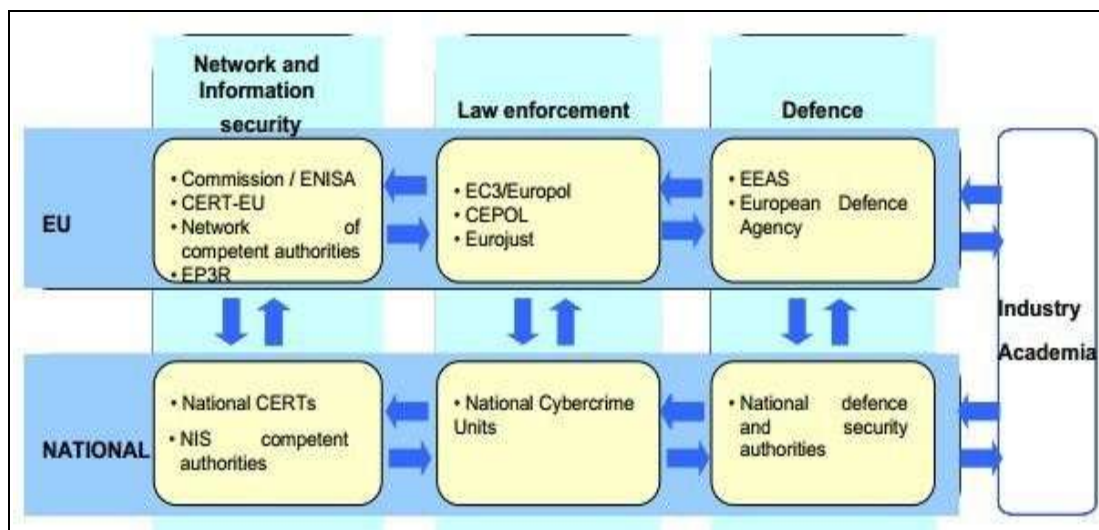
Cyber attacks undermined the physical borders and in an interconnected digital economy complexities require diverse range of stakeholder’s involvement. It is also a difficult task for an intergovernmental organisation to create a centralised agency to deal with cyber threats. Apart from government and private sectors, the role of civil society has a significant role to create awareness about the digital space, use and privacy (Pohle 2017)¹⁹. The CSSEU clearly explained that

¹⁹ This point was mentioned by Dr. Julia Pohle, Research Fellow, WZB, Berlin, in a personal interview on 23 March 2017.

...centralised, European supervision is not the answer. National governments are best placed to organise the prevention and response to cyber incidents and attacks and to establish contacts and networks with the private sector and the general public across their established policy streams and legal frameworks. At the same time, due to the potential or actual borderless nature of the risks, an effective national response would often require EU-level involvement (EC 2013a: 17)

The CSSEU has categorically drawn a power sharing thin line between the MS and the Union, therefore, EU agencies like ENISA and EC3 have certain limitations while dealing with national issues. However, the CSSEU has underlined the structure of better coordination between the MS, law enforcement, national agencies, EU agencies and other stakeholders, the Union proposed this formation (see Figure 3.9).

Figure 3.9: Coordination between NIS competent authorities/CERTs, law enforcement and defence



Source: Cybersecurity Strategy EU 2013a, 17.

The strategy has five principles to address the cyber issues at large and with specific concerns towards *regulations, data protection and personal privacy*. Those principles are

The EU's core values apply as much in the digital as in the physical world; Protecting fundamental rights, freedom of expression, personal data and privacy; Access for all; Democratic and efficient multi-stakeholder governance; A shared responsibility to ensure security (EC 2013a: 3-4).

Apart from these guiding principles to make a comprehensive action plans to cyber security, the CSSEU has also set out 'Five Strategic Priorities and Actions'.

Achieving cyber resilience; Drastically reducing cybercrime; Developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP); Develop the industrial and technological resources for cybersecurity; Establish a coherent international cyberspace policy for the European Union and promote core EU values (EC 2013a: 4-5).

The CSSEU also elevated the actorness of the EU on cyber resilience internally and it's potential to lead cyber diplomacy discourse externally. 2013 not only saw the launch of the CSSEU but also witnessed many cyber security related debates. On 28 March 2013, Aljazeera had reported a huge worldwide cyber attacks. As e Silva (2013) pointed out that it was "the biggest in history, the Distributed Denial-of-Service Attack (DDoS) of 300Gbps started as retaliation from the hosting server Cyber Bunker against the anti-spam organisation Spamhaus. The attack not only caused disturbances to Spamhaus and its hosts and partners, but also slowed down internet connection internationally, most notably in the UK, Germany and other parts of Western Europe" (e Silva 2013: 2).

The second bombshell and most significant incident of cyber security history was the revelation of ex- National Security Agency contractor, Edward Snowden in 2013. International media and analyst became more vocal towards the nature of this mass surveillance and due to this, the US had suffered in its bilateral relations with Germany, India, China, Russia, Brazil and other major powers. The disclosure on the closest ally Germany made US relations strained it for a certain period of time, with Federal Commissioner for Data Protection Peter Schaar German, calling it "monstrous monitoring" (EurActiv 2013).

After the news surfaced about the NSA's global surveillance, the EU had condemned the action and European lawmakers threatened to abandon data sharing agreements with the US. Moreover, "Members of the European Parliament (MEPs) were described as "furious" that US authorities had been accessing their e-mails and other personal data from leading internet companies. In a heated debate in the European Parliament, lawmakers complained that for a decade they had bowed to US demands for access to European financial and travel data and said it was now time to re-examine the deals and to limit data access" (Reuters 2013). On the other hand some

members of the European Parliament also said that they would “redouble efforts to strengthen a proposed EU-US data protection agreement in the field of police and judicial co-operation” (Wright and Kreissl 2013: 7).

This issue was also hotly debated in the EU and the European Commission Vice President Viviane Reding (2010-2014) also said that “Programmes such as PRISM... potentially endanger the fundamental right to privacy and to data protection of EU citizens” (Wright and Kreissl 2013: 8). EU officials demanded “swift and concrete answers” from the US government about its spying programs (The Guardian 2013). After the disclosure of the involvement of The Government Communications Headquarters (GCHQ)’s TEMPORA, Ms. Reding also sent a letter to the UK foreign minister William Hague asking for details. She asked if “TEMPORA is restricted to national security, if snooping is limited to individual cases or is in bulk, if the data is shared with third countries like the United States, and if UK and EU citizens have any legal recourse when it comes to their data” (Nielsen 2013).

The Snowden revelations have repealed decade old Safe Harbour agreement between the US and the EU that came into operation in 2000 after the EU determined that “the US standards were ‘inadequate’ in meeting the data protection principles of the EU’s Data Protection Directive of 1995” (Wright and Kreissl 2013: 18). Under the agreement, “US companies were allowed to handle or store European citizens’ data to self-certify annually with the Department of Commerce that they will abide by the standards” (Wright and Kreissl 2013: 18). This particular incident had a retrospective impact as well as it altered transatlantic political relation, and impacted the future discourse of trans-border data flows and cyber related issues.

Table 3.3: Evolution of the EU’s Data Protection Regime

Year	EU Regulations	Outcomes
1950	The European Convention on Human Rights	Human Right brought into the political platform
1980	OECD Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data	First regulation on privacy and personal data
1981	Council of Europe -Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	First step at codifying the rules

1995	The Data Protection Directive (officially Directive 95/46/EC)	First EU Regulation of Data
2000	The Charter of Fundamental Rights of the European Union	Expansion of the space of individual privacy
2001	Network and Information Security: Proposal for A European Policy Approach	Data is key to information security
2002	First E-Privacy Directive	Free flow of personal data within EU
2009	Treaty of Lisbon	Institutionalisation of Data Protection as Fundamental Rights
2010	The Digital Agenda for Europe	Better environment for data driven economy
2013	The EU Cyber Security Strategy	Securitisation of data
2013	Snowden Revelations	Global awakening on privacy and data protection
2014	The right to be forgotten judgement	Individual liberty
2015	Digital Single Market	European single data economy
2015	European Court of Justice Judgement on Safe Harbour Privacy Principles	End of safe harbour principles
2016	Privacy Shield Agreement	Creation of new regulations for cross border data flows
2018	The General Data Protection Regulation	Creation of the EU data protection regime with global implications

■ Non EU Influencer ■ Data Protection Regulations ■ Other EU Strategies

■ Major events ■ EU Treaties, Principles

Source: Author's work developed in consultation with Ph.D. supervisor

As the above table 3.4 shows, The EU's approach to data protection is crucial to global data governance. Moreover, the European Convention on Human Rights (ECHR); OECD guidelines on data protection and Council of Europe convention had

primarily influenced the EU data protection regulations. The timing of the Directive 95/46/EC was crucial to world politics. During this period, the world would experience that the World Wide Web was growing in to its fourth year. The 1995 Directive, showed the EU taking cognisance of the impact of technology on the developing digital economy, it was ahead of its time in laying down guidelines that data of the EU citizen must be protected with ‘adequate level’ of protection as per European standards. This aspect of data protection was also reflected in The Charter of Fundamental Rights of the European Union 2000, wherein, Article 8 talks about the protection of personal data.

In 2001 the EU would launch the Network and Information Security: Proposal for a European Policy Approach, one of the significant policy, by the Union that talked about three fundamental aspects of cyberspace – connectivity, threats and data protection. It sets the agenda for future evolution of the EU’s cyber security policies. The E-Privacy Directive 2002 is a complement to the 95 Directive, which further harmonised the data protection regulations for better service to the Community. Similarly, 2009 The Lisbon Treaty, made data protection as one of the fundamental rights of EU citizen under Article 16.

The EU is well aware about the opportunities of the digital age and thus, launched the ambitious Digital Agenda for Europe to transform it into a digital union. The then Vice President and Commission and responsible for the digital agenda, Neelie Kroes said that “...the data is new oil for the digital world. In the digital age data takes on a whole new value, and with new technology we can do great things with it. Opening it up is not just good for transparency, it also stimulates great web content, and provides the fuel for a future economy” (Kroes 2012b: 2). Thus, to address the security challenges of a digital union, the EU launched its CSSEU in 2013. Which stated that “cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values” (EC 2013a: 4), in other words, protection of fundamental rights, freedom of expression, personal data and privacy as crucial as security of the cyberspace. It can be seen that four major events – Snowden revelations, Right-to-be-Forgotten judgement, European Court of Justice Judgement on Safe Harbour Privacy Principles and Privacy Shield Agreement have added new segments to the evolution

of EU data regime. The implementation of the GDPR in 2018 has transformed the actorness of the EU internally along with global cyber governance. It has paved the way for the EU to become a pioneer of global data governance regime. In a nutshell, the EU is emerging as comprehensive and resilient cyber security actor.

CONCLUSION

As the above analysis shows, the EU's approach to each old and new security threats have been transforming it as a composite security actor both at European and global level. In the digital age, the EU has outlined and inculcated the European value based approach to entire area of cybersecurity discourse. The cyberspace is a melting pot in which threats emanate from unpredictable sources that multiply the risks of vulnerabilities to the government, business and society. However, incremental and norm based approach to cybersecurity and data protection shows that the EU became a proactive actor in the digital realm.

The protection of personal data and privacy is core to the EU's cybersecurity discourse. From the 1995 Directive till the implementation of the 2018 GDPR, the EU has always pushed forward the European values of protecting the citizen. The incidents like Snowden revelations expose that there are many issues hidden from the real world and how governments work with each other. In other words, "state does spy, allies do share information' and digital technologies are the enabler of this act" (Peters 2017)²⁰. In the digital platform, the private sectors and the states and both have a great stake in the data protection debate discourse.

The next chapter examines the US approach to cyber security and subsequently in Chapter-5 the issue of data protection in the formwork of cyber security examines in detail to find out the convergence and divergence between the EU and the US policy and approach.

²⁰ This point was mentioned by Dr. Ingo Peters, Associate Professor of Political Science, Center for Transnational Relations, Foreign and Security Policy, Otto-Suhr-Institute for Political Science, Freie Universität Berlin, in a personal interview on 26 June 2017.

CHAPTER 4

THE UNITED STATES APPROACH TO CYBERSECURITY

“...pay any price, bear any burden, meet any hardship, support any friend,
oppose any foe, in order to assure the survival and the success of liberty”
(John F. Kennedy 1961)

INTRODUCTION

The US has played a crucial role in shaping the world order in the 20th century and continuous to do so even now. The US’s economic, political, security and cultural influence in different parts of the world has been the central stimulus to the emergence of this order. The role of the US is exceptional in the emergence of the current international order which is based on – protection of national interest by securing first economic interest and industrial power, second, by building national security through power projections. In the making of the 21st century’s global security landscape, the US holds a decisive position to drive the key agendas. Kissinger paints the canvas quite profoundly about the US role in world affairs –

acting for mankind: no country has played such a decisive role in shaping contemporary world order as the US, nor professed such ambivalence about participation in it (Kissinger 2014: 234).

Even today, the 1945, Bretton Woods institutions continue to set the agenda and drive global politics. While the end of the Cold War led to the demise of the Soviet Union, the US would emerge as the victorious power which led Francis Fukuyama to speak about “the End of History”. The pursuit of American national interest has remained unchanged with each government in Washington. It is the national interest which drives the US foreign and security policy and this has helped them throughout the last century and now to set the global order and dictate the global regimes. The US had emerged from the Second World War as the most powerful nation (Morgenthau 1948: 73), however, it was constrained due to the Cold War confrontation with the Soviet Union.

The tectonic shift in the world affairs was witnessed in the last decade of the 20th century. The collapse of the Soviet Union, end of the bloc politics and demise of the balance of power structure offered a space to the US to rise as a ‘hegemon’ in international politics. The US enjoyed an unchallenged decade as a sole superpower,

however, the 9/11 terrorist attacks was a biggest security attack on the US, which had multiple political, economy, societal and security ramifications. Ten years after the End of the Cold War an unprecedented attack by a non-state actor sought to undermine its power thereby drawing attention to the changing security landscape and the rise of non traditional threats to security.

At the political level, the leadership of President George W. Bush Jr., was instrumental in transforming how the US would conduct its foreign policy. According to Nye “three major changes [were] made to [the] US grand strategy after the terrorist attacks of September 11, 2001: reducing Washington's reliance on permanent alliances and international institutions, expanding the traditional right of pre-emption into a new doctrine of preventive war, and advocating coercive democratization as a solution to Middle Eastern terrorism” (Nye 2006: 139). At the domestic level, President Bush was able to generate ‘national security’ among fellow Americans. In addition, he securitised internal security by creating institutions and policies that would be intrusive into lives of American and non-American living in the US. Under President Bush, it would not be wrong to say that with the creation of the Department of Homeland Security on 25 November 2002, transformed the US with a surveillance state which will make use of the latest technology to track all behaviour and activities of citizens and non-citizens alike.

Simultaneously the advancement of science and technology much prior to the 9/11 incident, Kirk (1945) warned that “in this era of mechanized warfare our geographic remoteness from other great centers of national power no longer assures us the same margin of safety as we formerly enjoyed” (Kirk 1945: 620). In the post Cold War period, the 9/11, emerged as the significant attack on the heart of the US sovereignty and challenged its superpower status. The scope of non-state actors to impact the kind of damage they did on the US was unprecedented in scale and impact.

THE UNITED STATES AS THE SECURITY ACTOR AND THE EMERGING SECURITY LANDSCAPE, 1990-2001

During the Cold War period from 1945-1990 the US was one of the key superpowers, along with the Soviet Union. The US identified its security interest at global level in the post war period. However, for the first time the US was ambitious to manoeuvre

vast Eurasian landmass. This was only possible by the “preservation of a favourable balance of power in Eurasia and good post-war relations among the Allies” (Leffler 1984: 349). In fact, conceptualisation US’s role in international security truly emerged. The end of the Cold War opened new avenues of challenges as well as opportunities to reshape global security landscape.

Table 4.4: the US as a Security Actor

Year	The Evolution of the US’s Actorness	Outcome
1947	National Security Act	Restructuring of Armed Forces and Intelligence services
1981	Packard Commission	Reform and management of Department of Defense
1986	Goldwater–Nichols Act	Fixed inter-service rivalry and created a chain of command
1987	National Security Strategy of the United States	First strategy after the Goldwater-Nichols Act, military is the core of power
1988	National Security Strategy of the United States	Economic security emerged as a key concerns
1990	National Security Strategy of the United States	Addressed the changes on the Eastern Europe due to the fall of Soviet Union
1991	National Security Strategy of the United States	New World Order
1993	National Security Strategy of the United States	Peaceful change
1994	A National Security Strategy of Engagement and Enlargement	Selective Engagement
1995	A National Security Strategy of Engagement and Enlargement	Regional instability
1996	A National Security Strategy of Engagement and Enlargement	Active engagement
1997	A National Security Strategy For A New Century	Cooperative security arrangements
1998	A National Security Strategy For A New Century	Open and competitive system
2000	A National Security Strategy For A New Century	Advance of US National interest
2001	A National Security Strategy For A Global Age	Security in New Millennium
2001	9/11 Terrorist Attack	Changing nature of security - Unpredictable
2001	The USA PATRIOT Act	Empowering law enforcement and intelligence services
2002	The National Security Strategy of the	Internationalisation of US

	United States of America	security and terrorism emerged as key threats to security
2002	Homeland Security Act	Established the Department of Homeland Security
2006	The National Security Strategy of the United States of America	Cyber as a disruptive challenge to national security
2010	National Security Strategy	Security of Cyberspace
2015	National Security Strategy	Collaborative efforts between establish and emerging powers
2017	National Security Strategy of the United States	American First (protection of national interest and security)

Source: Author's work developed in consultation with Ph.D. supervisor

During the aftermath of the World War II, the US adopted the National Security Act, 1947, to create a legitimate national security structure. This was followed by the Packard Commission 1981, which conducted a military stock taking as aimed to address the reformation and management of Department of Defense (DoD). Further steps to strengthen national security posture “the Goldwater–Nichols Department of Defense Reorganization Act of 1986”. Subsequently at the height of the standoff the Cold War the Regan administration released two National Security Strategies (NSS) which primarily focused on military and economic security aspects of the government.

In 1989 the dramatic developments in Europe with the fall of the Berlin Wall on 9 November 1989 and the reunification of Germany on 3 October 1990 brought a sudden end to the Cold War confrontation of 45 years, leaving America as the sole super power. War soon erupted that would test America as a security actor in the post Cold War period due to the annexation of the Kuwait by Iraq. This led to the President Bush launching the first Gulf War in January 1991 to expel Iraq to out of Kuwait. This shifting power equation became even more evident with the collapse of the Soviet Union in 1991. It was the time that witnessed very significant and notable transformations in the global security landscape.

President George H. W. Bush Sr., entered the White House at a period of tremendous change in the world politics which begun in 1989. He released his first NSS in 1990 and this clearly highlighted the changing security landscape, “the crisis in

Communism; rise of industrial democracies; the global economy; third world conflicts; trends in weaponry; illicit drugs; refugees and the rise of multipolarity” (NSS 1990: 5-7). By 1991, it was an entirely different world order which left America as ‘the lonely superpower’ (Huntington 1999), or ‘hyperpower’ (NYT 1999). It also indicated two prominent issues –unfolding in international politics – “*New World Order* (NSS 1991: v) or a multipolar world order and diffusion of threats into local level. Samuel Huntington famously described it as “a superpower with many minor powers” (Huntington 1999). The third and the last security strategy of the Bush Sr., administration emphatically stated that “today’s challenges are more complex, ambiguous and diffused – politically, economically and militarily’ (NSS 1991: 1). In other words, it recorded a paradigm shift in the national security landscape.

The national security agenda became wider and deeper during the Clinton administration and this was reflected in the three national security documents released in 1994, 1995 and 1996. The changing security terrain in Europe with the breakup of Yugoslavia due to the civil war and the inability of the newly emerging European Union to respond to the crisis draw America back into the European wars. Alongside, for the first time, China came to be regarded as the emerging threat due to its regressive and authoritarian regime, as the consequences of the Tiananmen Square protest and massacre 1989. Partial peace would come to the Balkans through the US initiated Dayton Accords of 1995 that resulted in the creation of Bosnia and Herzegovina as a separate country. It is significant to note that, the US NSS announced at this time spoke off “A National Security Strategy of Engagement and Enlargement”. The three NSS identified the new threats impacting the changing security landscape as “transnational phenomena such as terrorism, narcotics trafficking, environmental degradation, rapid population growth and refugee flows” as long term security threats (NSS 1994, 1995, 1996). The NSS strategies were showing that America was going to be even more actively engaged on multiple levels – regional and global as far as interest, security and foreign policy is concerned. America was also recommitting itself to be a global security actor.

The Clinton administration also changed the subsequent focus of the documents for another three consecutive periods 1997, 1998 and 2000 as the new challenges on the security landscape were visible and the strategy were called– “*A National Security*

Strategy for A New Century". The key focus of the strategies was "in areas as diverse as the advancement of peace in the Middle East and Northern Ireland, the elimination of nuclear weapons from Ukraine, Kazakstan and Belarus" (NSS 1997). In his 1997, State of the Union address, President Clinton outlined for a safer, more prosperous tomorrow, seeking to

foster an undivided, democratic and peaceful Europe; forge a strong and stable Asia Pacific community; continue America's leadership as the world's most important force for peace; create more jobs and opportunities for Americans through a more open and competitive trading system that also benefits others around the world; increase cooperation in confronting new security threats that defy borders and unilateral solutions; strengthen the military and diplomatic tools necessary to meet these challenges (NSS 1997).

The second, most important aspect, of these strategies dealt with the "protection of critical information infrastructure (includes telecommunications, energy, banking and finance, transportation, water systems and emergency services) and the need for a partnership with the industries" (NSS 1997, 1998 and 2000). In addition, the 1998, strategy had specific attention towards the "failed state, globalisation, international organised crime and challenges of international law" (NSS 1998: 7). However, two significant additions were seen in the 2000 strategy, the administrations took into consideration the issues of "information warfare and emerging security complexities in South Asia (mainly India and Pakistan)" (NSS 2000). The Clinton administration released its last strategy document in 2001 - *A National Security Strategy for a Global Age* – one of the longest strategies document since 1986. The strategy centred on the issue of economic security, democracy promotion, human rights, and terrorism. Ettinger (2017: 122) argued that "the Clinton era NSSs is associated with how the United States will manage the post-Cold War security environment. More specifically, the perils and possibilities of the new world order". The fundamental focus of Clinton administration was "interdependence and globalisation, and maintenance of American supremacy" (Ettinger 2017: 122). So, it caught Washington by surprise on September 11, 2001, because no one had anticipated the growth of a non state actor- terrorist in this manner.

THE 9/11 AND IMPACT ON AMERICAN SECURITY: RISE OF NON-TRADITIONAL THREATS

The unprecedented supremacy of the US was challenged in a dramatic manner by a group of non-state actors. The dramatic attack took place at the heart of the US's superpower architecture- which was a direct challenge to American supremacy and it had major implications for the US and global security. The 9/11 also underlined the era of traditional threats to security was now confronted in addition with the rise of non-traditional threats to security and even countries like the US were ill-prepared to assess and address these threats. For the first time, the US would recognise terrorism as one of the major threats to international peace and democracy and this was listed in the NSS-2002.

In the light of the 9/11 attacks, President Bush called to “strengthen alliances to defeat global terrorism and work to prevent attacks against us and our friends”. However, America adopted unilateral action against Afghanistan and adopted a pre-emptive strategy to wage the war against Iraq in 2003. Three years into the war with Iraq and in the face of growing non-traditional threats, the NSS 2006, identified 4 types of challenges – *traditional, irregular, catastrophic and disruptive*.

Disruptive challenges from state and non-state actors who employ technologies and capabilities (such as biotechnology, *cyber* and space operations, or directed energy weapons) in new ways to counter military advantages the United States currently enjoys (NSS 2006: 44).

The US would also recognise that the cyberspace also needed to be secure and it post new challenges that the national security institutions which needed to be transformed to address them. This aspect of cybersecurity was further expanded by the Obama administration, which was also influenced by the 2007 Estonian cyber attacks and followed by “the Five-Day war” between Russia and Georgia shook the world (King 2008) in August 2008. For the first time in the 21st century, “Russia bypassed established channels of conflict resolution and unilaterally changes the boundaries of another UN member state... [That] embarked on a new era of muscular intervention, showing little faith in multilateral institutions, such as the UN Security Council” (King 2008: 6-7).

This was also the first instance when the cyber domain was used (Russian attack on Georgian cyberspace) during war time to undermine the opponent. The rise of Russia and China and their use of cyber domain both in war and peace time made a strong case for the Obama administration to give significant consideration to cyber security issues.

However, in a dramatic makeover, the Obama administration created the Cyber Command 2009, as an offensive operation wing under the Department of Defense. This was the first instance when the White House directly became involved in the cyber affairs, which was a part of the Department of Homeland Security. Likewise, the Obama administration in its first national security strategy in 2010 outlined:

cybersecurity threats represent one of the most serious national securities, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority, but our unclassified government networks are constantly probed by intruders. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale (NSS 2010: 27).

Emphasising American digital economy and development of the strategy it noted that

The Internet and e-commerce are keys to our economic competitiveness, but cyber criminals have cost companies and consumers hundreds of millions of dollars and valuable intellectual property. The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states. Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient. Our digital infrastructure, therefore, is a strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority (NSS 2010: 27).

In addition, it also outlined the strong US commitments to “deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by: investing in people, technology and strengthening partnerships” (NSS 2010: 27-28). While making cyber security and technologies as a central debate in international security, it added cautionary note that how the future of next decade is unfolding due to the impact of digital revolutions. It can be argued that technology has made the US the superpower in the twentieth and twenty-first centuries and now the same technology

is posing disruptive threats to its security, economy, politics and society. What is unprecedented in cyberspace is that although other technological developments threaten the values of territoriality, however, cyber goes beyond conventional threat and the issue of territoriality. In addition, cyber threat today can be caused by an individual who could disrupt everyday function of government, business and society just by writing a strong code and releasing that into internet highway. Yannakogeorgos has argued that, “the US cyber security strategies do not adequately address the increasing activity of authoritarian states and their corporations within the technical bodies responsible for developing the protocols and standards on which current and next-generation digital networks function” (Yannakogeorgos 2012: 103). The last security strategy of the Obama administration NSS-2015, from an American perspective was more pragmatic, than the previous NSSs. It stated that “the challenges we face require strategic patience and persistence” (NSS 2015), which was entirely based on his vision of the world politics. This approach was criticised by some because it came after a gap of five years and there was no clear approach towards unsettled relationships with China and Russia. Patrick (2015) described it as “new framework, same policies”, although it pledged for a rules-based international order. However, along with other threats, cyber threats also remained as prime focus area for the administration.

The Trump administration released its first security strategy NSS-2017, which was based on his conservative vision of world politics was entirely different from its predecessors. The NSS-2017, has given much emphasis to the “sovereignty, economic and territorial” aspects of security. In a hyper-connected world, the NSS-2017, is designed with an ‘America first’ and competition-based approach national and global issues rather than taking a cooperative and multilateral approach to global security challenges. It also underlined that there is a need to save America in a cyber era. The growing impact on technology especially the growth of the cyber domain became an integral part of America security strategy, thereby drawing attentions that the fifth domain had to be countered in all security calculations.

THE UNITED STATES AND CYBERSPACE: DIGITAL CONNECTIVITY, VULNERABILITY AND REGULATION

At the age of quantum technology, “the size of computer, speed of the internet and programmable networks have the potential not only to make the Internet faster, more secure and more accessible, but also to enable completely new types of applications that have transformed how human beings live, communicate, work and learn” (National Science Foundation 2015). In 2018, the out of 326 million US’s population, 321 million (roughly above 95 percent) are connected to the Internet. Today around 50 per cent of the world’s population have access to the Internet which was only 1 per cent in 1995. This was the time when socialisation and privatisation of the internet actually began in the US, Europe and then it was extended to other parts of the world. “Commercial firms marked this popularity and effectiveness of the growing digital world and built their own networks” (National Science Foundation 2003). The advancement in science (research and development) and technology have been used by the state to get ahead of each other in the technological race.

The US responded to the Soviet Sputnik effect of 1957, by forming the Advanced Research Projects Agency (ARPA) and promoted science and technology application in the military through the Department of Defense, which funded the research in this respects. Robert H'obbes' Zakon (2018) has highlighted in “Hobbes’ Internet Timeline 25”, that there were five researchers four from The Massachusetts Institute of Technology (MIT), namely Leonard Kleinrock, J.C.R. Licklider, W. Clark, and Lawrence G. Roberts and Paul Baran from RAND Corporation, who truly pioneered the birth of internet through their scholarly work during 1961-1966. After years of prolonged research failures and system crashes, eventually the internet was born when University College of London (England) and Royal Radar Establishment (Norway) connected to the Advanced Research Projects Agency Network (ARPANET) in 1973 (Zakon 2018, Zimmermann et. al. 2017).

Vinton Cerf and Bob Kahn the founding figures of the Internet pioneered the second phase of development of the Internet. As a result, in 1976, Queen Elizabeth II sent out the first email in the world (Zimmermann et. al. 2017). Thereafter, internet research and internet funding got paramount attentions that paved the way for the creation Defense Advanced Research Projects Agency (DRAPA) and National Science

Foundation to grant funds to many universities to establish a computer science department and undertake research on computer networks (Zakon 2018). The period 1982 – 1984, was significant for the creation of the Internet architecture as America took the lead in creating the Internet backbone which even continues to exist today. The Internet backbone such as Transmission Control Protocol (TCP) and Internet Protocol (IP), the protocol suits emerged as the tool for ARPANET. Hence, for the smooth functioning, better understanding and wider connectivity of the Internet architecture, the Domain Name Systems²¹ (DNS) were designed. Human needs words to express feelings similarly computers rely upon the language of numbers. The DNS translates Internet names (e.g. www.jnu.ac.in) into IP numbers (e.g. 202.41.10.24) for the transmission of the information across the cyberspace. In addition, the creation of the DNS made Internet address easier to remember compared with the numerical equivalents (ITU 2009). Historically, six generic top level domains (gTLDs) were established, such as - .com (for commercial entities), .net (originally for networks, now unrestricted), .org (originally for organisations, now unrestricted), .gov (government use, primarily for US government institutions and agencies), .edu (education use, primarily for US colleges and universities), .mil (military use, primarily for US military). The DNS is significant to both Internet and issues related to its governance. Since then the US has the overarching as well as ad-hoc control over the DNS since its inception, which makes the internet governance debate geopolitically very crucial, because it gives America a greater power as a state in the fifth domain.

However, prior to the Internet governance debates, there were few other significant developments, paving the way for today's cyberspace viz. Hypertext Markup Language (HTML) and WWW (World Wide Web). In 1989 Tim Berners-Lee at the European Organization for Nuclear Research (CERN), in Switzerland, proposed “a distributed hypertext system” that was originally called “Mesh” (ITU 2009). In 1990 it was fully developed for what was now known as the ‘World Wide Web’. “Hypertext thus came into use. This was a form of document formatting that allows documents to be linked by making certain words or phrases ‘clickable.’ The web is therefore the

²¹ The DNS is the addressing system for the Internet. Almost anything that interfaces with the internet (e.g. computers, mobile devices, laptops, ATMs and POS terminals) relies on DNS services to exchange information (VeriSign, Inc 2019).

sum total of the multiple ‘hyperlinked’ documents (called web pages) or other files that are stored in computers around the world over the Internet. Hypertext Markup Language (HTML) is used to create web pages and tell browsers how to display pages” (Grech 2001). This was the first phase of socialisation of the Internet. The global networks connected to the Internet exchanged about 100 Gigabytes (GB) of traffic per day. Since then, data traffic has grown exponentially along with the number of users and the network’s popularity (Navarria 2016).

During this period, the Clinton administration also came up with the idea to privatise the DNS. On 1 July 1997, the administration adopted the *Framework for Global Electronic Commerce* that directed the Secretary of Commerce to privatize the DNS (basically the internet) in a manner that increases competition and facilitates international participation in its management (US Department of Commerce 1998) and to promote digital connectivity and economy. Both private and government investments in the internet market created the dot-com boom in the US. The dot-com story was generated since 1995, when the Internet commercially reached an estimated 18 million users, who were mainly in North America and Europe. This led to speculation that the “rise in usage meant an untapped market – an international market and control over new economy” (Beattie 2004). Which resulted as the internet boom during 1995-2000 (Naughton 2016), however, the dot-com crash took place 2000 - 2002 due to excessive speculation of growth.

Although the dot-com crash took place; it did not slowdown the internet growth. In 1998, in America, the Internet Corporation for Assigned Names and Numbers (ICANN) was established as a not-for-profit, public benefit corporation, under the California Law. The ICANN has responsibility for three critical functions: “the allocation of Internet Protocol number resources for individual computers and machines; their corresponding Domain Name Service names; and, the allocation of top-level domains (TLDs) to registries that assign identifiers to individual users and organisations globally” (ICANN 2012). The ICANN does not control the “content in the Internet. It cannot stop spam and it does not deal with access to the Internet. But it does have an important impact on the expansion and evolution of the Internet” (ICANN 2012). The ICANN commenced its work under contracts with the National Telecommunications and Information Administration (NTIA), United States

Department of Commerce. This is how the US has maintained ‘very strong oversight’ on ICANN policy and extended ‘soft power’ influence on global internet governance issues.

During the second phase of Internet growth and expansion, web 2.0 (Naughton 2016), post-dot-com crash period witnessed emergence and re-emergence of new internet start-ups especially in American Silicon Valley, which would lead in the technology. Soon those became unicorn in the digital society and now they are the key players in the digital marketplace. This period marked the rise of digital social networks such as Facebook, Twitter, and LinkedIn, similarly on the other hand, digital economy saw the rise - Amazon, Cisco, EBay, that began to perform well and found acceptability among users. America took the lead also in the creation of hardware (Apple, Microsoft, Dell, Compaq, IBM and HP) and software (Microsoft, Oracle and Google) that would contribute to the expansion of the ICT, internet and the growing digital economy. During this period the numbers of internet users in America grew from 43.08 per cent in year 2000 to 95.6 per cent in 2017.

Table 4.5: US's Percentage of Individuals using the Internet

Country Name	Year					
	2000	2005	2007	2010	2015	2017
US	43.08	67.97	75	71.69	74.55	95.6

Source: ITU Statistics, 2018 and Internet World Stats, 2018

To address the new age issues such as – mobile connectivity, surveillance, cybercrime and internet governance issues, the UN-sponsored two phases of the World Summit on the Information Society (WSIS) which took place in 2003 in Geneva and in 2005 in Tunis. This was the first instance that a large number of “governments representing both developing and developed countries from all regions of the world had attempted to agree on a comprehensive international framework for governing the internet that included principles, objectives, priorities, and governance agreements” (Kurbalija and MacLean 2007: 4). It adopted the resolution and paved the way for the private sectors, civil society, NGO, academics also to participate in the summit. In the Tunis summit, the “UN Secretary-General convened a new forum for multi-stakeholder policy dialogue called the Internet Governance Forum (IGF)” (Kurbalija and MacLean

2007). However, these proposals were not welcomed by the US government because the Summit urged for a multilateral approach and second, it posed a challenge to ICANN as it is not an intergovernmental organisation like the ITU (Weinberg 2011: 200). Third, it would undermine US dominance of the Internet.

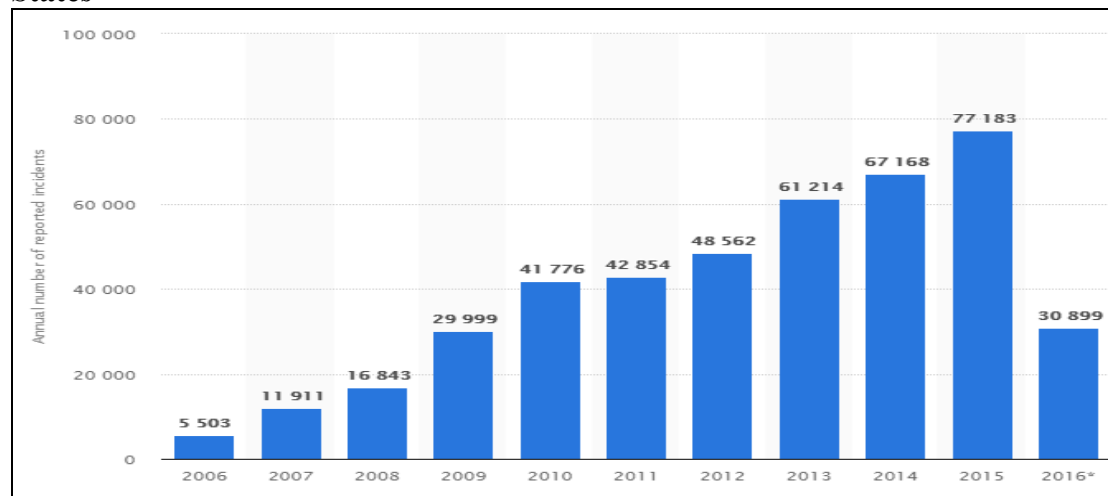
The European and other countries were however, unhappy with the US's influence on internet governance and the ways the domain names were being assigned (ASIL 2007). As a result, two big shifts emerged in 2009 under a new agreement among between the US government, ICANN, and the Affirmation of Commitments (AoC). However, the issue of representation, influence and accountability was far from being resolved. Second, it also witnessed 'power distribution', between the ICANN and national registers (Christou 2016: 37) which signalled the slow redistribution of power over internet governance between the US and other states. In 2012, at the World Conference on International Telecommunications (WCIT) in Dubai, Russia made an unsuccessful attempt to integrate the ICANN within the ITU, so as to curtail the US' influence (Weinberg 2011: 213) over the Internet. However, in contrast to the proposal, western and industrialized countries supported the existing ICANN governance model and refused to endorse the WCIT and Russian proposal (Pohle and Morganti 2012: 40).

The entire gamut of cyberspace debates got a major global attention in 2013, when the former National Security Agency contractor Snowden revealed about the US's mass surveillance on global internet communications. To guide the future of Internet Governance, to guide the future of internet governance and to reduce American influence over ICANN, Brazil convened NETmundial on 20 May 2014, in Sao Paulo, though it failed later to build any global consensus. The Snowden revelations also fed more general concerns about the existing systems of Internet governance, and led to a call for a new international multilateral (a government dominated) governance order. This was supported by the governments of Pakistan, Ecuador, Venezuela, Cuba, Zimbabwe, Uganda, Russia, Indonesia, Bolivia, Iran, and China (Shears 2014). However, all these developments could not make any impact on the US influence on the Internet.

Internet governance has been the key issue of the debate of the cyberspace since the 1990s. However, in October 2016, the Obama administration agreed to let the Department of Commerce pull out its control over the IANA which functions under the ICANN, effectively “ceding the last control that the US had over the Internet to an ambitious non-profit organization that will have no ties to the US Government” (Westby 2016). Although, the US gave away the control over the technical part of the internet governance, yet its influence still prevails. Cyberspace possesses both opportunities and poses disruptive challenges. For example, more recently, social media platforms were used to challenge authoritative regimes in the Arab world.

Cyber security threats emerged as a critical concern for the Obama administrations. James A. Lewis, one of the leading cyber analysts said “this (cyber issues) is a global problem and we are not doing enough to manage the risk” (Nakashima and Peterson 2014). According to the *Internet World State*, approximately 95 per cent of the US’s total population are connected to the Internet and simultaneously more than 240 million are active on Facebook. This growing digital connectivity shows the significant opportunities and challenges of digital economy to politics, economy and security (the 2016 US presidential elections are being investigated for manipulation of voter preferences through social networking platforms). A study on *Cost of Data Breach Study: Global Analysis*, states that over “37 percent of global incidents involved a malicious or criminal attack, 35 percent concerned a negligent employee or contractor (human factor), and 29 percent involved system glitches that includes both IT and business process failures” (Ponemon Institute 2013: 7). In this context, the *Wired*, one of the tech-foci magazines ran two stories, – in 2012 “*Does Cybercrime Really Cost \$1 Trillion?*” and in 2017 “*Global cybercrime. Costs a trillion dollars. Maybe 3*” thus, showing how swiftly and quickly the cyber crime industry is growing. Cyber threats are on the surge and will continue to be a concern for the foreseeable future. Stewart A. Baker, a former Department of Homeland Security policy official also holds that “the more that government understand what those costs are, the more likely they are to bring their laws and policies into line with preventing those sorts of losses” (Nakashima and Peterson 2014).

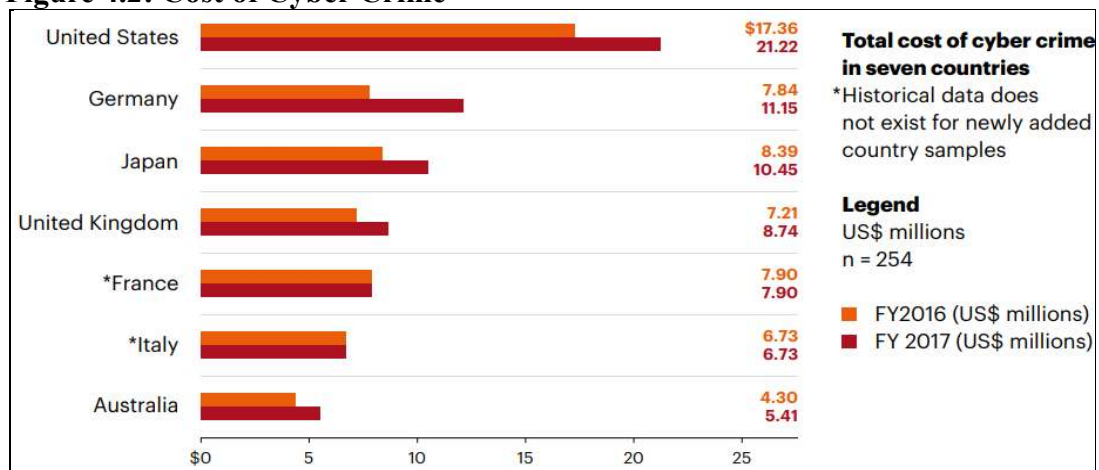
Figure 4.1: Cyber security incident reports by federal agencies in the United States



Source: Statista, 2018

The cyber revolution holds a lot of promise for the US economy and security, however as figure 4.1 shows there has been an unprecedented growth in cyber attacks which is cause for concern. In recent past, the US companies have been the prime target of the cyber attacks - 2014 and 2015 seems to be shocking years for - JPMorgan Chase, Home Depot, Target, Sony, Anthem, Inc., and Ashley Madison – as personal and private data got compromised by massive cyber attacks (Walters 2014, 2015). That made FBI Director James Comey, comment that, “there are two kinds of big companies in the United States. There are those who’ve been hacked...and those who don’t know they’ve been hacked” (Cook 2014). In 2016, figures recorded approximately 60 percent decrease in the cyber incidents, but it was largely due to changes in the US federal reporting guidelines (Statista 2018).

Figure 4.2: Cost of Cyber Crime

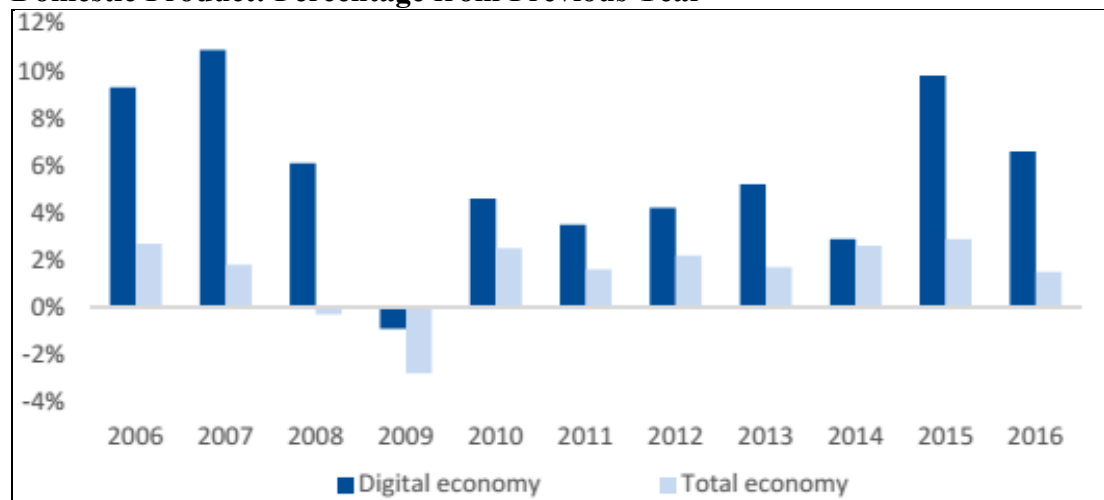


Source: Ponemon Institute, 2017

The sectors of US companies impacted by cyber attacks are in the areas of “finance, energy and utilities, and defense and aerospace, three of the most affected sectors as well as communication, retail, and health care” (Walters 2015). The *Ponemon Institute* report on *2017 Cost of Cyber Crime*, analyses the cost of all cyber crime for a variety of 254 companies in seven countries (see Figure 4.2) both public and private. The US in comparison with other countries in the study, continues to rank highest in the cost of cyber crime at an annual average of \$21.22 million which was \$17.36 million in 2016 (Ponemon Institute 2017: 13). However, on the other hand, a Symantec report on “Internet Security Threat Report, 2018”, analysis on targeted cyber attacks underlined that, “the US ranked first continuously for the past three years, followed by India and Japan are in number two and third position respectively” (Symantec 2018: 32).

Besides this, The Centre for Strategic and International Studies, a Washington based think tank report *Economic Impact of Cybercrime—No Slowing Down in 2018* has estimated that “the annual cost of cybercrime and economic espionage to the world economy is at more than \$600 billion or almost 0.8 per cent of global GDP” (Lewis 2018: 4). The digital economy has huge potential for the US national growth (figure 4.3). According to the US Bureau of Economic Analysis (BEA), estimate, the digital economy “grew at an average annual rate of 5.6 percent, outpacing the average annual rate of growth for the overall economy of 1.5 percent. In 2016, the digital economy was a notable contributor to the overall economy—it accounted for 6.5 percent of current-dollar GDP, 6.2 percent of current-dollar gross output, 3.9 percent of employment, and 6.7 percent of employee compensation” (Barefoot et. al. 2018: 12).

Figure 4.3: Digital Economy Real Value Added and Total Economy Real Gross Domestic Product: Percentage from Previous Year



Source: US Bureau of Economic Analysis, 2018

The digital revolution is becoming the key driver of the US economy and development. On the other hand, growing cyber attacks from internal and external actors have been multiplying the risk of vulnerabilities to the US political system, security, economy and society.

To address such issues, private industry and government need to support each other to enhance the ability to act against cyber criminals. The issue of cybercrimes has also become more urgent due to the transnational nature of the threats and lack of international cooperation, treaties, convention and law to address it at the global level.

THE UNITED STATES AND CYBER THREATS: ISSUE OF DATA PROTECTION

The last three Presidents of the US namely - Bill Clinton, G.W. Bush Jr., and Barack Obama – have cautioned about the security risks of the cyberspace. President Clinton’s remarks at the Technology Conference in San Francisco in 1998; President Bush’s Remarks at the World Bank in 2001 and United States Military Academy at West Point in 2008; and President Obama’s various speeches and executive orders have significantly underlined issues about – digital economy, cyber terrorism, protection of critical information infrastructure and other cyber threats. In this context, the release of the *National Cyber Security Strategy*, 2003 by the Bush Administration; *Department of Defense Strategy for Operating in Cyberspace*, 2011 and *International Strategy for Cyber Space Prosperity, Security, and Openness in a*

Networked World, 2011, by the Obama administrations shows the US commitments to address various issues of cyberspace both at the national and international level. President Obama at the Cybersecurity and Consumer Protection Summit, in Stanford University, California, in 2015 “it’s one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm. The same information technologies that help make our military the most advanced in the world are targeted by hackers from China and Russia who go after our defense contractors and systems that are built for our troops. The same social media we use in government to advocate for democracy and human rights around the world can also be used by terrorists to spread hateful ideologies. So these cyber threats are a challenge to our national security” (Obama 2015). Further President Obama outlined four basic principles to address these new threats – first, public private partnership, second, focus on unique strengths of both sides, third, to constantly evolved, and fourth, he stressed “in all our work we have to make sure we are protecting the privacy and civil liberty of the American people” (Obama 2015). This clearly indicates it is also important to understand the prevailing international cyber social contract and state of cyberspace.

The CSIS has conducted a study (2006-2018)²² on significant cyber incidents around the world on the basis of publicly available/reported incidents.

Figure 4.4: The US: Significant Cyber Incidents



Source: CSIS, 2018

²² This is continuous research project which updates on the basis of incidents reported and cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.

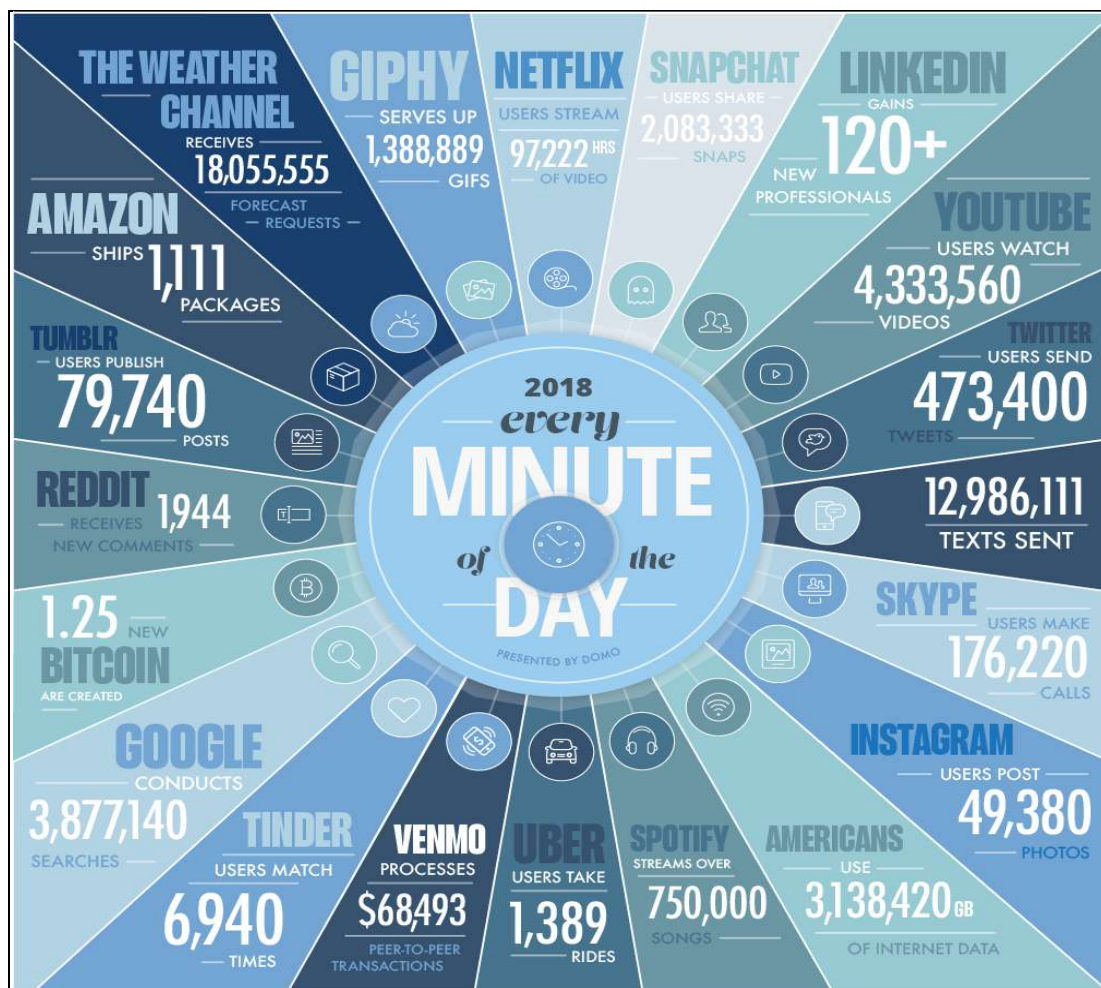
The figure 4.4 clearly shows that the US tops the list of cyber victims followed by India, South Korea, UK and China. The growing cyber incidents such as hacking, data breaches, political espionage, economic espionage, DDoS attacks, defacing government websites, social media hack, identity theft, social engineering and attack on critical information infrastructure became a paramount concern for the US government, businesses and society.

The DHS also underlies the fact that cyber security is critical to everyday life, economic vitality and national security (DHS 2018a). It further stated that underlying cyber infrastructures are vulnerable to a vast range of risk stemming from both physical and cyber threats and hazards. The rise of sophisticated cyber non-state actors and nation-states exploit vulnerabilities to steal information, data, money and disruptive capabilities has significant implications for the national and human security (DHS 2018a). According to a report published in July 2018 from the Office of the Director of National Intelligence stated that three countries (Russia, China and Iran) have conducted sophisticated, large-scale hacking attacks across multiple US industries, targeting the networks of technology and manufacturing contractors, defense contractors ... (Fortune 2018, The Reuters 2018).

The Trump administration has also placed cyber security matters at the forefront of the national security. The first National Security Strategy 2017 of the administration documented that the cyber threat is key area of concerns to national security. After a gap of 15 years, the second National Cyber Security Strategy was released in 2018. These developments highlighted the US has been proactively engaged in addressing the cyber security issues both by adopting strategies and building new institutions. For example, in 2009, US Cyber Command (USCYBERCOM) was created and located within the NSA, and had a defensive mission. In 2018, it was elevated to the status of full and independent unified combatant command and is one of the 10 unified commands of the US DOD. This was clearly documented in his first NSS-2017 that “as the reliance on computer and connectivity increases, the US becomes increasingly vulnerable to cyberattacks. Businesses and individuals must be able to operate securely in cyberspace” (NSS 2017: 13). In addition, the NSS-2017 further stated that while keeping safe America in the cyber era, “the government must do a better job of

protecting data to safeguard information and the privacy of the American people. Our Federal networks must be modernized and updated” (NSS 2017: 13). According to the Pew Research Center, social media interactions are extremely popular among Americans for various purposes. On the other hand, the concerns of the American public over the Cambridge Analytica’s use of Facebook data has a renewed concerns on how social media companies collect personal information and make it available to marketers (Rainie 2018).

Figure 4.5: US and Data Creation in every Minute, 2018



Source: Data Never Sleeps 6.0

The US as a sovereign nation has well established institutions, strategies and capabilities to address cyber offensive or defensive adversaries, however it lacks a unified data protection authority to protect individual privacy and data in the digital age. The study on Data Never Sleeps 6.0 suggested an American uses 3,138,420 GB

of internet data in every minute of the day in 2018 (see fig 4.5 above). That is significantly huge and such data are crucial to US LEAs, businesses, non-state actors and also creates issue of individual privacy and data protection. Recently reported data leaks in the US have raised several question marks on the US ‘patchwork quilt’ approach to address privacy and data protection. Cyber security and data protection go hand in hand and thus the US needs to address both issues with equal administrative and legal measures.

THE UNITED STATES’ APPROACH TO CYBER SECURITY

In the age of digital economy and growing internet connections, government, military, private corporations and retail shoppers have shifted their offline activities and functions to the World Wide Web, thus making cyber security a pressing concern for the US. The threats to cybersecurity are unlike any other security problem that the US has faced before. Harknett and Stever (2011: 455) argued that, “the cybersecurity problem does not fit conventional or traditional security categories based on individual security responsibilities, economic or corporate security issues, military security problems, as well as domestic versus international problems”. Thus, it requires different sets of approaches. According to Radu (2017), global actors have brought in a different lens to identify the threats in the cyberspace. The US’s approach to cyber threats is fundamentally underlined by national security apparatus²³. According to Phole (2017), the US pursues an economic approach to Internet policy in general but emphasises the role of a state centric approach to address cyber security issues, more particularly²⁴. The approach of the US to cybersecurity can be understood in three parameters – the Presidential approach, relationship with other countries and issues of civil liberties. The US’s approach to the information age was initiated by the Clinton administration, but it got momentum during the Bush administration.

²³ This point was mentioned by Dr. Roxana Radu, in a Skype interview to the researcher on 13 March 2017 in Berlin, Germany.

²⁴ This point was mentioned by Dr. Julia Pohle, in a personal interview to the researcher on 23 March 2017 in Berlin, Germany.

Table 4.3: Evolution of the US Approach to Cyber Security

Year	US Cyber Security Approach	Outcome
2000	The National Plan for Information Systems Protection	Protection of critical cyber infrastructure (securitisation of information age)
2001	9/11 Terrorist Attacks	Disruptive impact of technology on national security
2003	National Strategy to Secure Cyberspace	Identified cyber threats to national security
2006	National Infrastructure Protection Plan	Identified 17 infrastructure sectors, including agriculture, water, energy needs to be protected
2008	Comprehensive National Cybersecurity Initiative	Federal coordination between local governments and private sectors to develop cybersecurity technology
2009	Creation of the Cyber Command	Militarisation of Cyberspace
2009	National Cybersecurity and Communications Integration Center	Integration of different existing structures to address cyber threats
2010	Stuxnet	First cyber-war agent
2011	International Strategy for Cyberspace	Normative approach to cyberspace
2011	Department of Defense Strategy for Operating in Cyberspace	Military Cyber Modernisation
2011	Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise	Internal cyber capacity building
2013	NSA Global Surveillance	Cyber Hegemon
2015	The Department of Defense Cyber Strategy	Cyber Defense and Strategic Approach
2018	U.S. Department Of Homeland Security Cybersecurity Strategy	Resilient cyber secure future
2018	National Cyber Strategy of the United States of America	Securitisation of Cyberspace
2018	USCYBERCOM, independent unified combatant command	Weaponisation of Cyberspace
2018	CLOUD Act	Government oversight on Data

Source: Author's work developed in consultation with Ph.D. supervisor

The 9/11 terrorist attacks had a catalytic impact on US's approach to security in the 21st century, shifting the entire focus of the administration to address the terrorist issues. In addition, the US government was well aware of the emerging challenges from the information and communication technology. To address those challenges, the administration adopted the National Cyber Security Strategy 2003 (NCSS), the National Infrastructure Protection Plan 2006 and the Comprehensive National Cybersecurity Initiative 2008 to protect critical infrastructure and national cyber defense. The Bush administration's approach to cybersecurity is closely influenced by the Cold War realpolitik, in other words he used "deterrence logic to solve cybersecurity problem and bottom-up policy" approaches (Harknett and Stever: 456), because it has empowered the DHS as the nodal body to deal with cyber security activities. The Obama administration recognised the cyber risks and challenges, therefore, ordered then national security and homeland security advisors to examine the cybersecurity issue and develop a policy blueprint (Nojeim 2010: 121).

In a span of few years, DoD, DHS, and the White House released several strategies to deal with cyber threats (see table – 4.3 above). The Obama administration turned upside down the Bush approach to cyber security and directed a review team of government experts to conduct a 60-day 'clean-slate' review assessment. Furthermore, he used 'top-down, rational, comprehensive' approach to cyber security (Harknett and Stever: 457) which was dramatically different from the Bush period. He made the White House the nodal point for cyber security discourse, while DHS and DoD remained as core bodies for capacity building, threat assessments and threat mitigation. The Trump administration used only one part viz. 'top-down approach' from the Obama administration. Trump administration's four recent actions – NSS 2017, NCSS 2018, CLOUD Act 2018 and unified Combatant Cyber Command underlined a state centric approach to cyberspace. In other words, Trump administration has adopted a 'top-down, deterrence logic, realpolitik' approach to cybersecurity.

To understand the second aspect of US cyber security approaches there is a need to examine the US's cyber relations with third countries like India, EU member states, China and Russia.

The US and Third Country Cyber Relations

The United States and China are the two most significant national actors in the digital realm and these two leading states represent quite different views on the proper use and future of the Internet (Kenneth and Singer 2012). Out of the many issues, one of the major issues that stands out in the US- China cyber dialogue is the use of different cyber jargons - “information and cyber attack” (Kenneth and Singer 2012: vi-vii). Since the Clinton administration, China has been considered as one of the key threats to the US’s interest and security. Moreover, “since the early 2000s, cyber espionage issues have increasingly strained U.S.-China relations. ... In 2010, suspected Chinese cyber activities started to become a regular topic of discussion inside the U.S. government and press. By 2011, the eye-popping scope of China based cyber espionage catapulted the issue to centre stage, as new intrusions into U.S. corporate and government networks were reported on a regular basis” (Brown and Yung 2015). But Lan (2011) argues, there was a kind of good gesture ‘in the early 2011, Chinese authorities and the U.S. FBI conducted joint operations to dismantle and shut down an illegal website dealing with child pornography’ (Kshetri 2014: 11). However, except for a few “instances of successful cooperation, allegations and counter-allegations have been persistent themes in dialogues and discourses in the U.S.-China relationships in cybersecurity” (Kshetri 2014: 11).

Both the countries had reached the consensus to end the cyber stalemate in April 2013, as China's Foreign minister Wang Yi and U.S. Secretary of State John Kerry agreed to work together on cyber security and moved to ease months of tensions and mutual accusations of hacking and Internet theft (The Reuters 2013). The matters got complicated when the NSA contractor Snowden exposed the US’s hidden agenda of global surveillance programme to collect, store and analyse billions of metadata of both friends and enemies. This particular incident again kick started the cyber ‘blame game’ (Edwards et.al. 2017) between US and China.

The cyber stalemate further intensified in 2014 when for the first time in history, the US levelled cyber criminal charges against China. In a landmark judgement, the Justice Department indicted five members of the Chinese military on charges of hacking into computers and stealing valuable trade secrets from the leading steel, nuclear plant and solar power firms (Nakashima and Wan 2014). In another massive

cyber attack on the Office of Personnel Management (OPM hack) in December 2014, which compromised the fingerprint records of 5.6 million people and Social Security numbers and addresses of around 21 million former and current government employees (Peterson 2015) – China was blamed and criticised in various US media outlets. Adam Segal, one of the leading cyber experts at the Council on Foreign Relations has argued that, ‘China has drawn unwanted attention with its aggressive efforts to break into US government and business computer networks to steal information. The attacks are aimed at giving China a competitive economic advantage’ (Segal 2013: 38). Despite the blame game, the RAND research report - *Getting to Yes with China in Cyberspace* – underlines that the cybersecurity researchers of both the sides have ‘recognised the importance of finding a path forward on this issue, either through bilateral negotiations, multilateral agreements, or both’ (Harold 2016: 4).

Perhaps, more importantly, Chinese President Xi Jinping’s visit to the US and signing a ‘handshake agreement’ (Greer and Montierth 2017) cyber cooperation agreement with President Barack Obama in 2015, ended the long standing cyber stalemate. This was a ‘good first step’ (Harold 2016) towards a comprehensive cyber cooperation. There has been steady progress between the US and China cyber diplomacy and likewise, a significant amount of drop of direct cyber espionage.

China is not the only actor that poses threats to the US digital endeavours rather in this digital world, ‘the US and its adversaries have been at war for some time. Some of the largest U.S. threats are buzzing through Russian and Chinese computer systems operated by droves of highly skilled hackers’ (Summers 2014). In the post-Cold War period, both the US and Russia have followed some sort of common grounds to discuss cyber issues. However, they have similar disagreement on cyber jargons – data localisation, data sovereignty and information security, which Russia believes, states should oversee the cyber security matters. Nonetheless, Bryan-Low (2005) has argued that, “in the mid 2000s, U.S. law enforcement officials reported receiving help from their Russian counterparts on about one out of six cybercrime-related requests (Kshetri 2014: 14). Swartz (2008) reported that Russian cybersecurity agents were also trained in the U.S. (Kshetri 2013: 59). Moscaritolo (2010) reported that one of the most important signs of cooperation was Russia’s arrest of a St Petersburg-based

hacker, Viktor Pleshchuk who was indicted by the U.S. for stealing US\$9 million from the U.S. division of the Royal Bank of Scotland in 2006 (Kshetri 2014: 14). But, in 2009, during President Obama's visit to Moscow, the US and Russia cyber cooperation halted due to different views on the behaviour of states on a treaty for cyberspace (Markoff and Kramer 2009).

In this connection, The East West Institute's report - *Russia, The United States, And Cyber Diplomacy Opening the Doors*, upholds the fact that there is a 'clear and present danger in the digital world' and to address this it has four sets of recommendations "Public Key Infrastructure; Cyber crime emergency response; International cyber law; NATO-Russia cyber military exercises and exchanges" (Gady and Austin 2010). The report concluded that, "there is no shortage of political leaders and security specialists in both countries who see the relationship as essentially confrontational: their offensive threat, our defensive countermeasures. For these people, the idea of "common security" in the cyber domain does not have much appeal" (Gady and Austin 2010: 19). The report also draws the attention to common security challenges that "the common vulnerabilities are immense: from personal information, banking records, and controls on sensitive medical equipment to the controls on nuclear power plants and nuclear missiles" (Gady and Austin 2010: 19). On a positive note, the report puts forward a progressive perception for both the countries by saying

Consequently, old policy paradigms will have to change. Outdated concepts such as deterrence through mutual assured destruction make no sense in cyberspace. If Russia and the United States can begin to open the doors of their cyber homes a little more widely, this will be a major step toward building trust, safeguarding information infrastructure, and promoting an open information society at the global level (Gady and Austin 2010: 19).

In 2011, both the countries did 'reset' their cyber diplomacy and discussed steps to reduce cyber vulnerabilities through active diplomacy, policy coordination and technical collaboration (Schmidt 2011). All these new developments have shaped up in the milieu of US's International Strategy for Cyberspace, 2011. The cybersecurity pact also took into consideration the issue of information sharing and improving communication on security matters (Montalbano 2011).

In the backdrop of the G-8 summit in June 2013, the US and Russia signed ‘a landmark agreement to reduce the risk of conflict in cyberspace through real-time communications about incidents of national security concern. The pact, the first of its kind and was cast as a part of a broader bilateral effort to improve cooperation, including on counterterrorism and weapons of mass destruction’ (Nakashima 2013). This pact has also adhered to ‘ICT Confidence-Building Measures’ and created significant and ‘direct link House-Kremlin Direct Communications Line’ (The White House 2013). However, the Snowden revelations; disagreements, which intensified during the International Telecommunication Union summit on Internet governance (Sharikov 2013) and Ukraine crisis has impacted the US-Russia relationship. In 2015, a bilateral agreement between China and Russia was signed and this sent a warning signal to the US economic and security interests in cyberspace (Kulikova 2015). Wei (2016), argued that the Sino-Russian cyber-bromance “seemed to mark further Sino-Russian cooperation another arena—cyberspace. The pact has two key features: mutual assurance on non-aggression in cyberspace and language advocating cyber-sovereignty” (Wei 2016).

She further argues that, “if this pact is merely treated as a “non-aggression” pact, then Sino-Russian cybersecurity cooperation has a similar pattern to their overall relationship, which appears to be intimate but is actually problematic. However, looking past the non-aggression elements of the pact illuminates the key element of the agreement—China and Russia’s pronounced support for the concept of “cyber-sovereignty.” The support for cyber-sovereignty echoes the centrepiece of Sino-Russian cooperation in the general terms—a challenge to US dominance in the international system” (Wei 2016). After Russia’s alleged involvement in the US Presidential 2016 elections, it created a huge domestic and international furore that put the US-Russia bilateral cyber relations at a stake.

With the second largest population of internet users in the world, India’s increasing use of the Internet means it is also increasingly vulnerable to cyber warfare, cyber attacks and data theft. The government's digital push through policy initiative and its ambitions to be an active player in international cyber rule book makes it a destination for digital innovations and investment; likewise, its dependency on imported technology makes it necessary to have good relations with the leading cyber actors.

Unlike, Russia and China, the US and India have begun discussion on cyber security. They often share common interest while addressing cyber security issues and “have engagement on cyber security issues since 2001, when the Indo-US Cyber Security Forum was first established, concrete cooperation to manage the threat remains minimal” (Saran 2014: 5). After a decade of ‘waiting game’ (Gady 2012), the cyber discourse between the US and India has gained a considerable momentum. The Fourth US-India Cyber Dialogue was held in August 2015, led by India's Deputy National Security Advisor Arvind Gupta and the US Cybersecurity Coordinator and Special Assistant to the President, Michael Daniel. The dialogue encompassed a wide range of cyber issues including cyber threats, enhanced cybersecurity information sharing, efforts to combat cybercrime, Internet governance issues, and norms of state behaviour in cyberspace (MEA 2015). The commitments, to an open, interoperable, secure, and reliable Internet, underpinned by the multistakeholder model of Internet governance were reaffirmed again when Indian Prime Minister Narendra Modi visited US in June 2016 (PIB 2016).

In spite of having strong commitments, ‘the idea of a formal treaty to regulate cyber warfare draws mixed responses. For an entirely different set of reasons the US and India are both ambivalent towards cybersecurity treaties’ (Mohan 2014: 12). India’s issues pertaining to data sharing, data access, information sharing and individual privacy often stands in between the relationships. Although, they share common concerns on many grounds yet most of their approaches are based on the traditional rulebook. Most of the Indian data storage is under US jurisdictions and to access those data, New Delhi has to go by certain by-laws and a lengthy mutual legal assistance treaty (MLAT) procedures. On the other hand, for the US digital economy, the Indian marketplace provides a trillion dollar opportunity. In view of this, new cyber relationship is shaping up between Washington DC and New Delhi.

To understand the third aspect of the US’s cyber security approaches, there is a need to examine the US’s legal and civil liberty rules with respect to digital privacy.

The US and Digital Privacy

Technically, privacy comes under natural rights of all living being in the US. In 1890, Samuel Warren and Louis Brandeis, first coined the term ‘right to be let alone’ (Warren and Brandeis 1890) in a seminal article published by the Harvard Law Review. It is often understood as the first declaration of the US right to privacy. This was written in response to the technology of times - the newspapers - violating the privacy of influential people by printing stories about them (Data Security Council of India 2010). Things have been unprecedentedly altered by the growth of digital technology. Does a free society like the US need a new set of privacy laws? How does a marriage between offline and online privacy shape up? Does data protection regulation hold the key? How is the data protection debate in the US different from other parts of the world especially in EU? These are the critical questions with regard to data protection and privacy in the US.

Table 4.4: The US and Data Protection

Year	US: Privacy and Data Protection	Outcome
1792	Fourth Amendment to the United States Constitution	Right to Privacy
1974	Privacy Act 1974	Unwarranted intrusion to individual privacy
1978	Foreign Intelligence Surveillance Act	Judicial and congressional oversight on the government’s covert surveillance activities of foreign entities and individuals in the US
1986	The Electronic Communications Privacy Act	Governments restrictions on wire tap and computer data
2000	Safe Harbour Privacy Principles	Cross border data flows between the EU and US
2001	Terrorist Attacks	Impact: Individual liberty being compromised
2001	The USA PATRIOT Act	Empowerment of law enforcement agencies (LEA) – rise of surveillance society
2013	NSA Surveillance	Impact: Global outrage against individual privacy and data protection
2015	The CJEU’s Schrems judgment	End of Safe Harbour Privacy principles
2015	United States v. Microsoft Corp	LEA access to the cloud

		data
2016	Privacy Shield Agreement	Protection of EU data subject
2016	Russian Influence in the Presidential Election	Freedom of expression being compromised
2016	FBI–Apple encryption dispute	LEA influence to undermining the encryption standards
2018	Facebook–Cambridge Analytica data scandal	Lack of legal structure to protect individual privacy and data protection
2018	The Clarifying Lawful Overseas Use of Data Act	Global digital sovereignty
2018	Google+ Data Breach	Need for Privacy protection

Source: Author’s work developed in consultation with Ph.D. supervisor

Prior to the 9/11 terrorist attacks, the US legal structure provided several judicial protections to individual privacy (see table 4.4 above). The response to the 9/11 attacks had a significant impact on the legal and civil liberties rights of the Americans. The Bush administration adopted the ‘USA PATRIOT Act’, 2001, which created an overarching surveillance mechanism to monitor the activities of foreign nationals internally and internationally. The fertile terrain of Internet is fragmented by national laws. The global legal architecture is too fragile which substantially helped the US NSA to execute the world wide surveillance. The US privacy laws have developed slowly, in response to societal needs, but the country still has no overarching regulations. The fourth Amendment originally enforced the notion that ‘each man’s home is his castle’, secure from unreasonable searches and seizures of property by the government (US Constitution Fourth Amendment).

The new digital age needs to sharpen the rules. Within US common law, there were four privacy torts, which continue to exist today (Wade 2010) and distinct laws that protect information related to health, video rentals, educational records, credit reports etc (Wade 2010: 662). The US does not have a dedicated data protection law nor a single regulatory authority for overseeing data protection issues. Rather a patchwork quilt approach has arisen from the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act of 1996, Federal Trade Commission Act, Wiretap Act, etc (Jay 2014).

In the recent past, the Obama administration drafted two significant bills to stop misuse of personal data. The Student Digital and Parental Rights Act of 2015, sets to propose that students data must be protected and should not be used for the marketization of the education. Second, the Consumer Privacy Bill of Rights Act of 2015, seeks “to provide customers with more control over their data, companies with clearer ways to signal their responsible stewardship over data, and everyone with the flexibility to continue innovating in the digital age” (Chernichaw 2015). Since both the bills have not been enacted, it would be difficult to decide the future and final outcome of it. In the recent pasts, the legal tussles between the US LEAs and US companies (Microsoft, Apple, Facebook, and Google) are also raising questions about the US commitments to individual privacy and data protection in the digital age. In contrast to its internal privacy standards, the way the US companies and government agencies are using individuals’ personal data has given rise to a key legal tussle between the EU and the US.

CONCLUSION

The collection of large metadata and global interception of international content under the Foreign Intelligence Surveillance Act (FISA) which was amended several times after the 9/11 terrorist attacks, is a significant setback for the US data protection approach - the creation of the Department of Homeland Security in 2002, transformed the US with a surveillance state which will empowered the law enforcement agencies to make use of the latest technology to track all behaviour and activities of citizens and non-citizens alike. States around the globe have been working to create strong data protection regulations that could stop the misuse of personal data. In spite of being in the age of big data, algorithms and artificial intelligence which undermines the ‘core’ concept of privacy, a strong, updated and regulated data protection and privacy standards both at national and international level is the need of the hour. There is also a necessity of bringing about some reformation in the FISA to put restraints on NSA surveillance. In addition, a strong consumer protection privacy act would help to boost the digital economy of the domestic market. Furthermore, international collaboration in harmonising international legal standards and free flow of digital trade also needs to be addressed carefully.

CHAPTER 5
THE EUROPEAN UNION AND THE UNITED STATES APPROACH TO
CYBER SECURITY

“Power is a curious thing: ... Power resides where men believe it resides. It's a trick; a shadow on the wall and a very small man can cast a very large shadow”

(George R. R. Martin 1991)

INTRODUCTION

This chapter seeks to analyse the interplay between the traditional concepts of ‘power’ and ‘interest’ in a digital age with respect to the EU and the US. It examines how both actors’ regulations are shaped in regard to data protection, privacy and their dealings with the digital age challenges? Although, both the EU and the US have various common parlances and share a similar political culture and a liberal social order, yet many things are not as equal as it appears to be in the digital realm.

Since the beginning of the Cold War, the Transatlantic relationship has emerged as an epitome of discourse in the realm of global governance and security. Technically, this synergy first began during the British American Treaty, 03 September 1783, between the representatives of King George III of Great Britain and the United States of America. This understanding between US and Great Britain became a continuing partnership for many centuries. The US engagement with more contemporary Europe took place during the World War I, with President Woodrow Wilson’s 14 points at the Versailles Peace Conference and the US entry into World War II. During the Cold War period, the partnership became significantly stronger through the Marshall Plan for European economic reconstruction and NATO that created a security community in the Atlantic region. In the post - Cold War period, to manoeuvre the power vacuum that emerged after the disintegration of the USSR, the enduring partnership between the EU and the US has become crucial to the global security landscape.

Above all, in the digital world, modern technologies and technical knowhow have truly diffused power as well as translated the meaning of interest based engagements. However, in the cyber age, state proxies, role of small states and self motivated individuals can pose a serious threat to the most powerful countries of the world. In a technology driven world, the 240 characters of the twitter bird do carry disruptive

risks to domestic, foreign and security policy. Leaders of the digital world need to understand the impact of digital diplomacy vis-à-vis the urgency of global security, which is why, an enduring transatlantic partnership, is very crucial for the global political and security order. In a digital age, the types of partnership the EU and the US are creating between the Atlantic Ocean is keenly observed by other powers. The relevant question here is how convincingly and comprehensively is a centuries old partnership re-positioning itself in the digital realm? At the global security landscape, both countries have to overcome newer challenges. Further, how things are rapidly changing during the Trump administration are the key concerns for Europe in general and particularly for the EU. However, in the post-GDPR era, where are the points convergence and divergence between the EU and the US and are their interests on the issue of ‘Data and Privacy’ alike is of critical concern and this has been examined by this research.

THE EU’S CYBER-PREPAREDNESS

Cyber security has emerged as a key global challenge in the 21st century. The two factors which have a prominent influence on cyber security are – unpredictability and vulnerability. First, the ‘unpredictability’ is in locating the threats (unknown unknowns) – wherein the cyberspace has created a horizon that diffuses the threats, reduces the threshold of risk and produces an unpredictable challenge to the traditional syntax of security and strategic perceptions. Second, it creates a sphere of ‘vulnerability’ to national and human security (known unknowns) – the ubiquitous connectivity that has altered the way governments, business and individuals engage every day.

The universal connectivity has become a driving force for the global economy. Simultaneously, insufficient technical (hardware and software) security solutions have made it easy for the cyber criminals to attack the networks. In addition, a dearth of international legal framework on cyberspace has also left open the field of cybersecurity in the absence of regulation. Moreover, here it implies the emerging role of multi-stakeholders in protecting individual liberty, fundamental rights and privacy of individuals in a digital age. As societies are espousing newly invented disruptive technologies, the issues linked to the collection (intelligence and security), storing, sharing, use and misuse, abuse of personal data/information has emerged as

primordial concerns for the stakeholders. This is an emerging interplay between the interest and power in a borderless world that entails how the future of tech, industries, governments, societies, organisations and individuals are going to interact with each other at various intersections?

The European Union is an emerging global actor with its two distinctive approaches - the 'community' (Sbragia 1993: 23) approach for an European economic union and 'intergovernmental[ism]' (Keohane and Hoffman 1991 and Moga 2009: 796) approach for European security structure. However, the creation of the *European Single Market in 1993* sought to bring enable the "four freedoms – free movement of goods, capital, services and labour within the Union" (European Commission 1993) that became successful via the adoption of the *Schengen Area in 1995* to officially 'abolishing borders' (European Commission 2013) to encourage free movement of people'; common policies on trade, agriculture, the revoking of national currencies to embrace the common currency the '*Euro*'.

Furthermore, the Common Foreign and Security Policy (CFSP) has spearheaded the Union as a growing security actor as well as norm promoter in global affairs. At the digital level, espousal of the "*Digital Single Market*" to 'bringing down technical barriers to unlock online opportunities" (European Commission 2017e) and totally abolishing roaming charges in the EU from June 2017 indicates the intention, commitments and enthusiasm of a future 'European Digital Union' with a promise of 'open, safe and secure' norm-based digital world order. On the other hand, agreeing to reinforce the security and defence mechanism within the EU with the Permanent Structured Cooperation (PESCO) on 13 November 2017 (European Council 2017b) has also unfolded the emerging 'intergovernmental commonness' to create a 'European security union'.

In an interconnected world order, the EU has been repositioning itself as an actor. It is not a state but the gradual relocation of interest through proactive policy planning and strategy making that has made the EU as a security actor in the cyberspace. This is clearly evident from various "activities concentrating on fighting cybercrime and increasing Network and Information Security (NIS) which have provided important support to the development of European 'resilience' to serious cyberattacks"

(Klimburg and Tirmaa-Klaar 2011: 4). Kilmbrug and Tirmaa-Klaar have underlined the need for “resilience cyber architecture in the EU. There are significant differences between the individual Member State’s cybersecurity capabilities, and the EU institutions [themselves] which are poorly protected” (Klimburg and Tirmaa-Klaar 2011: 4). However, efforts have been made to enhance the EU’s cyber power capabilities and to reduce their differences and dichotomies. Prior to the release of the Cyber Security Strategy of the Union in 2013, the EU had to undergo through two significant challenges. First, was related to the limited CFSP engagement in the EU cyber security debate, “despite the obvious relevance of the subject to European peace and security” (Klimburg and Tirmaa-Klaar 2011: 4). Second, was the issues related to “proper political attention, higher-level awareness and Union-wide frameworks to manage cybersecurity both internally and internationally, the EU’s ability to ‘project cyber power’, or even the ability to prevent or manage serious cyberattacks, remains limited” (Klimburg and Tirmaa-Klaar 2011: 4). However, the Cyber Security Strategy 2013 has paved the way towards institutional building mechanisms and the need for synergising common interests between existing structures of EU and its member states.

A lack of cyber deterrence capabilities (or evolving frameworks) has significant implications for the EU’s digital ambitions in the long run. That brings many criticisms to the Union due to its fragmented approach (E Silva 2013). A report “*European Cyber Security Policy*” published by a Berlin-based research organisation *Stiftung Wissenschaft und Politik*, underlines that the EU’s cyber discourse is based on “the multi-level and multi-stakeholder structure of cyber security policy” (Bendiek 2012: 12) which influenced various stages of fruition such as “national level; international level; international organisations; regional international organisations; and transnational forums” (Bendiek 2012: 12-18).

In 2013, the Union has incentivised its cyber diplomacy with the ‘*Cyber Security Strategy* that has mooted for *an Open, Safe and Secure Cyberspace*’. An open, safe and secure online platform brings in online freedom and opportunities to a digital society. This syntax was used in the ‘*Digital Single Market Strategy 2015*’ to shape a ‘community based’ and ‘law based’ approach to digital business - an open, hassle free ecosystem for digital economy that would promulgate a – ‘*Digital Schengen Area*’.

The first step to commence this vision began with the end of roaming (voice and internet) charges all over the EU area in June 2017. However, a ‘*Digital Schengen Area*’ would not be practical if the key layer (infrastructure layer) is not secure and resilient to cyber attacks.

To create an overarching network and information resilience in the pan EU networks, both in internal and imported digital technologies, the Commission adopted the ‘*Directive on Security of Network and Information Systems* (a.k.a. NIS Directive)’ in July 2016. The NIS Directive’s *Para One* has clearly underlined that the “network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities and in particular to the functioning of the internal market” (EC 2016d: 1). The digital dependency is mounting exponentially. Simultaneously digital threats are unfolding security challenges that vary in ‘magnitude, frequency and impact of such security incidents’ at every new attack. Moreover, information systems are vulnerable to security breaches and any such planned, coordinated and deliberated harmful actions could damage or interrupt or disrupt the operation of the systems which has spill over impact on digital society and economy. Thus, “such incidents can impede the pursuit of economic activities, generate substantial losses, undermine user confidence and cause major damage to the [digital] economy of the Union” (EC 2016d). As the ‘*Digital Schengen Area*’ is still a work in progress, therefore, protection of the key layer is vital to its sustainability. The *NIS Directive Paragraph Three* underlines that

Network and information systems, and primarily the internet, play an essential role in facilitating the cross border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market (EC 2016d: 1)

Cyber security issues need to be addressed through better coordination, cooperation and a comprehensive approach. The Union has understood this aspect of cyber security very well, which has clearly been documented in the Directive. The Directive has categorically identified the heart of internal dichotomy lies within EU viz. the aspect of sovereignty and national security. However, the *Paragraph Five* has outlined that -

The existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union. *This results in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union.* Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level.... (EC 2016d: 2).

The existing capabilities of any country of the world are insufficient to ensure high level of security of network and information systems. Due to the overarching influence and volatile nature of the digital medium, it keeps the cyberspace insecure. This has become more evident in the EU due to the diverse nature of Member States. For example, German technology and legal systems have been always rated higher than any Central and Eastern European country. To address such divergence, the Directive's Article – 1, has solicited for a 'common level of security of network and information systems within the Union' and put in place obligations for the Member States to follow –

To adopt a national strategy on the security of network and information systems; to create a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them; to create a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation; to establish security and notification requirements for operators of essential services and for digital service providers; and also laid down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems (EC 2016d: 11-12).

It has made the case clear pertaining to the 'information sharing, trust building and to enhance greater digital cooperation' among internal stakeholders. However, the Article 13 of the Directive has briefed about 'international cooperation' which needs to take into account to ensure 'adequate level protection of data' (EC 2016d: 20). While the Article 14 and 16 chiefly emphasises on 'security issues' and responsibilities of – digital service providers (DSPs) and operators of essential services (OES). The Directive has also included various technical measures to address the risks of digital breaches through both legal and technically defensive architecture. It compels both DSPs and OES to essentially provide cyber incident information to

the CSIRTs for an in-depth research and assessment of their standards, information systems and security measures. Moreover, the Directive has outlined the core concerns and shared the responsibilities between the Union and among Member States to secure the cyberspace's infrastructure layer.

The Commission's factsheet on cybersecurity underlines that what a '*Digital Schengen Area*' could add-on to the EU's digital ambitions and economy. In a nutshell, it "could boost the EU's economy by almost 415 billion Euros per year by creating hundreds and thousands of new jobs but for new connected technologies to take off ...needs trust and confidence; efficient response to incidents, malicious activities and misuse; public private partnership and international cooperation" (EC 2017e). On the other hand, it has significant role in strengthening cyber security mechanisms as better digital economy needs secure digital infrastructure.

Furthermore, the Union recently has adopted a significant diplomatic toolbox to revitalise its 'cyber diplomacy' (EC 2017d) that brought in carrot and stick formula of the Union for malicious cyber activities. *The Reflection Paper on the Future of European Defence published in June 2017* – was the fourth in the series of reflection papers covering key topics for the future of the EU with 27 Member States that have been published subsequently since 1 March 2017. The reflection paper stated that, "the EU would [should] enable cooperation between Member States on systematic reporting on cyberattacks. It would help increase resilience, step up cyber exercises and include a defence dimension to them. Stronger cooperation and effective prosecution would increase the ability to find and punish criminals, thus providing a stronger deterrent against cyberattacks" (EC 2017d: 13). In this regard, on 13 September 2017, the European Commission and the High Representative issued a Joint Communication to the European Parliament and to the Council - *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, it has pioneered an ambitious, comprehensive and structured plan to improve cyber deterrence throughout the Union. It has also elevated the role of CFSP in the cyber security issues. It has a special reference to various institutional cooperation between the EU-NATO and also suggested further expansions in *key actions*-

advance the strategic framework for conflict prevention and stability in cyberspace; Develop a new Capacity Building Network to support third

countries' ability to address cyber threats and EU Cybersecurity Capacity Building Guidelines to better prioritise EU efforts; Further cooperation between EU and NATO, including participation in parallel and coordinated exercises and enhanced interoperability of cybersecurity standards (EC 2017d: 20).

On 13 September 2017, the Commission sketched out a *Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")*. The main aim of this proposal is to enhance the ENISA capabilities in the respects of – man, machine and money. Nevertheless, all these are recent policy makeovers of the EU. “The European Union’s approach to the foreign policy and defense aspects of cyber policy is a mix of good intentions and guidelines however, the EU needs to move beyond the ‘Patchwork Approach to Cyber Defense’ (Bendiek 2017). This is evident from the four significant policy guidelines – “the 2013 Cybersecurity Strategy, which sets out the EU’s cyber diplomacy; the 2015 Digital Single Market Strategy, which aims to bring down digital market barriers within the EU; the 2016 NIS Directive, which sets baseline cybersecurity measures and institutions every EU member state should have; and the ‘cyber diplomacy toolbox’ which provides foreign policy responses to cyberattacks against the EU” (Bendiek 2017). However, it is not evident how the EU would respond in the case of any cyber attack.

In September 2017, the Union updated its Cyber Security Strategy, 2013. It has received a mixed response among the experts and the research community. The Berlin-based *Stiftung Wissenschaft und Politik*’s research group has argued that it is a “*half-hearted progress on far-reaching challenges*” (Bendiek, et. al. 2017). Furthermore, they outlined that “the reformed strategy leaves open a number of questions as to how its objective of an “open, safe and secure cyberspace” will be credibly defended, both internally and externally” (Bendiek, et. al. 2017).

The growing interest on the EU’s role in the cyberspace including addressing the security concerns is evident from the increasing research outputs and publications. This is evident from the recent researches that “the EU's emerging security actorness in cyberspace” (Barrinha and Carrapico 2016: 104), or as the EU as a coherent cyber security actor (Carrapico and Barrinha 2017: 1254) which again conceptualised as

[EU's] [an] emerging “soft power in cybersecurity” (Christou 2017: 9), or “rising as a Digital Power” (Bendiek, et. al. 2017: 7). In essence, the EU has been situating itself as a proactive actor in cyberspace or as a supranational global cybersecurity actor.

THE US'S CYBER-PREPAREDNESS

On the other hand, in the US, issues of cybersecurity are closely linked to the Westphalian discourse of ‘territoriality and sovereignty’ that has been predominantly challenged throughout the evolutions of cyber and digital technologies. Thus, the question arises how does cyber security of a state needs to be addressed? Or what precisely is national cybersecurity? Moreover, with the advent of the global internet, how its overarching and decisive influence on national security is being defined, addressed, and protected. Hathaway and Klimburg (2012) has argued that ‘nations are increasingly facing the twin tensions’ –

First - how to expedite the economic benefits of ICT and the internet-based economy [digital economy]. Second- protecting intellectual property, securing critical infrastructure and providing for national security (Hathaway and Klimburg 2012: 1).

However, cyber threats have become one of the “quintessential security threats of modern times in the United States” (Cavelty 2008). Cyber-threats were an emerging phenomena in the 1990s. The industrialisation and socialisation of the Internet has opened up new networks that multiplied as well as diversified users and their needs. Cavelty (2008) has argued that in “the mid-1990s, cyber incidents were skyrocketed and that did unearth both qualitative and quantitative changes in threats landscape”. This has kick started a new policy horizon in US governments approaches – engagements of civilian agencies charged with internal security missions, computer security or law enforcement are responsible for cybersecurity – this set of conversion of threat cluster and policy renovations signifies the “traditional approach to cybersecurity” (Lewis and Timlin 2011: 3). This approach links to setting up national Computer Emergency Response Team (CERT), however, the cutting edge research for military organisations or creation of specific cyber commands to deal with cyber-warfare are rather more recent developments. The need for cyber command and cyber-warfare capabilities emerged as a key concern for the all. In a report submitted to *The United Nations Institute for Disarmament Research (UNIDIR)*, titled *Cybersecurity and Cyber warfare Preliminary Assessment of National Doctrine and*

Organisation, in 2011, stated that 12 countries²⁵ including the US have established or plan to establish military cyber warfare architecture (Lewis and Timlin 2011: 4). Likewise, a 2016 study, “*Strategic Land power and a Resurgent Russia: An Operational Approach to Deterrence*”, underlined Russia’s effective use of hybrid warfare in an ambiguous manner that highlighted its cyber power ambitions (Anderson et. al. 2016: 12). This study indicated that Russia posed a significant threat to US’s national security and global cyberspace stability.

The US’s cyber preparedness started from the very nascent stage of internet during the 1980s after the first incident of cyber attack recorded as the Morris Worm in 1988. But it was the Clinton administration, that for the first time however, made the first concrete attempt to revamp the national cybersecurity landscape. In 1997, *The Commission on Critical Infrastructure Protection*, chaired by retired US Air Force General Robert Marsh (a.k.a. Marsh Commission)’s recommendations on the cyber dimension of critical infrastructure protection fashioned the basis of Presidential Decision Directive 63 (PDD 63), which in turn framed the cybersecurity issue and the government’s intended course of action (Porteous 2010: 3). At government level, the second attempt was made to defend America’s cyberspace by President Clinton in 2000 *National Plan for Information Systems Protection*. The Clinton administration had also committed \$1.46 billion initiative to secure government systems and to protect critical information infrastructure (Hamblen 1999).

As the 1962 Cuban Missile Crisis had paved the way for the US’s strategic investment in the area of science and technology - nuclear, missile and space – likewise the 9/11 terrorist attacks did impacted the entire gamut of cyber security investments – intellectually, financially and strategically. That prompted President G. W. Bush Jr. to release the first of its kind cyber strategy – *National Strategy to Secure Cyberspace 2003* and *the Comprehensive National Cybersecurity Initiative 2007* - which formally established the US cybersecurity goals and frontline defence against cyberattacks.

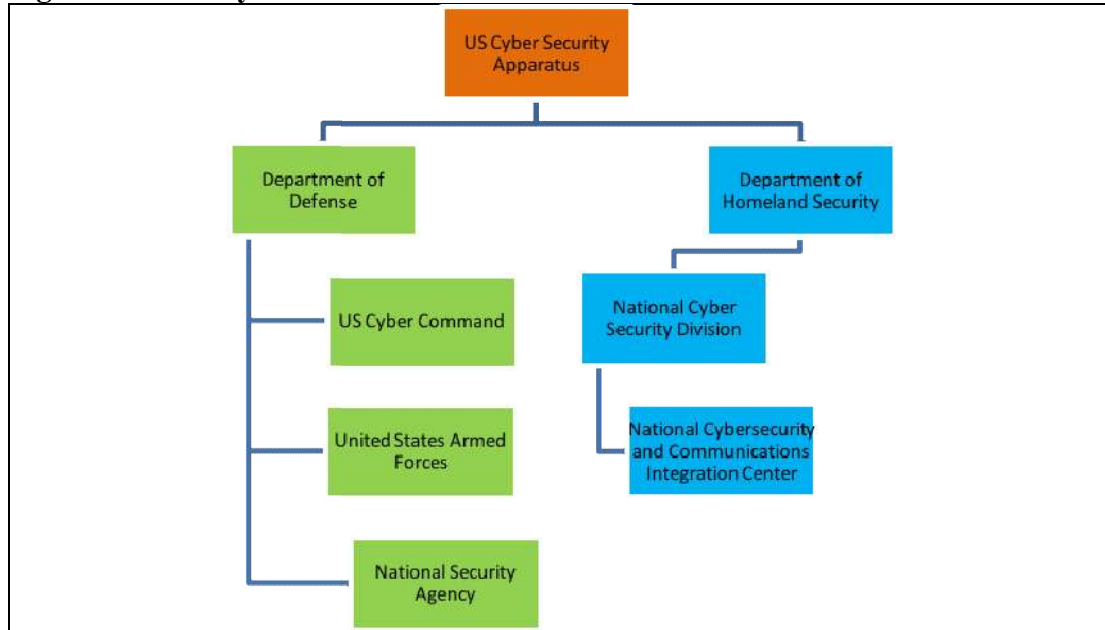
²⁵ Argentina, Brazil, Canada, China, the Democratic People’s Republic of Korea, Denmark, Germany, India, Iran, the Republic of Korea, Switzerland and the United States

The subsequent administration also tried to revamp and shape America's national cybersecurity architecture and international role in cyber governance. The Obama administration took first actions as the "President commissioned 'a-day review' of US cybersecurity policy" (Porteous 2010: 7). In this regard, Assistant to the President for Homeland Security and Counterterrorism, Mr. John Brennan addressed that:

Cybersecurity matters to all of us. Protecting the internet is critical to our national security, public safety and our personal privacy and civil liberties. It's also vital to President Obama's efforts to strengthen our country, from the modernization of our health care system to the high-tech job creation central to our economic recovery (Phillips 2009).

In addition, the 2009 Cyberspace Policy Review validated "CNCI's bridging of previously disparate defence, intelligence and law enforcement missions. It also set out 10 near-term action items, most of which relate to governance, legislation and policy" (Porteous 2010: 7). The Obama administration was well aware of the gravity of the global cyber attacks and thus established a Cyber Command (CYBERCOM) in 2009. It underlined two facts - the growing significance of cyber security in global security landscape and US's strong and precise commitments towards it. "The antecedent to these structural revolutions was links to the 2008 *Operation Buckshot Yankee*, which was the outcome of the US Department of Defense's digital breach" (Lynn III 2010: 97). The Former Commander of US Cyber Command General Keith Alexander once commented, as reported in the media that, "between 2009 and 2011, attacks on US critical infrastructures had 'risen 20-fold, and we see the threat [cyber threats] as real, and we need to act now. From our perspective, the dangers to our critical infrastructure are growing" (Reuters 2012). However, the Obama administration's 2011 *International Strategy for Cyberspace* was the first major "outward-looking US cyberspace initiative in this regard, laying out its vision of how the international community might proceed" (Kavanagh 2017: 31). This Strategy also underlines the core principle of US's global outlook viz. "reserves the right to use all necessary means" to defend itself and its allies and partners, but that it will "exhaust all options before [the use of] military force" (The White House 2011: 14 and Lewis and Timlin 2011: 21).

Figure 5.2: US Cyber Structure



Source: Author’s work developed in consultation with Ph.D. supervisor

To address the wide array of cyber issues both nationally and internationally, the responsibilities have been divided between the Department of Homeland Security, the Federal Bureau of Investigation, and the Department of Defense, including the new US Cyber Command (which has the National Security Agency as one of its components) (See figure 5.1 above). Offensive operations are mostly assigned to Cyber Command and to elements of the Central Intelligence Agency (Lewis and Timlin 2011: 21).

The Department of Homeland Security has primary responsibility for domestic defence (Newmeyer 2012: 116). Its National Cyber Security Division is tasked to “work collaboratively with public, private, and international entities to secure cyberspace and America’s cyber interest”. The Division also has a number of programmes to protect cyber infrastructure from attack. The National Cyber Response Coordination Group is comprised of 13 federal agencies and is responsible for “coordinating the federal response in the event of a nationally significant cyber incident. The Group operates under the National Cyber Security Division” (Lewis and Timlin 2011: 21-22).

The Department of Defense being the creator of the Internet has the primary and significant role to guide the development of cyber forces, strengthen of cyber defence and enhancement of cyber deterrence posture, moreover, it has three missions: to defend the networks, systems and information of the US defense (Department of Defense 2015). On the other hand, the Cyber Command, [was a military subcommand] under US Strategic Command, is responsible for dealing with threats to the military cyber infrastructure. “Cyber Command’s service elements include Army Forces Cyber Command, the Twenty-fourth Air Force, Fleet Cyber Command and Marine Forces Cyber Command” (Lewis and Timlin 2011: 21-22). Important steps were taken by the Obama administration to address the cyber issues in order to facilitate inter-institutional cooperation. That was the outcome of “a memorandum of agreement on cybersecurity between the DoD and DoHS in October 2010” (Lewis and Timlin 2011: 22).

However, since 2013 – 2017, the US posture in world affairs with respects to cybersecurity, individual privacy and surveillance has undergone changes, which has drawn criticisms. The US administration has stood “steadfast in its position that existing global norms should be the starting point for any discussion on ICTs in the context of international security and for ensuring stability of the ICT environment” (Kavanagh 2017: 31). To regain the old supremacy in the cyberspace, both US industries and US government have been pushing for normative engagement in the cyberspace.

A Germany based online statistics, market research and business intelligence portal - Statista – observed that in 2017, \$ 19 billion US dollar budget was given for cyber security, representing a 35 percent increase from the previous year (Statista 2017). The Trump administration directive to elevate United States Cyber Command (it was a division of the NSA) to the status of unified military command which has made the command even more agile and strengthened its voice in the department (DoD 2017) in the backdrop of Chinese, Russian, North Korean activities and the rise of ransomware (Newman 2017). President Trump has said that, “this new Unified Command will strengthen our cyberspace operations and create more opportunities to improve our Nation’s defense” (Trump 2017). This proactive decision implies, first, the US’s intention to give a legitimate push for cyber arms race. Second, strong action

will be taken against cyber intruders. Last, but not the least, the US's enduring endeavour to manoeuvre cyberspace, as it has been a legitimate actor in other international regimes.

THE EUROPEAN UNION'S APPROACH TO DATA PROTECTION

Internet privacy and data protection have been broadly associated with the traditional notion of privacy in the physical world. The idea of privacy has been contested and protected by the rule of the law or by the constitutional framework of a state. While moving away from the traditional aspect of privacy, to the internet or cyber domain, a critical question is who and how are the standards set for internet privacy? In an emerging digital society and digital economy, how are governments and their agencies, along with online retailers, search engines and social network providers using internet highways and personal information for personalising their products and, crucially, for targeting publicity to its users in order to make a profit (Rossi 2014). Thus, the treatment of personal data and the degree of privacy internet users represents a large part of the standardisation of the Internet. The business model of the present day prominent internet providers like "Google, Facebook and Twitter services would not be perceived as working in the same and standard way, if the treatment of personal data were radically different in different countries" (Rossi 2014: 65-66). This is because of a lack of global cyber rules of engagements, underdeveloped privacy layer in the infrastructure level, inadequate data protection regulations both at national and international level that has paved the way for the companies to mine the data, misuse the data and feed it into the users virtual world to manipulate their real world action. It is also creating new challenges to business as well to deliver better service and protection to their customers' personal information and privacy. From industry perspectives, it is quite challenging to do business under multiple rules of data protection²⁶ (Kent 2017). On the other hand, the lack of adequate laws has provided leeway to cyber criminals. Industries and public sector bodies are keenly espousing 'big data' as the 'new normal' "to build a better understanding of their customers and citizens" (Lewis 2014). The issue of big data is also influencing the data protection and privacy issues in the digital world.

²⁶ This point was mentioned by Ms. Gail Kent, in a WhatsApp interview on 3 August 2017 in London.

To address such pressing issues of the time, the EU adopted the General Data Protection Regulation (GDPR) in 2018 that has set the threshold to the highest level of data protection and privacy for Europeans at the global level, with the strict guidelines such as – ‘privacy by design and privacy by default’. The adoption of the GDPR has created a multi-layered robust data protection and privacy regulations. But the question is here how would the EU stand out to protect the privacy and data of its citizens when most of the companies are not hundred per cent compliant with the GDPR? Before going into this issue, it is noteworthy to examine the evolution of GDPR. The GDPR is the revised, updated and modern version of the data protection Directive. The EU had adopted ‘*the European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (a.k.a. Directive 95/46/EC or the Data Protection Directive) to regulate the collection and processing of personal data via cyberspace. The Directive states that:

Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals (EC 1995).

The Data Protection Directive had been implemented in all 28 EU Member States through national data protection laws (Long et.al. 2017). The second important development was *the European Telecommunications Directive*, which established specific protections covering telephone, digital television, mobile network and other telecommunications systems (Banisar and Davies 1999: 12). These two new Directives have created a new benchmark for individual freedom and privacy of the time. The Data Protection Directive’s Article 25 deals with transfer of personal data to third countries (non-EU countries), this article laid down the principles such as “the adequacy of the level of protection” (EC 1995: 45) as per the EU standards and if the third country does not ensure or failed to provide an adequate level of protection, the Member States shall take the measures necessary to prevent any transfer of data. Thus, the EU’s own regulations meant for internal protection of data, has an international aspect and went beyond EU borders. The EU has thus already been setting global standards by the 1995 Directive.

The European Charter of Fundamental Rights 2000, Articles 7 and 8 are two important sources of data protection at the primary law level. Both articles establish two comprehensive rights “protecting private life and personal data of individuals” (Boehm 2015: 11). The growing cyber vulnerabilities caused an occasion for enhancing the level of data protection in the Union. This led to an increasing consensus among the member states to address the issues of data protection. The same was given due significance by Article 16 of the 2009 Lisbon Treaty. The Article 16 states that:

1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39²⁷ of the Treaty on European Union (EC 2008: 55)

This has also strengthened the EU’s commitments towards data protection and individual privacy. To understand the attitudes on data protection and electronic identity and to map the awareness among the EU citizens, it conducted the largest micro level survey in 2010 which was later published in 2011. The Special *Eurobarometer 359* has outlined that there are two types of digital experts– ‘digital natives and digital initiates’²⁸, (EC 2011b: 4).

Furthermore, the survey also revealed common consensus on the protection of children and their rights in digital age. Other interesting outcomes of the survey suggested that “55 per cent of the Europeans trusted the European Parliament and European Commission more than any companies. Second, 70 per cent of the Europeans are concerned that their personal data held by companies may be used for a

²⁷ In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, “the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities” (EC 2008: 36).

²⁸ “digital natives: young persons born during or after the general introduction of digital technology. Second, ‘digital initiates’: they are not of a young age by definition, but have become experienced by interacting with digital technology e.g. through work or education, and have different viewpoints than digital natives” (EC 2011: 4).

purpose other than that for which it was collected” (EC 2011b: 2). The concern got bigger momentum in 2013 after the NSA contractor revealed about the US’s global surveillance project.

Another interesting development took place in 2014, that was the ‘right-to-be-forgotten²⁹’ issue that emerged as one of the key battles between *Google and Spain*. The EU’s highest court ruled in favour of Spain, and it has affirmed that individuals have the right to request that outdated or ‘irrelevant’ information about them be removed from search results. The Electronic Privacy Information Center (EPIC) called this decision as a shockwave which has a rippling effect around the world (EPIC 2015).

Back to the Data Protection Directive, it had two major loopholes³⁰, that allowed for the creation of safe harbours for companies that do not comply with the high levels of protection prescribed by the Directive (Rossi 2014: 71). Under this clause, the US governments and companies signed up for erstwhile Safe Harbour agreements to facilitate transatlantic data flows since 1995 till 2015. The decades old understanding of cross-border data sharing was challenged in the European Court of Justice which put an end to the agreement. However, a robust and new set of agreement (i.e. Privacy Shield 2016) was signed between the EU and the US for the cross border data flows.

As the concern over data protection and privacy grew bigger, in order to address the issues, the European Commission in 2012 proposed for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of the personal data and on the free movement of such data (a draft version of GDPR). The proposal was “meant to override the loopholes in the Directive. Interestingly, the proposal was the most lobbied piece of European legislation in history having over 4,000 amendments in opinions from committees in the European Parliament as well as from industries” (Long et.al. 2017: 12). American backed lobby groups from Microsoft, Facebook, Google, had tried hard to get leeway in the drafts

²⁹ The issue of ‘right to be forgotten’ gets substantial justice in the EUGDPR.

³⁰ the sixth paragraph of Article 25, which establishes that “the European Commission can unilaterally establish - in virtue of domestic law or international agreements – whether or not a third country offers an adequate level of protection for Europeans’ data, and Article 4, on the applicable national law” (Rossi 2014: 71).

(Kent 2017)³¹. After a long multi-stakeholder battle with regard to the GDPR, the final level of discussion or the commencement of the ‘trilogue’ process – “negotiations between the three EU institutions started. In May 2016, the Regulation was adopted by the European Parliament at the second reading” (Long et.al. 2017: 12). The Union gave a two years (May 2016-May2018) window period to the Member States to bring about compliance with the new regulations.

The GDPR has widened and deepened the horizon of data protection and Article 3 talks about ‘Territorial scope’, the Regulation will apply to “the processing of personal data in the context of the activities of a data controller or a processor in the EU and to a controller or processor not established in the EU where the processing activities are related to the offering of goods or services to EU citizens, or the monitoring of such individuals” (EC 2016b: 32-33). This means that many non-EU companies that have EU customers will now need to comply with the Regulation (Long et.al. 2017: 13). The new regulations enhances individual right and the end users legal capabilities. It has made significant changes in the matter of – consent, right of erasure (right-to-be-forgotten) and data portability.

Although, industries have been reshaping their privacy policies as compliance to the GDPR guidelines, yet there are many that have to reach hundred per cent compliance to the guidelines. Second, as per industry speculations the stringent privacy protection might impact EU’s digital ambitions and digital innovations. Third, in the age of big data, algorithm based decision making, Artificial Intelligence, Internet of Things, how could privacy and data protection regulations like GDPR be effective or counterproductive only time will tell.

THE UNITED STATE’S APPROACH TO DATA PROTECTION

In the US, privacy in the pre-digital age or privacy and data protection (personally identifiable information) in a digital age have always been an issue caught between two flanks – government and corporate. Who is more intrusive to individual’s private space? Why are they? And who gave them the authority to do that? Lack of adequate data protection framework is just the tip of the iceberg.

³¹ This point was mentioned by Ms. Gail Kent, Facebook, UK, in a WhatsApp interview with the researcher on 3 August 2017.

Privacy researchers argues that unlike the broad scope of coverage and the centralised standard-setting and enforcement features, “data privacy regulation in the United States is fragmented, ad hoc, and narrowly targeted to cover specific sectors and concerns” (Shaffer 2000: 22). In the US, right to privacy is “not explicitly recognised in the constitution” (Banisar and Davies 1999). Rather “implicitly granted against governmental intrusion form the *Fourth Amendment*, of the US constitution” (Boehm 2015: 51). The 1890 Warren and Brandeis article ‘*The Right to Privacy*’ has often been cited as the US right to privacy. Although, privacy as fundamental human rights is recognised in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties, yet it has always been contested at personal, social, national and regional and international level. In a digital society with the advent of social networking web, “the new generations are keen to share much personal information to get internet hits. This has created a privacy paradox” (Taddicken 2014: 248). The paradox is everyone shows concern about their privacy but just could not stop sharing (Murphy 2014) on the social media platforms.

Somehow, in US the history of privacy (loosely defined as freedom from being observed) is a matter that related to one of status. The issues further “institutionalised between the binary of good people/society and bad people/society. It has also been observed that criminal behaviour or ill health, children and the impoverished have less privacy than those who are upstanding, healthy, mature and wealthy” (Murphy 2014). Society changes at a slower pace than the technological advancements and that creates different layers within a socio-political framework. It is often noted that youth are more adaptable to technological changes and less concerned about privacy as compared to the older generations, who are also not so adept at using technology.

The Internet has impacted the traditional societal value systems and the notion of privacy is also becoming the most significant human rights issue of the digital age. The scope of “privacy have been debated for generations, theorists offer widely varying conceptual definition” (Wu et.al. 2011: 604). In the digital age, empowered with modern gadgets and mediums such as emails, social media (Facebook, Twitter, Snapchat – public in nature), instant messaging app (WhatsApp and Telegraph –

encrypted in nature), blogs bring new perspectives to privacy or how privacy should be understood in a digital realm. Likewise it also poses challenges to the dimensions of freedom of expressions.

In the US, issue of privacy and freedom of expression are often overshadowed by the national security concerns. Moreover, historically the US government has strong power over information (data), which was underway well before 9/11, “which helped the federal government gather, leverage and mine public and private data using database technologies” (Kline 2008: 444). This was also evidenced from a “fuzzy US telecommunications privacy policy that provides backdoor entry to both government and corporate agents to carry out intrusive acts” (Katz 1988). It was the time when researchers have sensed an emergence of the ‘surveillance society’ in the US. The arguments were that the advanced electronic technologies (or digital technologies) ‘dramatically increase the bureaucratic advantage’ in the “workplace, marketplace, and government by enabling – and encouraging – increasingly automatic methods of surveillance of the individual that the US legal system cannot control” (Gandy Jr 1989: 61). This indicates two things, first, mass scale data mining and misuse of such data, second, lack of adequate legal structure. The 9/11 terrorists attacks were one of the reasons that persuaded the US governments to pursue a ‘security theatre’ (Kline 2008: 443) because it changed the characteristic of threats to security as being unidentifiable, unpredictable and vulnerable.

The US Patriot Act 2001 elevated the power of law enforcement agencies to use intrusive methods to information and intelligence gathering. Furthermore, it paved the way for the Bush administration to initiate process (i.e. National Cyber Security Strategy 2003) to securitise the cyberspace. From historical evidences it has been understood that spying is an old game played by leaders. However, modern technologies are just enabling and empowering the old statecraft to expand the game through digital means.

Present day’s Internet giants are based in the US and is the outcome of database-driven information markets that started in the 1970s. Arthur R. Miller suggested in his 1971 book, *The Assault on Privacy*, “new information technologies seem to have given birth to a new social virus- 'data-mania' and that [we] must begin to realize what

it means to live in a society that treats information as an economically desirable commodity and a source of power” (Kline 2008: 447).

The Privacy Act of 1974 is the key element of the US’s laws for the protection of individual privacy. It has empowered the federal agencies to collect the information about the citizen. The Act,

Establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements (Department of Justice 1974).

This act has put legal restrictions such that there can be no disclosure without consent of personal identifiable information to the third parties. But, it could not justify sufficiently the need for such collection of mass data sets. Bignami (2015) has argued that the Privacy Act of 1974, among US laws is “the closest analogue to a European data protection law in that it seeks to regulate comprehensively personal data processing, albeit only with respect to federal government departments and agencies” (Bignami 2015: 10-11). There are few backdoors to the act where the government if wanted, could misuse the information in various ways. One of the major loopholes of the Act 1974 is it allows federal agencies to transfer information between themselves for what “they justify as a ‘routine use’ and it only applies to data processing conducted by the federal government, not by state governments or the private sector” (Shaffer 2000: 23). At the state level, there are 48³² regulations related to the privacy and data protection. This shows how fragmented is the data protection at the country and state levels creating opportunity for data misuse and theft.

The State of California was at the forefront in regulating “data security and data breach framework by first requiring that companies notify individuals whose personal information was compromised or improperly acquired” (Raul et. al. 2017: 365). For

³² Alabama and South Dakota remain the only states without legislation specifically requiring data breach notification (Raul et. al. 2017: 365).

example, California alone has more than “25 state privacy and data security laws” (Halpert, et.al. 2017: 628). At the state and federal level, there are various laws in “banking, healthcare, communication agencies that require companies to provide mandatory notification at times of breach to affected parties and impose affirmative action with the view to safeguard their sensitive personal information” (Stevens 2010: 4, Raul et. al. 2017: 365). Therefore, the data protection challenge is particularly acute in the US because it has “a lot of different data privacy laws but no over-arching data protection legislation” (Cobb 2016). There are instances when US administrations have lamented about their high standard data protection and privacy regulations. In one such event, then President Barak Obama underlined the US’s commitments towards cyber security and privacy -

Americans have always cherished our privacy. From the birth of our republic, we assured ourselves protection against unlawful intrusion into our homes and our personal papers. At the same time, we set up a postal system to enable citizens all over the new nation to engage in commerce and political discourse. Soon after, Congress made it a crime to invade the privacy of the mails. And later we extended privacy protections to new modes of communications such as the telephone, the computer, and eventually email (The White House 2012).

In contrast to the EU, the US does not apply ‘citizen first’ approach to data handling and protection. But, there are some specific federal laws that prevent ‘unfair and deceptive practices’ and make sure children’s data is protected properly (Williams 2017). The Federal Trade Commission (FTC) is the key institution for addressing concerns of consumer privacy. The FTC has authority to pursue companies that fail to “implement reasonable minimal data security measures, fail to live up to promises in privacy policies, or frustrate consumer choices about processing or disclosure of personal data” (Halpert, et.al. 2017: 628). The US government also has specific privacy laws for the types of citizen (consumer) data that are most sensitive and at risk. Such laws are closely associated with “(a) the financial, insurance and medical information; (b) information about children and students; (c) telephone, internet and other electronic communications and records; (d) credit and consumer reports and (e) background investigations at the federal level” (Stevens 2010, Raul et. al. 2017: 368). All of the laws that have existed in the US are primarily linked to how the administration defines it. Conversely, the Federal government use two kinds of classification for data which needs to be protected by the law – “personal data (information that can be used to contact or distinguish an individual) and sensitive

personal data (health data, credit reports, information collected online from *children under 13*, precise location data, and information that can be used for identity theft or fraud)” (Raul et. al. 2017: 370). In the post 9/11 period, the USA PATRIOT Act 2001, amended pre-existing privacy protection laws such as Foreign Intelligence Surveillance Act (FISA), the Electronic Communications Privacy Act (ECPA). However, many of its initially “time limited provisions have been reauthorized by successive Acts - the USA FREEDOM Act, 2015” (Boehm 2015, Bignami 2015, Raul et. al. 2017 Halpert, et.al. 2017). However, a lack of unified privacy and data protection law in the US, kept the door open for violation of individual liberty in the cyberspace.

There is no ‘citizen centric’ unified data protection law in the US, similarly, no data protection authority to address the issue in case of violations. There are huge gaps between data protection and privacy rights, procedures and laws applying to US citizens and non-US citizens. The rights “applying to the US citizen already lack a general data protection framework, this weakness has further intensified when a non-US citizen is concerned” (Boehm 2015: 65-66). In the post Snowden leaks era, the question of data privacy has led to vehement criticism of the US both internally and internationally. The leaks have significant and crucial immediate impact on US economy. As a result, its businesses lost revenues and market share as well as trade agreements paused. In the long run, at the global level, it has sparked various debates around data localization, data protection and internet governance.

In 2013, the *Wall Street Journal* raised the question that ‘should the US adopt European-Style Data-Privacy Protections?’. One camp that said ‘yes’, mostly belong to the activists and civil society. But the powerful camp that said ‘no’ includes industries and government. They have argued that lack of stringent privacy restrictions in the US has encouraged innovation in the online market industry which is still evolving (Wall Street Journal 2013). As cybersecurity remains an intense debated area in the US in recent past, what remains to be seen is how both governments and private industries such as - internet, telecom and tech - are getting ready to take a call in regard to a unified privacy and data protection regulations like GDPR.

CONVERGENCE AND DIVERGENCE IN THE EU AND THE US DATA PROTECTION APPROACHES

Prof. Hans Rosling, a Swedish physician once said that “Eighteen fifty-eight was a year of great technological advancement in the West. That was the year when Queen Victoria was able, for the first time, to communicate with President Buchanan, through the Transatlantic Telegraphic Cable. And they were the first to ‘Twitter’ transatlantically” (Great Thoughts Treasury 2018). Things have shifted dramatically in the last couple of centuries.

Prior to the emergence of a data driven digital world, the transatlantic partners shared and mutually consented to an agreement for cross-border data flows. Although, the EU and the US do share equal space, commonness and understanding for digital economy, still there is a significant difference with respect to the issues of data protection and individual privacy. To neutralise the difference in the post Directive period (1995-2015) the EU and US had developed *Safe Harbour Privacy Principles*, during 1998-2000. As per the 1995 Directive mandates, transfers of personal data take place only to non-EU countries that provide an ‘adequate’ level of privacy protection. To harmonize cross data flow, in July 2000, “the US Department of Commerce issued the Safe Harbor Privacy Principles which were subsequently recognized by the European Commission. However, according to the Commission’s Decision, the Safe Harbor principles could be limited to the extent necessary for national security, public interest, or law enforcement requirements” (Weiss and Archick 2016: 5). Furthermore, with this agreement, “a US company could self-certify (voluntarily) annually to the Department of Commerce that it had complied with the seven basic principles and related requirements that have been deemed to meet the data privacy adequacy standard of the EU” (Weiss and Archick 2016: 5). The seven basic principles are *Notice; Choice; Onward Transfer; Security; Data Integrity; Access and Enforcement* (EC 2000).

The first principles – *Notice* – The individual should have the knowledge for what purposes the data is being collected. It has stated that

An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for

limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party (EC 2000: 11).

The second principles – *Choice* – the individual should have choice to opt-out. It has underlined that

An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice (US Department of Commerce 2000).

The third principles – *Onward transfer* – one of the key principles that check the transfer of data to the third parties resides in US or outside of the US or elsewhere that is not a part of this agreement. It says that

To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles (EC 2000: 11).

The fourth principle – *Security* – this principle is crucial for present research as well as the entire gamut of digital privacy. It has emphasised that

Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction (US Department of Commerce 2000).

The fifth principle – *Data integrity* – it is very significant for the data subject to know how and for what the purposes for which her data is used. It has highlighted that

An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current (US Department of Commerce 2000).

The sixth principle – *Access* – it has empowers the data subject to have access to the collected data. This is one of the key aspects of the agreement. It has stressed that

Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information

where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated (US Department of Commerce 2000).

The last principle – *Enforcement* – this is principle is core of the agreement. It compiles to the agreed companies to must provided mechanisms to resolve the data subjects disputes over whether it is following the Principles. This has underpinned that

Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations (EC 2000: 12).

This agreement has set the new benchmark for the cross-border data flows until recently. However, the EU has emerged as a proactive security provider for data protection since 1995. While the EU has set out the global standards for Internet privacy, there are no such significant or generally applicable data transfer restrictions in the US; however, “the US has taken steps to provide compliance mechanisms for companies that are subject to data transfer restrictions set forth by the EU” (Raul et. al. 2017: 377). These issues of data protection and the safe harbour agreement were impacted after the revelations on NSA surveillance, followed by the “Maximilian Schrems vs. Irish Data Protection Commissioner Judgement 2015”. The Irish Data Protection Commissioner played “a crucial role in regulating and enforcing European policies in this area because key US companies have their headquarters in Ireland (Facebook, Google, Twitter, Microsoft, etc)” (O’Rourke and Kerr 2017: 22). The landmark judgement by the European Court of Justice (ECJ) in the Maximilian Schrems vs. Irish Data Protection Commissioner, on 6 October 2015, issued a decision that invalidated the ‘Safe Harbour’ with immediate effect.

The ECJ had found two significant flaws in the ‘Safe Harbour’ principles. First, it was the European Commission who was supposed to confirm that the domestic law of the third country (i.e. US domestic law) or its international commitments protect the right to the protection of personal data which should be ‘essentially equivalent’ to that as guaranteed under the Directive and Charter of Fundamental Rights. But the “Commission with its Decision of 2000³³, did not explore such legal background and only explored the Safe Harbour scheme” (Bu-Pasha 2017: 220). The Second issue, that the Court found was that “the US public authorities were kept immune from the applicability of the Safe Harbour scheme; rather, the scheme was meant to apply to the US-owned undertakings” (CJEU 2015, Bu-Pasha 2017). This had paved the way for the US federal agencies such as NSA and FBI to use data of non-US citizens (i.e. EU).

The entire judgment had brought to light the dichotomy and legal flaws in data sharing activities within multinational corporations operating in Europe and US. Second, it raised important questions about “the ability and willingness of states and corporations to protect citizen privacy” (O’Rourke and Kerr 2017: 21). Last but not the least, it expanded the ambit of the EU data protection regulations to extra-territorial jurisdictions. It can be interpreted that the EU data protection law for the EU data subjects favour to protect personal data and privacy even outside the EU/Europe.

The ‘invalidation’ of the Safe Harbour Framework has brought a considerable degree of “uncertainty to the fate of thousands of companies that rely on it as bedrock of day-to-day global digital operations” (Raul et al. 2017: 377). From an international trade perspective, “the framework had been considered as the most significant data sharing agreement of the period. The court has set a two years deadline to create a new and robust framework for transatlantic trade and data flows” (Lewis et al. 2018: 11). During the two years of transition phase, the ECJ has authorised “the Article 29 Working Group (advisory status and acts independently and they do not reflect the position of the European Commission) to look into the matter of data protection

³³ Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L215)

between the US and the EU” (Katulić and Vojković 2016). On 2 February 2016, two days after the two year deadline established by the Article 29 Working Group, the US and the EU officials announced their agreement, “in principle,” on a replacement to Safe Harbour— “*the EU-US Privacy Shield*, which if approved by the European Commission, would allow companies to continue to transfer EU citizen’s personal data to the United States while complying with the requirements outlined by the CJEU when it declared Safe Harbour invalid in October 2015” (Weiss and Archick 2016: 9).

The EU–US Privacy Shield provides a new and robust framework for transatlantic data transfers and it activated in August 2016, replacing erstwhile Safe Harbour. The Privacy Shield principles entail “seven distinct categories³⁴; a supplemental set of principles and provisions³⁵. To address the concerns raised by the CJEU through the landmark judgement, Privacy Shield provides a model for “arbitrating disputes and contains commitments from US national security officials, as well as letters from US government officials, concerning the protections afforded by Privacy Shield in regard to data from EU citizens” (Weiss and Archick 2016: 9-10). However, it needs to be noted that there are disparities between the values of trading regions, this is also influenced and affected by social contracts on privacy and data protection. This has also brought under the new agreement to create a balance between national interest, economic implications and protection of personal privacy and free flow of data.

Although, the Privacy Shield has much stronger regulations than its predecessor, the fact remains to be seen how the future of transatlantic commonness is unfolding under the new administration. But before reaching any conclusion it is essential to find out the policy convergence and divergence between the EU and US administration on the issue of data protection.

³⁴ Notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, and recourse, enforcement, and liability

³⁵ around sensitive data, secondary liability, the role of data protection authorities, human resources data, pharmaceutical and medical products, and publicly available data

CONVERGENCE AND DIVERGENCE: THE EU AND THE US DATA PROTECTION POLICY

The ubiquitous nature of the Internet and robust online services over the last few decades represent the most significant generation for international flows of data (personal and non personal information) since the first wave of “Cyberization” (Ma 2016: 85) in the 1970s. Since the beginning “fears of omnipotent and omnipresent collections of personal information’ mushroomed due to revolution in personal computer, large scale processing of data and centralised database” (Reidenberg 2000: 1318). This process of data-driven-cyberization has kept the matter of privacy as fundamental rights at bay. But time is changing as par with the awareness, emerging legal frameworks and changes in public policy approach.

Table 5.1: Data Protection Policy Convergence and Divergence between the EU and US

Year	Events	EU	US	Outcomes
1792			Fourth Amendment to the United States Constitution	Identified Privacy is Fundamental Rights
1974			Privacy Act 1974	Code of Fair Information Practice
1978			Foreign Intelligence Surveillance Act	Extra territorial surveillance power of the US
1980	OECD-Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data			
1981	CoE - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data			

1986			The Electronic Communications Privacy Act (ECPA)	Prevent unauthorised government access to data
1988	For the first time a cyber attack was recorded. A Cornell University student creates the first computer worm, which cripples 10 percent of the 88,000 computers on the Arpanet			Vulnerability of computers and data is created
1990	Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95			
1995		The Data Protection Directive (officially Directive 95/46/EC)		Regulation of Data
2000	Denial-of-service attacks to date, hackers launch attacks against eBay, Yahoo!, CNN.com., Amazon and others.	Safe Harbour Privacy Principles The Charter of Fundamental Rights of the European Union	The National Plan for Information Systems Protection (Clinton Administration) Safe Harbour Privacy Principles	Cross border free flow of data between the EU and US. The Charter identified data protection is a part of fundamental rights
2001	9/11 Terrorist Attack DNS attack on	Network and Information Security: Proposal for	A National Security Strategy for a Global Age (Clinton	Securitisation of Data at the EU level 9/11 attacks impacted

	Microsoft The Council of Europe - Convention on Cybercrime	A European Policy Approach	Administration – Published on 1 December 2000) The National Cyber Security Alliance (PPP) The USA PATRIOT Act (Bush Administration)	dramatically the US and global security landscape As a result the US moved towards a surveillance country
2002		First E-Privacy Directive	Homeland Security Act	The EU reviewed the 1995 Directive The US Institutionalised internal security apparatus
2003		The European Security Strategy	National Cyber Security Strategy 2003 (Bush Administration)	Convergence in identifying non-traditional threats Divergence in the approach – EU (multilateral); US (unilateral)
2004		Creation of European Network and Information Security Agency (operational in 2005)		The EU created new institutions to address the issues of information security
2006		The EU Strategy for a Secure Information Society	The National Security Strategy of the United States (Bush Administration)	The EU securitised of Information society The US identified cyber security threats to national security
2007	Estonian Cyber Attack			Benchmark events in the cyber security discourse, thus, changing narrative in cyber war discourse
2008	WikiLeaks Cyber attacks on Georgia	Report on the Implementation of the European		The EU identified cyber threats as a non-traditional threats to national security

	Established NATO Cooperative Cyber Defence Centre of Excellence	Security Strategy		
2009	Attack on the Homeland Security Information Network	The Critical Information Infrastructure Communication Treaty of Lisbon	The US Established Cyber Command under the NSA (in 2018 it was elevated as a unified combat command)	The EU observed and institutionalised individual privacy and data protection as a fundamental rights The EU took the significant steps to secure the CII The US adopted conventional approach to address the issues of Cyberspace
2010	Stuxnet Malware Sophisticated cyber attack on Google Very sensitive cyber attack on Morgan Stanley Arab Spring	The Digital Agenda for Europe The EU-US Summit	National Security Strategy (Obama Administration) The EU-US Summit	Convergence in identifying new challenges to national security
2011	Cyber espionage on the European Commission and EU's External Action Service		Department of Defense Strategy For Operating In Cyberspace International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World	The US observed a conventional norm based approach to networked world
2012	Espionage "Flame" attack			

	on Iran and West Asia			
2013	Edward Snowden, a former systems administrator at the NSA reveals the US's global surveillance project	The EU Cyber Security Strategy		The EU enhanced a comprehensive and strategic approach to cyber security Divergence in protecting individual privacy and data protection in the digital age
2014	US Office of Personnel Management hacked (OPM hack) Sony Hack The 2014 Wales Summit of the NATO	The right to be forgotten judgement		Upholding the individual liberty in the digital age
2015	The CJEU's Schrems judgment The Office of Personnel Management Hack Cyber attacks on Ukraine United States v. Microsoft Corp Ashley Madison data breach		National Security Strategy (Obama Administration)	The US mooted for a collaborative efforts between the established and emerging powers to deal with global threats (including cyber) End of the Safe Harbour privacy principles
2016	Russian Influence in the Presidential Election Sophisticated attack on the	The Directive on security of network and information systems (NIS Directive)	Privacy Shield Agreement	The EU created common standards for information systems between Member States

	<p>Society for Worldwide Interbank Financial Telecommunication</p> <p>Hackers targeted AdultFriendFinder, a dating website, compromised 412 million users data</p> <p>Sophisticated cyber attack on Ukraine</p> <p>Petya</p> <p>FBI–Apple encryption dispute</p>	<p>Privacy Shield Agreement</p>		<p>Privacy Shield created new regulatory framework for the cross border data flows between the EU and the US</p>
2017	<p>WannaCry ransomware attack</p> <p>Data breach at Equifax</p>	<p>The cyber diplomacy toolbox</p>	<p>National Security Strategy of the United States of America (Trump Administration)</p>	<p>The EU adopted a sanction regime against cyber offenders</p> <p>The US adopted nation first approach to cyber security</p>

2018	Facebook– Cambridge Analytica data scandal	The General Data Protection Regulation Permanent Structured Cooperation (PESCO) Digital Single Market: EU negotiators reach a political agreement on free flow of non-personal data	National Cyber Strategy of the United States of America (Trump Administration) Unified Combatant Cyber Command The Clarifying Lawful Overseas Use of Data Act	The EU created a global regime to protect individual privacy and data in the digital age The EU created defensive mechanise to deal with cyber threats The EU mooted for a common digital union The US securitised the digital age The US elevated its offensive militarisation approach to deal with cyber threats The US enhanced the legal capacity to access the global data The EU adopted a regulatory approach to cyber security and data protection, on the other hand, the US adopted a state centric conventional approach to cyber security and data protection
------	---	--	---	---

Source: Author’s work developed in consultation with Ph.D. supervisor

Under the EU law, the right to privacy and protection of personal data is comprised of a number of legal guarantees which are defined in the Charter of Fundamental Rights, erstwhile Data Protection Directive, Lisbon Treaty, and GDPR. But in the US law, the matter of privacy can be read in to the Fourth Amendment in 1792. It prohibits

“unreasonable searches and seizures”³⁶ by the government. Though, it has defined the context and matter of privacy in “the pre –digital era, thus it does not underline any ground for the data protection issues. In other words, it has very limited scope and regulations protecting privacy of third country citizen” (herein meaning the EU citizen privacy) (Bignami 2015a: 5).

The first most important legal development that has taken place in the US regulatory framework during the initial phase of cyberization is the Privacy Act 1974. This is the closest analogue to the European data protection law (Bianami 2015a: 5), yet there are huge differences of how both view and regulate data-space. The fundamental difference between the EU and the US lies in their legal approaches. While “the EU views its laws as reflecting and making concrete the broader mandates of a fundamental privacy right, the United States anchors its information privacy law in the marketplace” (Reidenberg 2000: 1318, Schwartz and Peifer 2017: 132). Moreover, at a general level, the Privacy Act contains most of the elements of the EU right to personal data protection. However, “it only protects US citizens and permanent residents, not EU citizens” (Bignami 2015a). The Privacy Act also allows to sharing of the data among federal agencies which is contradicting to the EU’s understating of personal data protection. In 1978, the US has enacted the Foreign Intelligence Surveillance Act. It has empowered the federal agencies to carryout electronic surveillance and data collection of foreigners both from classified and unclassified sources. It has empowered the US national security apparatus, likewise as per the need it has amended from time to time.

As the cyberization process began to grow more rapidly, the personal information was ‘levelled’ as another “commodity in the market and human flourishing was furthered to the extent that the individual can maximize his/her preferences regarding data trades” (Schwartz and Peifer 2017: 132). To stop and regulate the ‘commodification of personal data’, three significant developments have surfaced – first, OECD’s personal protection guidelines for trans-border flow of personal data. Second, significant development happened just a year after the OECD guidelines. The Council

³⁶ Reasonableness is established if the search or seizure is conducted pursuant to a valid warrant, that is, a judicial order based on a showing of probable cause and on a particular description of the property to be searched and the items to be seized. Reasonableness can also be established if one of the exceptions to the warrant requirements exists.

of Europe has adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981. Third, significant guidelines came from the UNGA i.e. Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95, in 1990.

These developments have given a sense of urgency for data privacy and data protection in the digital realm, but could not be considered international binding principles due to limited legal compliance. However, the OECD's guidelines did influence the shaping of the EU data protection Directive in 1995. During the same time in 1986, the US had passed the Electronic Communications Privacy Act (ECPA), it has four set of principles – “Prohibition on Interception of Communications; Prohibition on Access of Communications; Pen Registers and Trap and Trace; Disclosure of Records” (ECPA 1986). But it was criticised by the researchers as it was a redundant act in the digital realm (Helft and Millerjan 2011), that was because during that period cyber security threats were unknown to policy and law enforcement horizons. This is evident from the first recorded cyber attacks in 1988, coordinated by a Cornell University student which had crippled 10 per cent of the 88,000 computers on the Arpanet. However, an updated version of the ECPA is the Email Privacy Act 2016 which is still pending in the US Congress.

On the other hand, the EU has evolved a positive approach towards the future of the data protection. In this regard, the Union had adopted the Data Protection Directive (officially Directive 95/46/EC), in 1995. This was adopted just three years after the Maastricht Treaty, the official birth of the European Union. The Directive's data protection principles are unprecedented in nature and had exhibited the depth of European legal standards. This is for the first time at the global level that electronic information or computerised information or data of a European data subject is treated as a natural entity and part of fundamental rights. But on the US side there was no such development in this period for the protection of individual privacy in the cyberspace. Thus, this posed huge challenges to the US law enforcement agencies as well as private companies to have access to personal data of the EU citizens. That was considered as a major blowback for the transatlantic trade. So to mitigate the legal differences, both parties have agreed to the erstwhile Safe Harbour principles after two years of prolonged discussion.

Eventually, in 2000, the Safe Harbour principle has come into being. Indeed, this has marked as one of the key year of policy convergence between the two transatlantic partners, first both have agreed on the principles for the cross-border data flows and harmonisation of the trade relations. Second, after a noted DOS attacks against then “top US companies like – Ebay, Yahoo!, CNN.com., Amazon and others, the Clinton administration first committed \$1.46 billion to fight cyber-terrorism” (Hamblen 1999) and second, adopted the National Plan for Information Systems Protection, 2000. Moreover, the administration released National Security Strategy, 2001, the strategy, for the first time, gave emphasis on cyber threats. In other words, this was the first such attempt by the US administration to ‘*securitise the cyberspace*’.

The year 2001³⁷, in a broader configuration has marked the diffusion and re-centring of global power (Buzan and Lawson 2012: 452) due to the terrorist attacks on 11 September 2001, on the projected image of global security i.e. Pentagon. What was unprecedented about the attack was the terrorists had used no weapons rather opted for civilian airplanes to carry out the attack. This has unfolded two things first – technologies posed huge vulnerabilities to national sovereignty; second – the US as a global hegemon was challenged.

The year also marked as greater convergence in security affairs rather than cyber issues between the EU and US. However, on the cyber front, the Union released *the Network and Information Security: Proposal for A European Policy Approach*, here it underlined the new challenges of digital world with special reference to the Information security, data protection, hacking and cyber crime, but the report does not included cyber security. On the other hand, the administration under the leadership of President G. W. Bush Jr. adopted the USA PATRIOT Act³⁸. This particular act had given the federal agencies and law enforcement agencies a significant amount of power to intrude upon individual privacy. This is one of the major setbacks for the entire privacy and data protection debate in the US, because it has given birth to a surveillance state.

³⁷ The actual beginning of the current research

³⁸ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

This was vehemently criticised by the Electronic Privacy Information Center (EPIC)³⁹, it has argued that “the Act introduced a plethora of legislative changes which significantly increased the surveillance and investigative powers of law enforcement agencies in the United States. On the other hand, the Act did not, however, provide for the system of checks and balances that traditionally safeguards civil liberties in the face of such legislation” (EPCI 2018). From the industries side, Microsoft has suffered huge DNS attack and increasingly cyber attacks have opened the door for public private partnerships. The partnerships were concretised through the National Cyber Security Alliance, with the cooperation between the Department of Homeland Security and industries like Microsoft, Symantec, Cisco Systems, and McAfee etc.

In 2002, the EU adopted the E-Privacy Directive, it is meant to further strengthen the data protection regulations within the Union. It has a mandate to “safeguard the confidentiality of electronic communications in the EU. The E-Privacy Directive is a key instrument to protect privacy and it includes specific rules on data protection in the area of telecommunication in public electronic networks” (EPIC 2018). However, it has been updated timely as per the need of the hour. On the other hand, the Bush administration adopted the Homeland Security Act to empower its internal security apparatus. The Act has created the United States Department of Homeland Security (DHS) and Secretary of Homeland Security at par to the cabinet level. Since the inception of the DHS technology, information security, cyber security and protection of critical infrastructure remain as the key areas of its jurisdiction. With this move the US added another layer of security measures in cyber security approach.

The release of the 2003 European Security Strategy (ESS) can be considered as the benchmark year for the EU’s approach to global security, but not in cybersecurity issues. It is the time when security thinking fed into the EU policy approaches. On the other hand, during the same period, the Bush administration adopted a dedicated strategy for the cyberspace. This strategy clearly stated the challenges and vulnerabilities that are mushrooming in the cyberspace. And there is a need for

³⁹ EPIC an independent non-profit research center in Washington, D.C.

awareness, training, funding and security of the cyber-infrastructure. However, a year later in 2004, the EU ratified its approach by creating the European Network and Information Security Agency (ENISA), that became operationalised in 2005. However, no such major developments were recorded in the US on cyber security matters. The EU strategy for a secure information society was released in 2006. It had the ambition to develop a “dynamic, global strategy in Europe, based on a culture of security and founded on dialogue, partnerships and empowerment” (EC 2005: 3). Moreover, it underlined three emerging challenges to the Union information security, privacy and fight against the cybercrime. On the other hand, the Bush administration also released its second National Security Strategy of United States. It had given special attention to cyber security, information security, cyber crime and other emerging issues. Indeed, this was the year when securitisation of the information society (aka cyberspace) was recorded from both sides of the Atlantic.

If 2001 is considered as the benchmark year in international politics, then 2007, could be noted as the ‘*benchmark year for cyber security studies*’. This was for the first time that large scale cyberattacks were recorded against a sovereign nation. A then sophisticated Distributed Denial of Service (DDoS) attack on the Estonia cyberspace which crippled it for more than 24 hours marked a watershed moment of the cyber war history. Russian influence could not be overlooked totally, but this “landmark incident changed Estonia entirely. It was transformed from being a cyber-victim, to a trend-setter, in digital world” (Heller 2017, Tamkin 2017, McGuinness 2017).

Nonetheless, 2008 was not lesser eventful than the 2007, sophisticated cyber attack on Georgia during the 2008 Russo-Georgian war marked the state intrusion in to the cyberspace during the war time. Second, most significant incident was the WikiLeaks⁴⁰, which published dark secret information especially about the US collecting information.

On the backdrop of major cyber incident with the rise in state involvement persuaded the Union for the first time to view the cyberspace through a security lens. The review of the ESS - Report on the Implementation of the European Security Strategy,

⁴⁰ The process of leaks has started since 2006, but they had disclosed more secret information in 2008 onwards.

categorically addressed the issues of cyber threats. On the other hand, through a strategic move, the NATO established NATO Cooperative Cyber Defence Centre of Excellence, in Tallinn, Estonia, to address the Russian interference in its member states cyberspace.

The Union has given significant consideration for the protection of critical information infrastructure. By releasing the Critical Information Infrastructure Communication in 2009, the Union made it clear that the protection of the critical information and infrastructure is important to its digital security and economy. However, “2009 was a landmark year for the European data protection legal framework. The Lisbon Treaty entered into force in 2009 and it has made data protection and privacy as the prominent aspects of the EU legal order” (Fuster and Gellert 2012, Reding 2012). The Treaty also outlined significant considerations for the protection and processing of personal information. But no convergence was recorded between the EU and US in 2009, in other words, there were no policy outcomes adopted in the US. However, the US established the Cyber Command to enhance its cyber warfare capabilities.

During 2010⁴¹-2012,⁴² one the critical time frame of cyber security research, significant number of cyberattacks such as – Stuxnet malware, sophisticated cyber attack on Google; sensitive cyber attack on Morgan Stanley, use of cyberspace for the Arab uprising, cyber espionage attacks on the Commission and EU’s External Action Service, outbreak of ‘Falme’ espionage attack on Iran and West Asia took place. In a nutshell, the entire period witnessed the rise of state involvement in cyber operations (covert and overt); second, the diffusion of the power, this was the first instance when individual with the help of cyber technologies and social media influence would be able to undermine authoritarian regimes. In the context of the Arab Uprising, yet it was the period when a common individual enjoyed power with the help of cyber technologies; third, business suffered due to increasing cyber and espionage attacks; last but not the least, data protection and privacy was overshadowed by the cyber

⁴¹ Due to outbreak of Stuxnet cyber warfare emerged as a buzzword in security and strategic documents and research outputs.

⁴² Adam Segal in his book Hacked World Order has stated that – 2012 marked a transformation in geopolitics and the tactics of both the established powers and smaller entities looking to challenge the international community.

security issues. In 2010, the EU proposed its Digital Agenda for the Europe to bring in common approach to digital economy within its Member States.

Under the Obama administrations three strategies were released with special attention to the cyberspace - the National Security Strategy in 2010; DoD released its Strategy for Operating in Cyberspace in 2011, and finally the International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World, by the President in 2011. All these strategies have entailed the rising concerns and the US ambitions to shape a global cyber regime. Except 2010 there were no convergence recorded between the US and EU. In 2010, after EU-US Lisbon Summit, “both the parties have recognised the growing challenge of cyber-security and cyber-crime, and thus, established an EU-US Working Group on Cyber-security and Cyber-crime” (Council of the European Union 2010).

The decades of understanding and cooperation had undergone ‘year of stalemate and cyber divergence’ in 2013. A former NSA contractor Edward Snowden exposed the US NSA’s global surveillance project. The EU had treated this matter as serious concerns. The European Parliament President Martin Schulz said in a statement that “he was [I am] deeply worried and shocked about the allegations, [and] if the allegations prove to be true, it would be an extremely serious matter which will have a severe impact on EU-US relations. On behalf of the European Parliament, I demand full clarification and require further information speedily from the U.S. authorities with regard to these allegations” (Levs and Shoichet 2013). Similarly, the then European Commissioner for Home Affairs, Cecilia Malmstrom also showed her concern to her US counterpart Homeland Security Secretary, Janet Napolitano and David Cohen, Treasury under-secretary for terrorism and financial intelligence that “the EU-US relations are going through a ‘delicate moment’ [and] mutual trust and confidence have been seriously eroded and I expect the US to do all that it can to restore them” (Croft 2013).

This trust deficit from its allies and friends around the globe has compelled “the US to restoring trust in internet privacy and data security” (Bendiek and Ridout 2013). After the revelations, Germany and Brazil took the matter with seriousness. First step in this regard was drafting “a non-binding resolution at the UN calling for the protection of

civil and political rights in the digital era” (Bendiek and Ridout 2013). Second, Brazil’s unsuccessful attempt via *NETMundial Initiative* in 2014 for internet governance and cyber security matters. But that fell apart in 2016 just after the withdrawal of World Economic Forum and ICANN. Moreover, the NSA surveillance incidents particularly had lowered the European consumer trust on the US companies. However, things are different now and European consumers are using internet products of US companies. As the new threats are unfolding and rise of cyber incidents necessitates a transatlantic commonness to address the issues.

During the stalemate the Union had taken one step ahead by releasing its first comprehensive Cyber Security Strategy in 2013. The strategy has mooted for ‘an Open, Safe and Secure Cyberspace’. To achieve this, the Union upheld the European values - “the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace” (EC 2013a: 2). Second, there is need for greater coherence among innovation, growth and security between various stakeholders. Third, there is a need to secure the cyberspace through a comprehensive public private partnerships, because “the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading role” (EC 2013a: 2). The cyber security strategy formalised, crystallised and securitised the Union’s approach to cyberspace.

The cyber stalemate and divergence had continued for two more years. In 2014, the US government and industries had faced serious cyber attacks around the globe – US Office of Personal Management and Sony Corporation hack were two incidents that stands out. On the other hand, NATO at the Wales Summit had agreed to enhance its cyber security apparatus. This was evident in the Wales declaration in which the cyber word had been used 22 times. Moreover, they reached a consensus to invoke Article 5 in an outbreak of serious cyber attack on NATO and its member countries.

In the EU legal order, this year has marked another milestone i.e. right-to-be-forgotten landmark judgement on *Google Spain v AEPD and Mario Costeja González*. The European Court of Justice affirmed that “after a particular event of the past and the impact on the community elapsed, the individual has the right to regain his

anonymous life and privacy” (Mantelero 2013: 230). This judgment has significant implications for the individual privacy in the digital age and also observed that living life in an autonomous way is based on the fundamental need of an individual. There are similar instances observed in other parts of the world such as in US, Argentina, India, South Korea and China.

Another watershed judgement was delivered by the CJEU in 2015. In its landmark judgement on “*Schrems vs. Data Protection Commissioner (Case C-362/14)*” that invalidated the decade old ‘Safe Harbour’ agreement between the EU and US for cross border data flows. This year hackers and proxies were quite active in cyberspace. Second time in a row the Office of Personal Management was hacked by cyber attackers.

Since 2015, new trends to hack dating sites, data mining companies, banking and health systems and releasing such information to the dark web were adopted by the cyber hackers. Such incidents were attack on Ashley Madison in 2015, attack on AdultFinder in 2016, sophisticated attack on the Society for Worldwide Interbank Financial Telecommunication in 2016 and Equifax data breach in 2017 created bigger concerns. On other hand, state involvement in cyber intrusion was also on rise, since 2015. Ukraine was the target of multiple sophisticated cyber attacks allegedly linked to Russian sources. Similarly, the Russian hybrid involvement via social media, fake news, disinformation and misinformation to influence US’s 2016 Presidential election has urged the need of cyber governance.

The last national security strategy in 2015 by the Obama administration although covered cyber security matters (19 times appeared) but did not mention data protection and while privacy issues emerged twice in entire documents. The new administration under the leadership of Donald Trump has shown greater commitments towards cyber security if not data protection. The Trump administration’s first national security strategy was released in 2017 and the strategy has also underlined that “there is need to keep America safe in the Cyber Era” (USNSS 2017: 12). The strategy also identified that Russia, China and North Korea is infiltrating the US cyberspace to gain access to data of the Americans. However, the administration also emphasised that “data is like the energy” (USNSS 2017: 3) of cyber world and US

future economic prosperity and future strategy relies on this.

The second most significant development was the release of National Cyber Security Strategy 2018 after a gap of 15 years. In one sentence, the President has expressed the entire strategy “we [US] will continue to lead the world in securing a prosperous cyber future” (USCSS 2018: 2). Third significant step was the enactment of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) 2018 by the Trump administration. It amends the Stored Communications Act (SCA) of 1986 and while updating new laws, it has granted law enforcement agencies to have access to the data that is stored in the cloud outside the US’s territorial jurisdiction. This has brought to an end to the ongoing legal war between the Microsoft Corp. v US (Jeong 2018). The main cause of the legal tussle was that the law enforcement agencies seeking access to the Microsoft data that was stored in the cloud storage, under the provisions of the 1986 Stored Communications Act and the Electronic Communications Privacy Act of 1986 (ECPA). These acts were the product of pre-digital era and thus have thin legal binding to give extraterritorial access of the data to the Law Enforcement Agencies. Therefore, the Microsoft Corp. has little edge over the LEAs to provide the extraterritorial data access. However, the CLOUD Act 2018 now empowered the LEAs to have extraterritorial access to the cloud data.

On the other hand, the EU has adopted the Directive on security of network and information systems (the NIS Directive) in 2016. It has aimed to build a robust and secure digital Union while inculcating “security culture, cooperation and preparedness” (EC 2018) among all Member States. To strength its cybersecurity diplomacy, the Union has adopted *the Cyber Diplomacy Toolbox* in 2017. It has stated that “the EU is concerned by the increased ability and willingness of state and non-state actors to pursue their objectives through malicious cyber activities. Such activities may constitute wrongful acts under international law and could give rise to a joint EU response” (EC 2017d). This could be the new toolbox to cripple the cyber threats through “diplomacy and cyber sanctions regime” (Moret and Pawlak: 2017). The Union has mooted for Permanent Structured Cooperation (PESCO) and Digital Single Market: EU negotiators reach a political agreement on free flow of non-personal data in 2018. The PESCO has clear mandate to develop *Cyber Rapid Response Teams and Mutual Assistance in Cyber Security*, it can be viewed as EU’s

smooth approach to create a cyber defensive and resilient Union. The political agreement on free flow of non-personal data is linked to the digital political economy of the Union, in post GDPR period. This will help to boost the Digital Single Market ambitions of the Union.

An unprecedented legal regime was created around data protection and individual privacy in the EU on 25 May 2018, by adopting the GDPR. The GDPR has not only changed the European data protection laws but nothing less than the whole cyber world as we know it. Cost of not complying with the GDPR would be “punishable by a sanction of up to 4 per cent of the yearly worldwide turnover in case of an enterprise or up to 100 million Euros in all cases” (Albrecht 2016: 287). Industries must follow the privacy by design protocols. In addition, all the experts interviewed by the researcher were of the opinion that encryption of data is extremely important and is an area on which both the EU and the US can further co-operate. However, at this point both the EU and the US have different approaches to data encryption.

In essence, both the EU and the US approaches converge while addressing the issues of cyber security, cyber crime, online radicalisation and cyber terrorism. They have mutual agreed understanding for intelligence sharing. But when it comes to protection of individual privacy and data protection a lot more divergence is evident. In the US, “the law contain data protection principles which also apply when it comes to data processing connected to the protection of national security” (Boehm 2015: 10). While in the EU, the law contain data protection principles that only applies to data protection of European data subject which need to be taken care of legally and technologically. This particular intention is missing in the US legal order. However, “despite their differences on privacy, espionage, and surveillance, the European Union and the United States need to cooperate to solve the attribution problem” (Bendiek 2016). As data is becoming the source of energy, oil and power of the cyber world, thus, data protection and data processing needs to be addressed with similar strategy. Because in the digital age who controls the data, holds the power and can manoeuvre their interest.

CONCLUSION

Sharing same political culture and social culture may not create equal political participation and similar social structure and political outcomes. This has been evident from the transatlantic digital crisis in recent past. Rising incidents of cyber attacks – sovereign states involvement in the internal affairs of another sovereign state implies return of traditional engagements in the cyber ecosystem. Therefore, “one way they could do this is by supporting an effort to create an independent court of arbitration with the forensic capabilities to identify parties responsible for offensive cyber activities. An independent third party would improve the credibility of attributing an incident to a particular state thereby making it responsible” (Bendiek 2016). But then the question arises as to willingness of states concerned in abiding and complying with the court’s decision.

A report by the United States Chamber of Commerce, *Transatlantic Cybersecurity Forging a United Response to Universal Threats*, suggests that there has been a consensus in dealing with the issue of cyber threats. This is an issue both the EU and the US have been working since the 2010 Lisbon Summit. However, the report also underlines “the need for broader and deeper EU and US collaboration on cybersecurity both at the governmental level and within the private sector” (USCC 2017). The transatlantic digital economy relies heavily on how both are acting together because “between them the EU and the US make up the two largest economies in the world, accounting 50 per cent of global GDP, more than 50 per cent of unique IP address in the world and approximately one-third of global trade flows” (USCC 2017: 5). But recent tussle between the Trump administration and EU over data sharing agreement and second the CLOUD Act legislations could be “potentially in conflict with the EU data protection law” (Evans and Mercer 2018) and are thus making the EU and US relations under the cloud.

On other hand, lack of deterrence and due diligence has increased the vulnerabilities to the digital ambitions of the US vis-à-vis the EU. The transatlantic cooperation needs to revitalise and rejuvenate towards ‘*transatlantic commonness*’. In their strategic doctrines, both the EU and the US have given emphasis on multilateral approach to cyber security, normative approach to cyber conflicts, global standards for privacy, data protection and commitments to open, safe and secure cyberspace.

Given the fact that the growing militarisation of cyberspace needs to be addressed soon, in this regard, the EU and the US have a major role to play in the coming years in the cyberspace.

CHAPTER 6

CONCLUSION

The issues related to security are dynamic in international politics and has been the central theme to global politics because, it is essential to all states. No matter whether threats to security have originated internally or outside of the country, it always has tangible repercussions on all aspects of state security. The traditional concept of state security is intertwined with the idea of modern state security – sovereignty, territorial integrity and autonomy. The expansion of the security vocabulary brought in expansion of the security discourse and the expansion of threats to cover non-traditional threats to security that has moved the focus to other aspects such as – human, environmental, political, social, cultural, ethnic, transnational drug and crime syndicate impact on state and society, terrorism and cyber threats.

Cyber security is a new non-traditional threat which poses challenges to state, business, society and individual that increases the unpredictability and vulnerability, and this led to the securitisation of the cyberspace. The states and businesses around the globe are proactively engaged in employing technological solutions to protect the military, strategic and critical infrastructures as well as legal and regulatory approach to address the issue of individual privacy and data protection in the digital age. However, the issue of privacy and data protection has been transformed from a mere political, business and social into technological, legal, regulatory and security problem. Data is the critical resources of all digital activities and the core assets to state, businesses, non-state actors, group and individual and also has issues of privacy, security and power. The future of the digital age is significantly impacted in the way data is being stored, used by governments, businesses and others that would pave the way for new technological developments.

Technological developments are always critical to power equations between states, influencing security concepts and also a driver of global change. The invention of the Gutenberg Press in 1440, (printing press) dramatically changed printing style and the transfer of knowledge and also influenced the social, cultural and industrial behaviours of people, society and states. Likewise, the invention of the steam power influenced the growth of future industries and the invention of the gun powder transformed the future of the warfare.

Above all, the invention of the Internet followed by revolution in computer technology transformed the way state, business and individual interacts in – security, intelligence gathering, warfare, strategy stimulations, risk analysis, business models, social, cultural, economic, political, moreover in industrial research and development. As a result, a new battle-space has opened up: where physical presence has been replaced by bots, drones, robots and virtual presence. The exponential growth in human and machine interactions has created a complex-interconnected-network-interdependence-digital-age.

This complex-interconnected-network-interdependence-digital-age is purely data driven, thus, data is treated as the core element of national power. Through the custody of data, even a small state can enhance its bargaining power in international politics (e.g. Singapore). Similarly, if a corporation get hold of the data, it can challenge the position of a state in global politics. Likewise, by gaining access to the data, non-state actors (groups or individuals) can also challenge the security of state, business, society and individual. Moreover, in the bigger picture, data misuse and leaks compromise, state and business security as well, as it is interlinked to the right to life (e.g. Article 21 Constitution of India), privacy (e.g. GDPR) and liberty (e.g. under the US legal system) of individual in the digital age.

Historically, data was being collected by the states (e.g. Census), businesses (as product feedback) and organisations, groups and society to assess, comprehend, address, and deliver various security and services to update and upgrade the state, businesses and individual. The growth of the Internet in the 1990s paved the way for rapid cyberisation to present digitisation, which transformed various aspects of data collection, reduced the costs and harmonised the access, simultaneously, reduce the human element to collect data by analysing the ‘clicks’.

The ‘click/browse/search’ are observed, recorded, stored (data collection), analysed (metadata), purified (big data), used (AI, IoT, strategising security and business models and delivering services), misused (Facebook and Cambridge Analytica data scandal), all these factors in the digital realm is creating a synergy between the ICT and non-traditional threats. This is why the international security landscape became

more unpredictable while cyber threats are reducing the vulnerability threshold of national and human security. Thus, data security through technological solutions (high end encryption) and data protection through legal, regulatory and political solutions is the need the need of the hour.

The research examined the issue pertaining to cyber security and evaluated and analysed the approach of a post-modern (supranational) actor (the EU) and a modern (state) actor (the US) as actors in international politics and the kind of approaches they have towards cybersecurity and in particular evaluated the convergence and divergence in their policies towards data protection.

Being one of the pioneers for the growth and development of the Internet in 1990s, subsequently, the EU has been enhancing its position as a supranational security actor in the digital age. However, the EU is not a state, thus, that limits its power projection in international politics. The EU has released multiple policies, directives, strategies and regulations to address one of the pressing issues of the 21st century to elevate its status in the global digital security landscape. On the other hand, the EU also engaged in providing widespread affordable access, reliable services, high-end telecommunications networks, easy-to-use-technology to its citizens. Being a highest regulatory body through various timely regulations, it encourages business, start ups to scale up their digital capacities to reach what would attuned as per with global standards. The EU does not have a unified institution (offensive and defensive) to address the diverse nature of cyber threats. The Union's cyber preparedness is a multilayered and patchwork approach which is based on consensus and distributed among the EU level agencies and the national level agencies. The EU perceives cyberspace and cyber security through the diplomatic, normative, economic hard measures and citizen centric approach to cyberspace. The EU is a combination of 27(and UK) member states and their capacities in the cyberspace varies between them and in the long run this could pose challenges to the Union and its digital ambitions. Thus there is a need for harmonising those challenges through active engagement between the member states and EU institutions to enhance both its offensive and defensive capabilities for a better, secure and open digital European Union.

The US created the Internet through the Department of Defense project in response to the Soviet Sputnik followed by the 1962 Cuban missile crisis. Being a modern actor in international politics, it pursues cyber security issues through the prism of national security. The US federal agencies are significantly empowered with modern technologies to access, assess, analyse, comprehend and address various cyber threats. The US proactively manoeuvres its cyber capabilities and capacities to deal with any cyber adversaries. The White House being at the centre of all policy responses to cyber related activities is provides strategic inputs to other federal organisations to develop offensive mechanisms and implement new legislations. The US however in comparison to the EU has and state centric approach to cyber security and also multiple state legislation and frameworks. Over the years, the US approach to the cyber security underwent a significant change from a civilian oversight to a military approach to cyberspace. However, its digital supremacy is constantly challenged by the dynamic growth of technology.

This indicates the volatile, unpredictable and vulnerable nature of the cyber threats. There is a global need to address the difficult terrains of cyberspace to make it secure, open and accessible to all.

Above all, the EU and the US have similar set of agendas to deal with the various issues of cyber preparedness, but there are some differences in their respective approaches to cyber security. At different platforms both shares similar concerns to address different aspects of cyber security - political, economic, social, technological, legal and security related issues. However, there is a huge difference in the way both actors perceive and protect individual privacy and data in the digital age.

The European Union and the United States Approach to Data Protection: Divergence versus Convergence

In a complex-interconnected-networked-interdependent-digital-age, who controls the data? This question is very difficult to answer as there is an extremely complex digital interdependence between state, business and individual which is not found in different level of interactions. One can differentiate between four kinds of cyber actors.

State at the top - There are one set of states that intrude into everything and try to control every action that is under their territorial ambit such as China, Russia and North Korea, erstwhile repressive regimes in West Asia. They have partial to complete state control over digital and natural life of a citizen. In this scenario, the cyberspace is not open and not risk free to access.

Mixed approach – There are second type of states that promote business models for disruptive innovation but it always has backdoor access to everything in the cyberspace. The US model of cyber security and data protection follows a mixed approach. First, it allows businesses to grow rapidly with the condition that whenever it wants to access any metadata that should made available to security agencies. Second, national security is top priority and comes first. Third, it lets business to create its own set of privacy models to protect their consumer’s privacy, and if any violations take place, then the state would intervene.

Regulatory Approach – the EU promotes a regulatory approach to data protection. Being a supranational actor, it has consensus to create regulatory mechanisms to address most complex issues of the digital world. The Union welcomes innovative and disruptive industries to deliver their products and services in the European marketplace but it controls the market monopoly and gives importance to the individual’s freedom of choice and privacy.

Laissez-faire approach – there are set of countries that export the technology and produce data and import to the US. Second, they have very modest and not very effective data protection regulations and no controls over the collection, storage and (mis)use of data. India is one of the prime examples in this regard. Though, New Delhi has been trying but it has not yet been able to produce concrete and robust data protection regulations.

The EU’s approach to data protection is crucial to the emergence of global data protection regimes. The US monopoly in setting agenda and standards visible in other regimes that address security, human rights, preventions of WMD and transfer of technology issues is seen to take a back seat in data protection regime creation. Here the European Union with its GDPR is the path beaker and global standard setter. In

fact, the present day EU regulations have been inspired by decades old regulations and gradual evolution in regulatory frameworks.

During the ARPAnet age in the 1980s and in the initial stages of the World Wide Web in the 1990s, cross border data flows and individual privacy had emerged as one of the key concerns for the world's biggest trading blocs. To address such issues for the first time in 1980, the OECD- Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data, adopted to increase trade relations. Second, the Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in 1981. This is technically for Europe, as well as for the world, the first treaty for the protection of personal data. Third, the UN - Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly Resolution 45/95, passed in 1990 to address the regulatory concerns over computerised personal data.

Just two years after the EU was created in 1992, it came up with one of the strongest data protection regulations - 'the Data Protection Directive (officially Directive 95/46/EC)', to address the pressing issues of the emerging digital age. The Directive had underlined several measures for the protection of European data subjects. And it had also stated that third country must provide 'adequate level' of protection if they would seek to access data. Hereafter, every EU technology related policy has provided ample importance to individual privacy and data protection, placing it over and above economic motives.

The Lisbon Treaty in 2009 further reiterated under Article 16 that personal data protection is a fundamental human right. The Treaty gave prominence to the pre-existed principles in the 1995 Directive and The Charter of Fundamental Rights of the European Union in 2000. Furthermore, the EU Cyber Security Strategy in 2013 and ECJ right to be forgotten judgement in 2014 also have made significant contributions to the emergence of a European data protection regime.

Privacy by design and default in the digital age became a reality after 25 May 2018 as the GDPR came into force. The EU-GDPR is the outcome of two decades of gradual, sophisticated and regulatory revolution that set the robust data protection benchmark for a global regime creation. The GDPR brought in several changes to regulation, data access, data transfer and consequences for the misuse and inadequate security standards. It has also expanded the ambit of EU regulations to each corner of the world, in other words it has given extra territorial right to the EU citizens to protect their privacy in the digital age.

On the other hand, the US views the data protection issues through a different legal framework. The US understanding of privacy and data protection could largely be divided into two parts – first part starts dated back to the Fourth Amendment till 9/11 terrorist attack; second is, Post 9/11 impact till today.

The issue of privacy is core to the US constitutional, judicial and legal developments that is primarily linked since the Fourth Amendment of the US constitution in 1792. In modern days (pre-digital era) the Privacy Act 1974, Foreign Intelligence Surveillance Act 1978, the Electronic Communications Privacy Act 1986 are few developments to understand the regulatory framework in the US. There are other several acts that deal with telecommunications, health, consumer rights and education, these all have provisions for privacy but there is no unified law at the federal level. However, in all these developments, state and national security is seen as the prime area of concerns while individual privacy became a secondary part. In addition the 9/11 terrorist attacks on the US has also pushed the individual privacy to second place and given priority to national security matters.

In the post 9/11 period, the matter of individual privacy and data protection has been a least significant issue in most of the policy and strategic releases of the US. Five national security strategies, two cyber security strategy, and one international strategy for the cyberspace has shown the least concerns to data protection and rather focused on how to securitise the cyberspace from a perspective of enhancing state power and national interest. This is also evident from the four recent incidents – first, the FBI-Apple fiasco – here the FBI ordered Apple Inc. to give access to an Iphone that belongs to a home-grown radical. Apple refused to give the access because it was the

matter of 'trust' between the company and the customer. Later, FBI broke into the device through other means. Second, United States vs. Microsoft Corp. in this case, the US government order Microsoft to give access to the data that was stored in Microsoft cloud in Ireland, under Irish jurisdiction. Microsoft declined, but recent CLOUD Act 2018 empowered the US federal agencies and law enforcement agencies extra-territorial power to access the data. Third, Facebook-Cambridge Analytica data scandal, in this case, the Senate served notice to Mark Zuckerberg to explain the involvement to manipulate the results of the 2016 Presidential election results through big data analytics. Fourth, Google+ data breach issue, the Senate again served a notice to Google CEO, Sundar Pichai to appear and to explain the cause and impact and its policy on data protection and individual privacy. In all three incidents, the privacy and data protection of a US citizen seems more myth than reality as no penalty was imposed on the three companies.

In first two cases, private companies showed unwillingness and drew the silver lining of 'trust' between them and the customers. In the third example, the company involved, manipulated individual privacy for money making. In the Google case, privacy was compromised and exploited due to security flaws in the application. In few hours' long question and answer between the tech-giants and the senators it was clearly evident that, physical world is still very far to understand the metaphor of digital world.

Convergence in Data Protection Approach

The research has found out less convergence between the EU and the US approach to data protection. In the post Directive period, the EU and the US regulatory bodies have agreed to outline the Safe Harbour Privacy Principles (SHPP) for the trans-border data flows in 2000. The US administration has agreed to provide 'adequate level' of protection to the European data stored in the US. In 2015, the European Court of Justice found out that the US had failed to provide 'adequate level' of protection to the EU data subjects. Thus, in a landmark judgement, the ECJ had revoked the decades old SHPP and as per the order, the SHPP was replaced by the Privacy Shield Agreement in 2016. In the new agreement, the US administration has removed redundancy, thin legal bindings to further enhance the trans-border digital data flows.

The EU and the US are the two largest trading partners in the World. They share common political, social and cultural proximities which help trade and economy to flourish. On the other hand, big business like Microsoft, Google, Apple, Facebook, Twitter, have generated most of their profit from the EU as well. In other words, economic linkages are driving forces between the EU and the US both in physical and digital realm. Although, both the partners share common understanding that privacy, freedom of expression, data protection and human rights are the core concepts to keep cyberspace secure, open and accessible to all, their approaches are different and privilege different elements of the cyber world.

Divergence in Data Protection Approach

The research found out few divergences between the EU and US approach to data protection based on – regulation, policy, approach, industry and political aspect

Regulation – It is one of the significant diverging points between the EU and the US. The EU's regulatory evolution is faster, robust and considered individual privacy is vital to both online and offline world. This was evident from the Directive 1995 and the GDPR 2018 which provided unified legal regulations to data protection. In case of the US it is nowhere in the horizon.

Policy – Policy outcomes are often providing the intentions and key concerns of any government. While EU policy documents have treated the data protection as equal to security of a state, the US stands contrary to this. For example the CLOUD Act is meant to give legal access to the US administration to the data have been collected by the US tech companies (Microsoft, Facebook, Google, Apple, Twitter etc). In other words, it has provided an extra-territorial legal access to the administrations to get data access that are stored in the cloud of the India or other countries cyberspace. In contrast, the GDPR provides extra-territorial right to EU citizen to sue a data collector if it failed to protect their privacy and thus has global implications for doing business with the EU.

Approach – There is a big difference in the EU and US approach to data protection. The EU sees the matter of data protection through a human/ individual centric

approach. It implies that rule of law, human rights, fundamental freedoms, and individual privacy, needs to be protected both in the physical and the digital domain. On the contrary, the US national security is top priority than the other things. For instance, the Snowden revelations about NSA surveillance clarify that the prime US concern is securitisation of cyberspace and enhancing state power. That was the reason, the Safe Harbour Privacy agreement was replaced by the Privacy Shield, because there are few legal backdoors through which the US administrations were granted access to the European data.

Industry – the industries have played a vital role in shaping up relationships between states. Most of the US tech companies have collected the European data without providing proper level of protection to it. That was the reason the CJEU’s Scherms judgement has invalidated the Safe Harbour agreements. The Court had found clear violations of EU Directive 1995. In the post-GDPR period if this happens, the concerned company has to pay big fine along with other legal implications.

Political– The present transatlantic political climate is not so conducive for the EU and the US. Given the uncertain future of the Transatlantic Trade and Investment Partnerships, unpredictable and unusual political decisions of President Trump also jeopardise the data protection understanding between them. There are also concerns that Privacy Shield may not be that effective due to US’s uneven decisions making process.

Summary of the Research Findings

The concept of security is dynamic and the advent of cyber technologies has made the security landscape even more unpredictable and enhanced the vulnerability at multiple levels. Thus, there is a need for greater cooperation among states. In the digital age, national security and human security should not be treated with different approaches. There is plethora of challenges that affects both and the state alone cannot deal with, thus here is a need for comprehensive public private partnerships.

Cyberspace is a volatile terrain. Emerging technologies are making significant changes in the cyber security realm. There are two cycles of threats are shaping up, first cyberspace gradually coming under state influence; second the rise and influence

of Big Data and AI would change future of social contract. Data is the power of digital world. Thus, data protection is vital to individual privacy and cyber security. But the lack of national and global regulations is making it difficult to address the issue. A globally accepted law, data protection norms and data protection authority would create a feasible environment for the digital economy and disruptive innovation, with due respect to individual privacy.

The EU is a supranational Union of 27 states that consists of commonness, consensus and connectivity. The EU promotes multilateral and norm based approach to deal with global challenges. The EU approach to cybersecurity is also clearly influenced by its basic premises to deal with threats, such as – norm creation, diplomatic solutions and sanction regime.

The EU approach to data protection is clearly an outcome of gradual evolution in law and legal systems. The EU allows the industries to grow as well due to diligence to protect individual privacy. There would be data protection authority in all member states to address data protection matters apart from traditional judicial systems. The GDPR has outlined a unified and single data protection regulation for all 27 member states and its citizen. It is based on a individual centric approach which would help in global norm creation.

The US approach to cyber security is based on the traditional understanding to address the threats. The US perceives cyberspace as an instrument of national security, like land, water, air and space. The US is militarising the cyberspace, to manoeuvre its offensive and defensive apparatus to address various issues cyberspace. It uses unified approach to cyber security that empowers state to response to an adverse situation.

The US approach to data protection is driven by business model and the state intervenes if any discrepancy would come to the knowledge. The US has patchwork laws to address the data protection issues, which provide scope to the businesses and LEAs to do surveillance and violate consumer/individual rights. The US doest have any data protection authority or ombudsman for public grievance redressal and there is need for robust data protection regulations and data protection authority who would

understand, comprehend and address the issues of the digital world.

The transatlantic partners have converged closely when dealing with cyber security, cyber terrorism, cyber crime, online radicalisation, online drug syndicate, child pornography, political and economic espionage and cyber threats. But data protection does not show similar convergence between them that might be huge factor for misunderstanding and needs to be addressed carefully.

The EU is approaching towards a unified digital union, for that – information, infrastructure and individual rights to be secure from external threats. Thus, there is a need for both offensive and defensive apparatus to deal with emerging threats from cyberspace, if not a unified agency.

The study has found out that both the EU and the US are addressing the issue of cyber threats to security. Both the transatlantic partners have vital convergence while dealing with cyber threats, cyber terrorism, cyber security, online radicalisations, cyber crime and intelligence sharing in all these aspects. But the ‘privacy and data protection’ has emerged as a core divergence between them. The European values on individual privacy, regulatory frameworks on data protection are significantly different from the US’s understanding and commitments to individual privacy and data protection.

The Cyberspace is the rapidly growing fifth domain linked to security and state sovereignty on the one hand and economy and society on the other hand. Current and future technologies are impacting the political and security aspects of the state, while simultaneously transforming the digital economy and security aspects of privacy and data protection. In such a rapidly evolving arena, both the EU and the US will need to be proactive actors in order to build a strong, stable, secure, open and resilient cyber domain. There is greater divergence between the actors on the issue of data protection as they privilege different aspects related to data. In addition, since there are other technology enabled players, the cyber domain provides a good opportunity, for an inclusive regime building in the fifth domain. Thus, creating a global data protection regime may become possible, if the EU and the US enhance their cooperation in this field.

REFERENCES

PRIMARY SOURCES

Ashton, C. (2012), High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the European Commission, *Cyber Security: An Open, Free and Secure Internet*, SPEECH/12/685, October 4, Budapest, [Online: web], Accessed 20 December 2018, URL: http://europa.eu/rapid/press-release_SPEECH-12-685_en.pdf.

Bendiek, Annegret (2017), personal interview, SWP, Berlin, 21 June 2017.

Bush, G.W. (2002), *Outlines Iraqi Threat*, Ohio, Cincinnati Museum Center-Cincinnati Terminal Cincinnati, October, [Online: web], Accessed 05 December 2018, URL: <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB80/new/doc%2012/President%20Bush%20Outlines%20Iraqi%20Threat.htm>.

Byrne, D. (2000), European Commissioner for Health and Consumer Protection, *Cyberspace and Consumer Confidence*, SPEECH/00/316, 18 September, Brussels, [Online: web], Accessed 10 December 2018, URL: http://europa.eu/rapid/press-release_SPEECH-00-316_en.pdf.

Cavelty, Myriam Dunn (2017), Skype to the author, 13 March 2017.

Clinton, B. (2000), *National Plan for Information Systems Protection Version 1.0*, The White House, Washington DC, [Online: web], Accessed 20 October 2018, URL: <https://fas.org/irp/offdocs/pdd/CIP-plan.pdf>.

Commission of the European Communities (2006), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *A strategy for a Secure Information Society – “Dialogue, partnership and empowerment”*, COM(2006) 251, -----, Brussels, [Online: web], Accessed 20 October 2018, URL: http://ec.europa.eu/information_society/doc/com2006251.pdf.

Commission of the European Communities (2001), Communication from the Commission on the Council, the European Parliament, *eEurope 2002 Impact and Priorities*, COM (2001) 140, March 13, Brussels, [Online: web], Accessed 20 October 2018, URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0140:FIN:FR:PDF>.

_____ (2001a), Communication from the Commission on the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *Network and Information Security: Proposal for a European Policy Approach*, COM (2001) 298, June 6, Brussels, [Online: web], Accessed 20 October 2018, URL: http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf.

_____ (2002), Communication from the Commission on the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *eEurope 2005: An Information Society for All*, COM (2002) 263, May 28, Brussels, [Online: web], Accessed 20 October 2018, URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0263:FIN:EN:PDF>.

_____ (2005), Communication from the Commission on the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *i2010 – A European Information Society for Growth and Employment*, COM (2005) 229, June 1, Brussels, [Online: web], Accessed 20 October 2018, URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF>.

_____ (2007), Communication from the Commission on the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *Towards a General Policy on the Fight Against Cyber Crime*, COM(2007) 267, May 22, Brussels, [Online: web], Accessed 20 October 2018, URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>.

Council of the European Union (2005), *The European Union Counter Terrorism Strategy*, November 30, Brussels, [Online: web], Accessed 10 May 2018, URL: <http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf>.

Court of Justice of the European Union (2015), *Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner the Court of Justice declares that the Commission's US Safe Harbour Decision is Invalid*, PRESS RELEASE No 117/15, 6 October 2015, Luxembourg, [Online: web], Accessed 20 October 2018, URL: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>.

Department of Defense (2011), *Department of Defense Strategy for Operating in Cyberspace*, July, Washington DC, [Online: web], Accessed 17 September, 2018, URL: <http://www.defense.gov/news/d20110714cyber.pdf>.

_____ (2015), *The Department of Defense Cyber Strategy*, 17 April 2015, Washington DC, [Online: web], Accessed 17 September, 2018, URL: http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

_____ (2017), “DoD Initiates Elevation Process for U.S. Cyber Command to a Unified Combatant Command”, *Release No: NR-297-17*, 18 August, Virginia, [Online: web], Accessed 17 December, 2018, URL: <https://www.defense.gov/News/News-Releases/News-Release-View/Article/1282920/>.

Department of Homeland Security (2011), “Enabling Distributed Security in Cyberspace Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action”, 23 March, [Online: web], Accessed 17 September, 2018, URL: <https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf>.

_____ (2018a), “Cybersecurity”, Official website of the Department of Homeland Security, Washington DC, [Online: web], Accessed 17 December, 2018, URL: <https://www.dhs.gov/topic/cybersecurity>.

_____ (2018b), “National Cybersecurity and Communications Integration Center”, Washington DC, [Online: web], Accessed 17 December, 2018, URL: <https://www.dhs.gov/national-cybersecurity-and-communications-integration-center>.

Dewar, Robert Scott (2017), Skype to the author, 07 July 2017.

Ebert, Hannes (2017) personal interview, German Institute of Global and Area Studies, Berlin, 27 April, 2017.

ECOSOC (1974), *United Nations: Reports on the Impact of Multinational Corporations on The Development Process and on International Relations: The Report of the Secretary—General to the Economic and Social Council*, International Legal Materials, 13(4): 791-869.

European Commission (1993), *The European Single Market*, [Online: web], Accessed 2 August 2018, URL: https://ec.europa.eu/growth/single-market_en.

_____ (1995), “Directive 95/46/EC of the European Parliament and of the Council”, *Official Journal of the European Communities No L 281/3124*, 24 October, Brussels, [Online: web], Accessed 17 December, 2018, URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en>.

_____ (1997), Electronic Commerce: Commission Presents Framework for Future Action, *A European Initiative on Electronic Commerce*, IP/97/313, 16 April, Brussels, [Online: web], Accessed 10 December 2018, URL: http://europa.eu/rapid/press-release_IP-97-313_en.pdf.

_____ (1999), “Europe without Frontiers”, *Europea.eu*, Brussels, [Online: web], Accessed 17 December, 2018, URL: https://europa.eu/european-union/about-eu/history/1990-1999_en.

European Commission, (2002), *Candidate Countries Eurobarometer 2001*, March 2002, Brussels, [Online: web], Accessed 2 August 2018, URL: http://ec.europa.eu/commfrontoffice/publicopinion/archives/cceb/2001/cceb20011_en.pdf.

_____ (2003), *The EU Becomes Cyber Sherlock Holmes*, IP/03/1443, 24 October, Brussels, [Online: web], Accessed 18 January 2013, URL: http://europa.eu/rapid/press-release_IP-03-1443_en.pdf.

_____ (2004), *Regulation No460/2004 of the European Parliament and of the Council has Establishment of the European Network and Information Security Agency*, Brussels, [Online: web], Accessed 20 October 2012, URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML>.

_____ (2007a), *Funding Opportunities in the Justice, Freedom and Security Policy Areas, for the Period 2007-2013*, MEMO/07/60, 15 February, Brussels, [Online: web], Accessed 20 October 2012, URL: http://www.libertysecurity.org/IMG/pdf_MEMO-07-60_EN.pdf.

_____ (2007b), *Global Policy on the Fight against Cyber Crime*, IP/07/689, 22 May, Brussels, [Online: web], Accessed 20 October 2012, URL: http://europa.eu/rapid/press-release_IP-07-689_en.pdf.

_____ (2007c), *Cross-border Cooperation against Cyber Crime in Europe*, IP/07/1706, 16 November, Brussels, [Online: web], Accessed 20 October 2012, URL: http://europa.eu/rapid/press-release_IP-07-1706_en.pdf.

_____ (2008), “Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union”, *Official Journal of the European Union C 115/01*, 51: 1-361.

_____ (2009a), *Social Networking: Commission Brokers Agreement among Major Web Companies*, IP/09/232, 10 February, Brussels, [Online: web], Accessed 20 October 2012, URL: http://europa.eu/rapid/press-release_IP-09-232_en.pdf.

_____ (2009b), *Commission acts to Protect Europe from Cyberattacks and Disruptions*, IP/09/494, 30 March, Brussels, [Online: web], Accessed 20 October 2012, URL: http://europa.eu/rapid/press-release_IP-09-494_en.pdf.

_____ (2009c), *EU Commissioner Reding Calls for Preventive Action to Make the EU Resilient against Cyber Attacks*, MEMO/09/199, 27 April, Brussels, [Online: web], Accessed 20 October 2012, URL: http://europa.eu/rapid/press-release_MEMO-09-199_en.pdf.

European Commission (2010a), “A Digital Agenda for Europe”, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 245 final/2, 26 August 2010, Brussels, [Online: web], Accessed 17 December, 2018, URL: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN)

European Commission (2010b), Communication From the Commission to the European Parliament and the Council, *The EU Internal Security Strategy in Action: Five Steps Towards a More Secure Europe*, Com (2010) 673 Final, 22 November, Brussels, [Online: web], Accessed 2 August 2018, URL: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0673&from=EN>.

_____ (2011a), Communication from the Commission on the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *Critical Information Infrastructure Protection: Achievements and Next Steps: Towards Global Cyber-Security*, COM (2011) 163, March 31, Brussels, [Online: web], Accessed 20 October 2012, URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF>.

_____ (2011b), *Attitudes on Data Protection and Electronic Identity in the European Union SPECIAL EUROBAROMETER 359*, DG COMM Research and Speechwriting Unit, June, [Online: web], Accessed 05 June 2018, URL: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf.

European Commission (2011c), *Cyber security: EU prepares to set up Computer Emergency Response Team for EU Institutions*, PRESS RELEASE, 10 June, Brussels, [Online: web], Accessed 17 December, 2018, URL: http://europa.eu/rapid/press-release_IP-11-694_en.htm.

_____ (2011d), *Digital Agenda: EU & US Conduct Readiness Tests for Cyber Attacks in Cyber Atlantic 2011*, IP/11/1305, November 3, Brussels, [Online: web], Accessed 20 March 2018, URL: http://europa.eu/rapid/press-release_IP-11-1305_en.pdf.

_____ (2011e), *Internal Security: The EU needs Better Tools to Fight Crime, Terrorism and Extremism*, IP/11/1453, November 25, Brussels, [Online: web], Accessed 20 October 2018, URL: http://europa.eu/rapid/press-release_IP-11-1453_en.pdf.

_____ (2011f), *Internal Security, Special Eurobarometer 371*, DG COMM Research and Speechwriting Unit, November, [Online: web], Accessed 05 June 2018, URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf.

_____ (2011g), “The history of the European Union – 2011”, *Europea.eu*, Brussels, [Online: web], Accessed 17 December, 2018, URL: https://europa.eu/european-union/about-eu/history/2010-today/2011_en.

_____ (2012a), *Europe this week*, 30 March, Brussels, [Online: web], Accessed 20 January 2018, URL: http://europa.eu/rapid/press-release_ETW-12-3003_en.pdf.

_____ (2012b), Europe’s Information Society, *Internet Safer Day*, [Online: web], Accessed 01 July 2018, URL: http://ec.europa.eu/information_society/activities/sip/events/day/index_en.htm.

_____ (2012c), *Cyber security Strengthened at EU Institutions Following Successful Pilot Scheme*, IP/12/949, September 12, Brussels, [Online: web], Accessed 20 January 2018, URL: http://europa.eu/rapid/press-release_IP-12-949_en.pdf.

_____ (2013a), European Union External Action, *EU Cybersecurity plan to Protect Open Internet and Online Freedom and Opportunity*, Press Release, IP/13/94, 7 February, Brussels, [Online: web], Accessed 17 September 2018, URL: http://europa.eu/rapid/press-release_IP-13-94_en.pdf.

_____ (2013b), Commission Staff Working Document Executive Summary of the Impact Assessment, *Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union*, SWD(2013) 31 Final, 7 February, Strasbourg, [Online: web], Accessed 17 September 2018, URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_res_en.pdf.

_____ (2013c), *Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union*, COM(2013) 48 Final, 7 February, Brussels, [Online: web], Accessed 17 September 2018, URL: <http://ec.europa.eu/transparency/regdoc/rep/1/2013/EN/1-2013-48-EN-F1-1.Pdf>.

_____ (2013d), *European Commission Welcomes European Parliament's Vote to Extend Mandate of ENISA and Strengthen EU Cybersecurity*, MEMO/13/341, 16 April, Brussels, [Online: web], Accessed 17 September 2018, URL: http://europa.eu/rapid/press-release_MEMO-13-341_en.pdf.

European Commission (2013e), *Schengen Area*, Migration and Home Affairs, 1 July, [Online: web], Accessed 2 August 2018, URL: <https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen>.

_____ (2013f), *Statement by Vice President Neelie Kroes "On the Consequences of Living in an Age of Total Information"*, MEMO/13/654, 4 July, Brussels, [Online: web], Accessed 17 September 2018, URL: http://europa.eu/rapid/press-release_MEMO-13-654_en.pdf.

_____ (2016a), "Regulation (EU) 2016/679 of the European Parliament and of the Council", *Official Journal of the European Union*, 4 April, Brussels, [Online: web], Accessed 17 December, 2018, URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.

European Commission (2016b), "Regulation (EU) 2016/679 of The European Parliament and of the Council", *Official Journal of the European Union L 119/1*, 27 April, Brussels, [Online: web], Accessed 17 December, 2018, URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en>.

_____ (2016c), *Shared Vision, Common Action: A Stronger Europe, A Global Strategy for the European Union's Foreign and Security Policy*, June, Brussels, [Online: web], Accessed 17 December, 2018, URL: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

European Commission (2016d), *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, Official Journal of the European Union, 19 July 2016, [Online: web], Accessed 20 October 2018, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

European Commission (2016e), “European Commission - Enlargement - Acquis”, European Neighbourhood Policy and Enlargement Negotiations, December, Brussels, [Online: web], Accessed 17 December, 2018, URL: https://ec.europa.eu/neighbourhood-enlargement/policy/glossary/terms/acquis_en.

European Commission (2017a), *EU Cybersecurity Initiatives Working Towards a More Secure Online Environment*, January, Brussels, [Online: web], Accessed 17 December, 2018, URL: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.

_____ (2017b), *Europe 1957-2017: 60 Years of Peace, Democracy, Solidarity*, European Union External Action, 25 March 2017, [Online: web], Accessed 20 October 2018, URL: https://eeas.europa.eu/headquarters/headquarters-homepage_en/23459/Europe%201957-2017:%2060%20years%20of%20peace,%20democracy,%20solidarity.

European Commission (2017c), *Reflection Paper on the Future of European Defence*, COM(2017)315, 7 June, Brussels, [Online: web], Accessed 17 December, 2018, URL: https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf.

European Commission (2017d), “Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions”, Press Release-357/17, 19 June, Brussels, [Online: web], Accessed 17 December, 2018, URL: <http://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/>.

European Commission (2017e), *Digital Single Market, Bringing down barriers to unlock online opportunities*, 07 July 2017, [Online: web], Accessed 2 August 2018, URL: https://ec.europa.eu/commission/priorities/digital-single-market_en.

European Commission (2017f), “Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act)”, COM(2017) 477 final, 13 September, Brussels, [Online: web], Accessed 17 December, 2018, URL: <https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF>.

European Commission (2017g), “Resilience, Deterrence and Defence: Building strong cybersecurity for the EU”, European Commission and the High Representative - Joint Communication to the European Parliament and the Council, JOIN(2017) 450 final,

13 September, Brussels, [Online: web], Accessed 17 December, 2018, URL: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN>.

European Commission (2018a), “Building a European Data Economy”, *Digital Single Market*, 12 October, Brussels, [Online: web], Accessed 17 December, 2018, URL: <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>.

_____ (2018b), “Justice, Freedom and Security”, *EUR-Lex Access to European Union law*, [Online: web], Accessed 17 December, 2018, URL: https://eur-lex.europa.eu/summary/chapter/justice_freedom_security.html?root_default=SUM_1_CODED%3D23&locale=en.

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013), Joint Communication To The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Join (2013) 1 Final, 7 February, Brussels, [Online: web], Accessed 17 September 2018, URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

European Council (2003), *European Security Strategy: a Secure Europe in a Better World*. 12 December. Brussels, [Online: web], Accessed 05 May 2018, URL: <http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>.

_____ (2007), *Lisbon Strategy*, Euro Found 19 March, [Online: web], Accessed 25 June 2018, URL: http://www.eurofound.europa.eu/areas/industrialrelations/dictionary/definitions/lisbon_strategy.htm.

_____ (2008), *Report on the implementation of the European Security Strategy: Providing security in a changing world*. S407/08, 11 December, Brussels, [Online: web], Accessed 05 May 2011, URL: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf.

_____ (2010a), ‘*The Stockholm Program*’ *Summarise of EU Legislation*, (Last Update 16/03/2010), 16 March, [Online: web], Accessed 09 January 2013, URL: http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/jl0034_en.htm.

_____ (2010b), *The Stockholm Programme- an Open and Secure Europe Serving and Protecting Citizens*, *Official Journal of European Union*, 4 May, Brussels, [Online: web], Accessed 20 October 2012, URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF>.

_____ (2010c), *EU-US Summit 2010 Background*, 20 November, Lisbon, [Online: web], Accessed 20 January 2018, URL: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/er/117785.pdf.

_____ (2011), “Opinion of the European Economic and Social Committee on the ‘Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)’”, *Official Journal of the European Union*, C 107/58, Brussels, [Online: web], Accessed 20 January 2018, URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011AE0363&from=HU>.

_____ (2013), *Digital Agenda for Europe*, [Online: web], Accessed 09 June 2013, URL: <https://ec.europa.eu/digital-agenda/en/our-goals/international>.

European Council (2017a), *Cyber attacks: EU ready to respond with a range of measures, including sanctions*, Press Release 357/17, 19 June 2017, Brussels, [Online: web], Accessed 20 October 2018, URL: <https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/>.

European Council (2017b), *Defence cooperation: 23 member states sign joint notification on the Permanent Structured Cooperation (PESCO)*, Press Release, 13 November 2017, [Online: web], Accessed 20 October 2018, URL: <http://www.consilium.europa.eu/en/press/press-releases/2017/11/13/defence-cooperation-23-member-states-sign-joint-notification-on-pesco/>.

European Data Protection Supervisor (2017), *Measuring compliance with data protection rules in EU institutions*, REPORT Survey, 27 November, Brussels, [Online: web], Accessed 20 December 2018, URL: https://edps.europa.eu/sites/edp/files/publication/17-11-27_survey_2017-0130_en.pdf.

European Network and Information Security Agency (2008), *Children on Virtual World: What parents should know*, 01 September, Heraklion (Crete), Greece, ENISA, [Online: web], Accessed 10 December 2018, URL: http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2008/children-on-virtual-worlds/at_download/fullReport.

_____ (2011), *The First Joint Cyber Security Exercise between the EU and US*, 03 November, [Online: web], Accessed 09 June 2018, URL: <http://www.enisa.europa.eu/media/press-releases/first-joint-eu-us-cyber-security-exercise-conducted-today-3rd-nov.-2011>.

_____ (2012), *EU Cyber Cooperation the Digital Frontline*, 05 December, Heraklion (Crete), Greece, ENISA, [Online: web], Accessed 10 June 2018, URL: http://www.enisa.europa.eu/events/enisa-events/enisa-high-level-event-2012/eu-cyber-cooperation-the-digital-frontline/at_download/fullReport.

Europol (2018), “European Cybercrime Centre - EC3 Combating Crime in a Digital Age”, Netherlands, [Online: web], Accessed 17 December, 2018, URL: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>.

Executive Office of the President National Science and Technology Council (2011), *Trust Worthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, December, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf.

Federal Republic Germany (2009), Federal ministry of the interior, *National Strategy for Critical Infrastructure Protection*, (Translation – federal ministry of the interior translation service) 17 June, Berlin,[Online: web], Accessed 20 December 2018, URL: http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf.

_____ (2011), *Cyber Security Strategy for Germany*, February, Berlin,[Online: web], Accessed 20 December 2018, URL: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile.

Frattini, F. (2007), the European Commissioner responsible for Justice, Freedom and Security, *The Changing Nature of Security Threats requires a strong Public-Private Dialogue in Security Research and Innovation*, SPEECH/07/515, September 11, Brussels,[Online: web], Accessed 20 October 2018, URL: http://europa.eu/rapid/press-release_SPEECH-07-515_en.pdf.

Gaycken, Sandro (2017), personal interview, The Digital Society Institute at ESMT, Berlin, 05 July 2017.

Hohmann, Mirko (2017), personal interview, Global Public Policy Institute, Berlin, 17 May 2017.

House of Representatives (2018), *Clarifying Lawful Overseas Use of Data Act, H.R.4943 — 115th Congress (2017-2018)*, United States, [Online: web], Accessed 17 December, 2018, URL: <https://www.congress.gov/bill/115th-congress/house-bill/4943/titles>.

Ilves, T.H. (2007), “H.E. Mr. Toomas Hendrik Ilves President of the Republic of Estonia to the 62nd Session of the United Nations General Assembly”, *United Nations Headquarters*, 25 September, New York, [Online: web], Accessed 17 December, 2018, URL: <http://www.un.org/webcast/ga/62/2007/pdfs/estonia-eng.pdf>.

International Telecommunication Union (2009), “Anniversary year of the Internet and the World Wide Web”, December 2009, [Online: web], Accessed 17 September, 2018, URL: <http://www.itu.int/net/itunews/issues/2009/10/34.aspx>.

International Telecommunications Union (2010), *The World In 2009: ICT Facts and Figures*, ITU, [Online: web], Accessed 20 December 2018, URL: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2009.pdf>.

_____ (2011a), *Understanding Cybercrime: A Guide for Developing Countries*, ITU, [Online: web], Accessed 20 December 2018, URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf.

_____ (2011b), *The World In 2010: ICT Facts and Figures*, ITU, [Online: web], Accessed 20 December 2018, URL: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2010.pdf>.

_____ (2012), *The World In 2011: ICT Facts and Figures*, ITU, [Online: web], Accessed 20 December 2018, URL: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2011.pdf>.

_____ (2013), *The World In 2013: ICT Facts and Figures*, ITU, [Online: web], Accessed 20 June 2018, URL: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf>.

_____ (2018), “Percentage of Individuals using the Internet (excel)”, [Online: web], Accessed 03 December 2018, URL: https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2018/Individuals_Internet_2000-2017.xls.

Johanne, Ahlefeldt (2018), personal interview, PKGr, SPD, Berlin, 12 July 2017.

Kent, Gail (2017), WhatsApp to the author, 03 August 2017.

Klimburg, Alexander (2017), e-mail to the author, 28 February 2017.

Klimburg, A. and Heli, Tirmaa-Klaar (2011), “Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU”, *European Parliament*, 15 April, Brussels, [Online: web], Accessed 17 December 2018, URL: [http://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPOSEDE_ET\(2011\)433828_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPOSEDE_ET(2011)433828_EN.pdf).

Kroes N. (2012), Vice-President of the European Commission responsible for the Digital Agenda, *Public-private cooperation in cybersecurity*, SPEECH/12/47, January 30, Brussels, [Online: web], Accessed 20 December 2018, URL: http://europa.eu/rapid/press-release_SPEECH-12-47_en.pdf.

Liikanen. E. (2000), Member of the European Commission responsible for Enterprise and the Information Society, *The EU Regulation for Cyber Space*, SPEECH/00/319, 19 September, Brussels, [Online: web], Accessed 20 October 2018, URL: http://europa.eu/rapid/press-release_SPEECH-00-319_en.pdf.

_____ (2003), Member of the European Commission responsible for Enterprise and the Information Society, *The European Network and Information Security Agency*, SPEECH/03/65, 10 February, Brussels, [Online: web], Accessed 20 October 2018, URL: http://europa.eu/rapid/press-release_SPEECH-03-65_en.pdf.

Malmström C. (2012), European Commissioner responsible for Home Affairs, *Public-Private Cooperation in the Fight against Cybercrime*, SPEECH/12/409, 31 May, Brussels, [Online: web], Accessed 05 April 2018, URL: http://europa.eu/rapid/press-release_SPEECH-12-409_en.pdf.

Meity (2018), Ministry of Electronics and Information Technology, Government of India, New Delhi, *The Personal Data Protection Bill, 2018*, [Online: web], Accessed 03 January 2019, URL: http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

Ministry of External Affairs India (2015), Ministry of External Affairs, Government of India, New Delhi, *Joint Statement: 2015 United States- India Cyber Dialogue*, 14 August, New Delhi, [Online: web], Accessed 17 December, 2018, URL: http://mea.gov.in/bilateral-documents.htm?dtl/25726/Joint_Statement_2015_United_States_India_Cyber_Dialogue.

Ministry of Defence, Estonia (2008), *Cyber Security Strategy*, Tallinn, [Online: web], Accessed 20 November 2018, URL: http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.

National Science Foundation (2003), “A Brief History of NSF and the Internet”, August, Virginia, [Online: web], Accessed 17 December, 2018, URL: https://www.nsf.gov/od/lpa/news/03/fsnsf_internet.htm.

National Science Foundation (2015), “From programmable backbones to advanced 'apps': An end-to-end vision of the future Internet”, March 26, Virginia, [Online: web], Accessed 17 December, 2018, URL: https://www.nsf.gov/news/news_summ.jsp?cntn_id=134549.

North Atlantic Treaty Organization (2014), *Wales Summit Declaration*, Press Release (2014) 120, 5 September 2014, Wales, [Online: web], Accessed 20 October 2018, URL: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

Obama, B. (2009), *Securing Our Nation's Cyber Infrastructure*, 29 May, The White House, Washington D.C., [Online: web], Accessed 17 September 2018, URL: <http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>.

_____ (2010), *Cyber Security*, The White House, [Online: web], Accessed 05 January 2013, URL: <http://www.whitehouse.gov/cybersecurity>.

_____ (2012), “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy”, *The White House*, February, Washington DC, [Online: web], Accessed 17 December, 2018, URL: <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf>.

_____ (2015), *Remarks by the President at the Cybersecurity and Consumer Protection Summit*, The White House, [Online: web], Accessed 03 January 2019, URL: <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit>.

Organisation for Economic Cooperation and Development (2012), *Internet Economy Outlook 2012 Highlights*, OECD, [Online: web], Accessed 20 January 2018, URL: <http://www.oecd.org/sti/ieconomy/internet-economy-outlook-2012-highlights.pdf>.

Patten, C. (2004), “The Western Balkans: The Road to Europe”, European Commission, SPEECH/04/209, 28 April, Berlin, [Online: web], Accessed 17 December, 2018, URL: http://europa.eu/rapid/press-release_SPEECH-04-209_en.htm#content.

Panetta, L. E. (2012), *Cybersecurity to the Business Executives for National Security*, New York City, U.S. Department of Defense, [Online: web], Accessed 10 January 2018, URL: <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>.

Peters, Ingo (2017), personal interview, Otto-Suhr-Institute of Political Science, Freie Universität Berlin, 26 June 2017.

Phillips, M. (2009), “Introducing the New Cybersecurity Coordinator”, The White House Archives, 22 December, Washington DC, [Online: web], Accessed 17 December, 2018, URL: <https://obamawhitehouse.archives.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator>.

Pohle, Julia (2017), personal interview, WZB, Berlin, 23 March 2017.

Press Information Bureau (2016), “The United States and India: Enduring Global Partners in the 21st Century”, 07 June, New Delhi, [Online: web], Accessed 17 December, 2018, URL: <http://pib.nic.in/newsite/PrintRelease.aspx?relid=146041>.

Radu, Roxana (2017), Skype to the author, 13 March 2017.

Reding V. (2005), Member of the European Commission responsible for the information society and media, *On Internet Governance*, SPEECH/05/457, 15 July, Luxembourg, [Online: web], Accessed 20 October 2018, URL: http://europa.eu/rapid/press-release_SPEECH-05-457_en.pdf.

_____ (2009), Member of the European Commission responsible for information society and media, *Internet of the Future: What Policies to make it Happen?*, SPEECH/09/231, 11 May, Prague, [Online: web], Accessed 20 October 2018, URL: http://europa.eu/rapid/press-release_SPEECH-09-231_en.pdf.

_____ (2014), Vice-President of the European Commission, EU Justice Commissioner, *A data protection compact for Europe*, SPEECH/14/62, 28 January Brussels, [Online: web], Accessed 11 March 2015, URL: http://europa.eu/rapid/press-release_SPEECH-14-62_en.pdf.

Republic of France (2010), *Information System Defence and Security – France’s Strategy*, France, [Online: web], Accessed 20 November 2018, URL: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

Roth, Volker (2017), personal interview, Institute of Computer Science, FU Berlin, 03 March 2017.

Schmidt, H. (2011), “U.S. and Russia: Expanding the “Reset” to Cyberspace”, The White House, 12 July, Washington DC, [Online: web], Accessed 17 December, 2018, URL: <https://obamawhitehouse.archives.gov/blog/2011/07/12/us-and-russia-expanding-reset-cyberspace>.

Schmidt, P. (2000), *ESDI Separable but not Separate*, [Online: web], Accessed 05 June 2013, URL: <http://www.nato.int/docu/review/2000/More-capable-balanced-alliance/ESDI-Separable-but-not-separate/EN/index.htm>.

_____ (2000), “ESDI Separable but not Separate”, *Spring-Summer*, Web edition, 48 (1):12-15 [Online: web], Accessed 05 June 2018, URL: <http://www.nato.int/docu/review/2000/0001-04.htm>.

Schulze, Matthias (2017), personal interview, SWP, Berlin, 21 June 2017.

Skierka, Isabel (2017), personal interview, The Digital Society Institute at ESMT, Berlin, 16 May 2017.

The Council of Europe (2001), *Convention on Cyber Crime*, ETS No. 185, 23 November, Budapest, [Online: web], Accessed 5 September 2018, URL: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

The Department of Justice, (2015), "The Privacy Act of 1974, 5 U.S.C. § 552a", 17 July, Washington DC, [Online: web], Accessed 17 December, 2018, URL: <https://www.justice.gov/opcl/privacy-act-1974>.

The White House (1987), *National Security Strategy of the United States*, January, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1987.pdf>.

_____ (1988), *National Security Strategy of the United States*, January, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1988.pdf>.

_____ (1990), *National Security Strategy of the United States*, March, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1990.pdf>.

The White House (1991), *National Security Strategy of the United States*, August, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1991.pdf>.

_____ (1991), *National Security Strategy of the United States*, August, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1991.pdf>.

The White House (1993), *National Security Strategy of the United States*, January, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1993.pdf>.

_____ (1993), *National Security Strategy of the United States*, January, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1993.pdf>.

The White House (1994), *A National Security Strategy of Engagement and Enlargement*, July, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1994.pdf>.

_____ (1995), *A National Security Strategy of Engagement and Enlargement*, February, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1995.pdf>.

_____ (1996), *A National Security Strategy of Engagement and Enlargement*, February, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1996.pdf>.

_____ (1997), *A National Security Strategy for a New Century*, May, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1997.pdf>.

The White House (1998), *A National Security Strategy for a New Century*, October, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1998.pdf>.

_____ (1998), *A National Security Strategy for a New Century*, October, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/1998.pdf>.

The White House (2000), *A National Security Strategy for a New Century*, December, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/2000.pdf>.

_____ (2001), *A National Security Strategy for a Global Age*, December, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://nssarchive.us/NSSR/2001.pdf>.

The White House (2002), *The National Security Strategy of the United States of America*, September, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://www.state.gov/documents/organization/63562.pdf>.

_____ (2003), *The National Strategy to Secure Cyberspace*, February, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf>.

_____ (2006), *The National Security Strategy of the United States of America*, March, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: <http://www.comw.org/qdr/fulltext/nss2006.pdf>.

_____ (2009), Center for Applied Cybersecurity Research, *Comments to the White House 60-Day Cybersecurity Review*, 27 March, Bloomington, USA, [Online: web], Accessed 17 September 2018, URL: <http://www.whitehouse.gov/files/documents/cyber/Center%20for%20Applied%20Cybersecurity%20Research%20-%20Cybersecurity%20Comments.Cate.pdf>.

_____ (2010), *The National Security Strategy*, May, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

_____ (2011a), *Fact Sheet: Cybersecurity Legislative Proposal*, 12 May, Washington D. C., [Online: web], Accessed 17 September 2018, URL: http://www.whitehouse.gov/sites/default/files/fact_sheet-administration_cybersecurity_legislative_proposal.pdf.

_____ (2011b), *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

The White House (2011c), *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, April, Washington D.C. [Online: web], Accessed 17 September 2018, URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

_____ (2012a), *National Strategy for Information Sharing and Safeguarding*, December, Washington D.C., [Online: web], Accessed 17 September, 2018, URL: http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

The White House (2012b), “We Can’t Wait: Obama Administration Unveils Blueprint for a “Privacy Bill of Rights” to Protect Consumers Online”, *Office of the Press Secretary*, 23 February, Washington DC, [Online: web], Accessed 17 December, 2018, URL: <https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights>.

_____ (2013), Executive Office of the President President’s Council of Advisors on Science and Technology, *Report to the President Immediate Opportunities for Strengthening the Nation’s Cybersecurity*, November, Washington DC [Online: web], Accessed 17 September 2014, URL:

http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf.

_____ (2014), “FACT SHEET: U.S.-EU Cyber Cooperation”, Office of the Press Secretary, 26 March, Washington DC [Online: web], Accessed 17 September 2014, URL:

_____ (2015), *The National Security Strategy of the United States of America*, February, Washington DC [Online: web], Accessed 09 March 2015, URL: http://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

The White House (2017a), *Statement by President Donald J. Trump on the Elevation of Cyber Command*, STATEMENTS & RELEASES, 18 August 2017, Washington DC, [Online: web], Accessed 20 October 2018, URL: <https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/>.

_____ (2017b), *National Security Strategy of the United States*, December, Washington D.C. [Online: web], Accessed 09 December 2018, URL: <http://nssarchive.us/wp-content/uploads/2017/12/2017.pdf>.

The White House (2018a), “The Cost of Malicious Cyber Activity to the U.S. Economy”, *The Council of Economic Advisers*, February, Washington DC, [Online: web], Accessed 17 December, 2018, URL: <https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>.

_____ (2018b), *National Cyber Security Strategy of the United States of America*, September, Washington D.C. [Online: web], Accessed 09 December 2018, URL: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

The White House (2018c), *Cyber-Insurance Metrics and Impact on Cyber-Security*, Washington D. C., [Online: web], Accessed 17 September 2018, URL: <http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf>.

The White House (2018d), *Cybersecurity Framework for Improving Critical Infrastructure: What Others are Saying*, Washington D. C., [Online: web], Accessed 17 September 2018, URL: http://www.whitehouse.gov/sites/default/files/docs/cybersecurity_framework_-_what_others_are_saying.pdf.

The White House (2018e), *National Cybersecurity Center Policy Capture*, Washington D. C., [Online: web], Accessed 17 September 2018, URL: <http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf>.

The White House Archives (2016), "Cyberspace Policy Review", *The White House*, Washington DC, [Online: web], Accessed 17 December, 2018, URL: <https://obamawhitehouse.archives.gov/cyberreview/documents/>.

United Nations General Assembly (1996), "Measures to Eliminate International Terrorism", *A/RES/51/210, 88th Plenary Meeting*, 17 December, New York, [Online: web], Accessed 17 December, 2018, URL: <https://www.un.org/documents/ga/res/51/a51r210.htm>.

United Nations General Assembly (1999), "Developments in the Field of Information and Telecommunications in the Context of International Security", *Resolution Adopted by the General Assembly [on the report of the First Committee (A/53/576)]*, 4 January New York, [Online: web], Accessed 17 December, 2018, URL: <http://undocs.org/A/RES/53/70>.

United Nations Office for Disarmament Affairs (2017), "Developments in the Field of Information and Telecommunications in the Context of International Security", [Online: web], Accessed 17 December, 2018, URL: <https://www.un.org/disarmament/topics/informationsecurity/>.

United Kingdom Cabinet Office (2009), *Cyber Security Strategy of the United Kingdom – Safety, Security and Resilience in Cyber Space*, June, London, [Online: web], Accessed 20 November 2012, URL: <http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf>.

_____ (2010), *A Strong Britain in an Age of Uncertainty: the National Security Strategy*. October, London, [Online: web], Accessed 20 November 2012, URL: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf.

United States Department of Commerce (1998), "Statement of Policy on the Management of Internet Names and Addresses", *National Telecommunications and Information Administration, Docket Number: 980212036-8146-02*, 05 June 1998, Washington DC, [Online: web], Accessed 17 September, 2018, URL: <https://www.icann.org/resources/unthemed-pages/white-paper-2012-02-25-en>.

United States Government Accountability Office (2009), Testimony Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives, *National Cybersecurity Strategy Key Improvements Are Needed to Strengthen the Nation's Posture*, Statement of David Powner, Director, Information Technology Management Issues, GAO-09-432T, 10 March, Washington D.C. [Online: web], Accessed 17 September, 2014, URL: http://www.whitehouse.gov/files/documents/cyber/Congress%20-%20GAO-Powner-SFR_10Mar09.pdf.

Wagner, Ben (2017), personal interview, SWP, Berlin, 16 June 2017.

SECONDARY SOURCES

Adriana, B. (2010), "Reassessing European Union Limits: What Role for the New Regional Partnerships?", *Romanian Journal of European Affairs*, 10 (2): 69-78.

Alasuutari, P. (2004), "The Principles of Pax Americana", *Cultural Studies, Critical Methodologies*, 4 (2): 246-249.

Albrecht J. P. (2016), "How the GDPR Will Change the World", *European Data Protection Law Review*, 2(3): 287-289.

Alberts, S.D. and D.S. Papp (1997), *The Information Age: An Anthology on Its Impact and Consequences*, Vol. I, Washington D.C.: CCRP Publication.

_____ (2000), *Information Age Anthology: National Security Implications of the Information Age*, Vol. II, Washington D.C.: CCRP Publication.

_____ (2001), *Information Age Anthology: The Information Age Military*, Vol. III, Washington D.C.: CCRP Publication.

Alex, M. (2012), "Cyber Probing: The Politicisation of Virtual Attack", *Defence Academy of the United Kingdom, England: Special Series*, [Online: web], Accessed 05 June 2013, URL: http://www.conflictstudies.org.uk/files/Cyber_Probing.pdf.

Algieri, F. (2006–2007), "A Weakened EU's Prospects for Global Leadership", *The Washington Quarterly*, 30(1): 107–115.

American Society of International Law (2007), "The Future of Internet Governance", *Proceedings of the Annual Meeting (American Society of International Law)*, 10: 201-213.

Anderson, et.al. (2016), "Strategic Landpower and a Resurgent Russia: An Operational Approach to Deterrence", *Strategic Studies Institute*, A U.S. Army War College Integrated Research Project in Support of: U.S. European Command and U.S. Army Europe, and U.S. Army War College Press: US.

Armbrecht, Arwen (2016), "What if the internet went down for a day?", *World Economic Forum*, Switzerland, [Online: web], Accessed 17 September, 2018, URL: <https://www.weforum.org/agenda/2016/01/what-if-the-internet-went-down-for-a-day/>.

Ashworth, L. M. (2002), "Did the Realist-Idealist Great Debate Really Happen? a Revisionist History of International Relations", *International Relations*, 16(1): 33-51.

Austin, Robert (2017), "The Balkans: Bad news rising", *European Council on Foreign Relations*, 24 March 2017, [Online: web], Accessed 17 August, 2018, URL: http://www.ecfr.eu/article/commentary_the_balkans_bad_news_rising_7253#.

Archer, C. (2008), *The European Union*, London: Routledge.

- Arquilla, J. and D.A. Borer (2007), *Information Strategy and Warfare: A Guide to Theory and Practice*, New York: Routledge.
- Banisar, D. and Davies, S. (1999), “Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments”, *Journal of Computer & Information Law*, XVIII: 3-108.
- Baran, P. (1964), “On Distributed Communications: I. Introduction to Distributed Communications Networks”, RAND, US, [Online: web], Accessed 20 December 2018, URL: https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf.
- Barrinha, A. and Helena Carrapiço (2016), “The EU’s Security Actorness in Cyber Space: Quo Vadis?”, in, Laura Chappell et al. (eds.), *The EU, Strategy and Security Policy: Regional and Strategic Challenges*, UK: Routledge.
- Bava, U.S. (2007), “The European Union as a Security Actor”, in Rajendra Jain (eds.), *India and the European Union: Building a Strategic Partnership*, New Delhi: Radiant Publisher.
- Bava U.S. (2008), *India–EU Relations: Building a Strategic Partnership*, in, Balme R., Bridges B. (eds.) *Europe—Asia Relations*, London: Palgrave Studies in European Union Politics, Palgrave Macmillan.
- Baylis, J. et al. (eds.) (2011), *The Globalisation of World Politics: An Introduction to International Relations*, Fifth Edition, New York: Oxford University Press.
- Bendiek, A. (2012), “European Cyber Security Policy”, *Stiftung Wissenschaft und Politik (SWP)*, Research Paper-13, October, Berlin [Online: web], Accessed 20 December 2018, URL: https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf.
- _____ (2014a), “Europe Must Balance Digital Hegemon”, *Stiftung Wissenschaft und Politik (SWP)*, 21 January, Berlin, [Online: web], Accessed 2 February 2015, URL: <http://www.swp-berlin.org/en/publications/point-of-view/europe-must-balance-the-digital-hegemon.html>.
- _____ (2014b), “Tests of Partnership Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection”, *Stiftung Wissenschaft und Politik (SWP)*, SWP RP5, March, Berlin, [Online: web], Accessed 2 February 2015, URL: http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2014_RP05_bdk.pdf.
- _____ (2014c), “The Networking of European Foreign Policy: From Cacophony to Choir?”, *Stiftung Wissenschaft und Politik (SWP)*, SWP Comments 48, November, Berlin, [Online: web], Accessed 2 February 2015, URL: http://www.swp-berlin.org/fileadmin/contents/products/comments/2014C48_bdk.pdf.

_____ (2014d), “Cybersecurity and Civil Liberties: A Task for the European Union”, *Ethics and Armed Forces*, 2: 3-5, [Online: web], Accessed 2 February 2015, URL: http://www.ethikundmilitaer.de/fileadmin/Journale/2014-12_English/Cybersecurity_and_Civil_Liberties_-_A_Task_for_the_European_Union_-_Annegret_Bendiek.pdf.

_____ (2016), “Making States Responsible for Their Activities in Cyberspace: The Role of the European Union”, *Council on Foreign Relations*, 15 June, New York, [Online: web], Accessed 20 December 2018, URL: <https://www.cfr.org/blog/making-states-responsible-their-activities-cyberspace-role-european-union>.

Bendiek, A. (2017), “Europe’s Patchwork Approach to Cyber Defense Needs a Complete Overhaul”, *Council on Foreign Relations*, 30 August, New York, [Online: web], Accessed 20 December 2018, URL: <https://www.cfr.org/blog/europes-patchwork-approach-cyber-defense-needs-complete-overhaul>.

Bendiek, A. and Tim, Ridout (2013), “Restoring Trust in Internet Privacy and Data Security”, *SWP*, 25 November, Berlin, [Online: web], Accessed 20 December 2018, URL: <https://www.swp-berlin.org/en/point-of-view/point-of-view-restoring-trust-in-internet-privacy-and-data-security/>.

Bendiek, A., et al. (2017), “The EU’s Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges”, *Stiftung Wissenschaft und Politik, SWP Comments 47*, November, Berlin, [Online: web], Accessed 20 December 2018, URL: https://www.swp-berlin.org/fileadmin/contents/products/comments/2017C47_bdk_etal.pdf.

Bertolotti, M. (1983), *Masers and Lasers: An Historical Approach*, US: CRC Press.

Bignami, Francesca (2015), “The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens”, *Study for the LIBE Committee, GWU Law School Public Law Research Paper No. 2015-54*, Brussels, [Online: web], Accessed 20 December 2018, URL: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2433&context=faculty_publications.

Bindi, F. (2010a), *The Foreign Policy of the European Union: Assessing Europe’s role in the World*, Washington DC, The Brookings Institutions.

_____ (2010b), “EU Foreign Policy: Myth or Reality?”, in Bindi F. (eds.) *The Foreign Policy of the European Union: Assessing Europe’s role in the World*, Washington DC, The Brookings Institution’s press.

Biswas, R.N. (2011), “Is Environment a Security Threat? Environmental Security beyond Securitization”, *International Affairs Review*, Winter, XX (1): 1-22.

Biscop, S. and J.J. Andersson (eds.) (2007), *The EU and the European Security Strategy: Forging a Global Europe*, London: Routledge.

- Biukovic, L. (2002), "International Commercial Arbitration in Cyberspace: Recent Developments", *Northwestern Journal of International Law & Business*, 22(3): 319-352.
- Bock, P. G., and Morton Berkowitz (1966), "The Emerging Field of National Security", *World Politics*, 19(1): 122-36.
- Booth, K. (2007), *Theory of World Security*, New York: Cambridge University Press.
- Bossong, R. and Mark, Rhinard (2013), "The EU Internal Security Strategy Towards a More Coherent Approach to EU Security?", *Studia Diplomatica*, 66(2): 45-58.
- Braumoeller, F. B. (2010), "The Myth of American Isolationism", *Foreign Policy Analysis*, 6, 349-371.
- Bretherton, C. and J. Vogler (2006), *The European Union as a Global Actor*, London: Routledge.
- Bridges B. and Richard, Balme (eds), (2008), *Europe-Asia Relations Building Multilateralisms*, London: Palgrave Macmillan.
- Brown, G. and Christopher D. Yung (2015), "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace", *The Diplomat*, 19 January, [Online: web], Accessed 20 December 2018, URL: <https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/>
- Bryant, Ian and Jasvinder Mahrra (2012), "Challenges to a Trustworthy Cyber Ecosystem", *CrossTalk*, September/October, 8-10, [Online: web], Accessed 17 September, 2018, URL: <https://pdfs.semanticscholar.org/1204/a1499668992da19e1fc1699f8fdd26a78818.pdf>.
- Bryant, R. (2001), "What Kind of Space is Cyberspace?", *Minerva - An Internet Journal of Philosophy*, 5: 138-155.
- Bu-Pasha, S. (2017), "Cross-Border Issues Under EU Data Protection Law With Regards to Personal Data Protection", *Information & Communications Technology Law*, 26(3): 213-228.
- Bush, V. (1945), "Science: The Endless Frontier", Washington DC [Online: web], Accessed 20 December 2018, URL: <https://www.nsf.gov/about/history/vbush1945.htm>.
- Buzan, B. (1983), *People, States, and Fear the National Security Problem in International Relations*, Great Britain: Wheatsheaf Books Ltd.
- _____ (1991), "New Patterns of Global Security in the Twenty-First Century", *International Affairs*, 67 (3): 431-451.

Buzan, et al. (1998), *Security a New Framework for Analysis*, USA: Lynne Rienner Publishers.

Buzan, B. and L. Hansen (eds) (2007), *International Security*, Vol. I, the Cold War and Nuclear Deterance, London: Sage.

_____ (2007b), *International Security*, Vol. II, the Transition to the Post-Cold War Security Agenda, London: Sage.

_____ (2007c), *International Security*, Vol. III, Widening Security, London: Sage.

_____ (2007d), *International Security*, Vol. IV, Debating Security and Strategy and the Impact of 9-11, London: Sage.

_____ (2009), *Evolution of International Security Studies*, New York: Cambridge University Press.

Buzan, B and G. Lawson (2012), "Rethinking Benchmark Dates in International Relations", *European Journal of International Relations*, [Online: web], Accessed 10 March 2018, URL: http://eprints.lse.ac.uk/44759/1/_libfile_REPOSITORY_Content_Lawson%2C%20G_Lawson_Rethinking_%20benchmark_%20dates_2012_Lawson_Rethinking%20benchmark%20dates_2013.pdf.

Bygrave, L. A. (2004), "Privacy Protection in a Global Context – A Comparative Overview", *Scandinavian Studies in Law*, 47: 319–348.

Calvocoressi, P. (2009), *World Politics Since 1945*, Ninth Edition, Harlow: Longman.

Carneiro, R. L. (1970), "A Theory of the Origin of the State", *Science, New Series*, 169(3947): 733-738.

Carrapico, H. and André Barrinha (2017), "The EU as a Coherent (Cyber)Security Actor?", *Journal of Common Market Studies*, 55(6): 1254-1272.

Cassidy, Ben (2003), "Machiavelli and the Ideology of the Offensive: Gunpowder Weapons in 'The Art of War'", *The Journal of Military History*, 67(2):381-404.

Carus, W. S. (2012), "Defining "Weapons of Mass Destruction", Center for the Study of Weapons of Mass Destruction", *Occasional Paper, No. 8*, January, Washington, D.C., National Defense University Press, [Online: web], Accessed 10 March 2015, URL: https://ndupress.ndu.edu/Portals/68/Documents/occasional/cswmd/CSWMD_OccasionalPaper-8.pdf.

Cavelty, D. M. (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, London: Routledge.

Cavelty, M. D. (2007), "Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory", (eds.) in Johan Eriksson, Giampiero Giacomello, *International Relations and Security in the Digital Age*, Abingdon: Routledge, 85-105.

Cavelty, M.D. (2002), *Information Age Conflicts: A Study of the Information Revolution and a Changing Operating Environment*, Zurich, Switzerland: Center for Security Studies.

_____ (2007), "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate", *Journal of Information Technology & Politics*, 4(1): 19-36.

_____ (2007a), Critical Information Infrastructure: Vulnerabilities, Threats and Responses, *Disarmament Forum*, [Online: web], Accessed 17 September 2014, URL: http://mercury.ethz.ch/serviceengine/Files/ISN/47163/ichaptersection_singledocument/738c100b-869a-46c0-8ad9-a05c1ff5f859/en/4_Critical+information+infrastructure.pdf.

Cavelty, M.D. (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Routledge, USA.

_____ (2010), "Cyber-threats", in Myrian D. Cavelti and Victor Mauer (eds.), *The Routledge Handbook of Security Studies*, London: Routledge.

_____ (2011), "Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefence Posture", *IP Global Edition*, 12 (3): 11-15.

_____ (2013), "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies Review*, 15 (1): 105-122.

_____ (2014), "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", *Science and Engineering Ethics*, Springer. Published Online 30 April 2014, [Online: web], Accessed 17 September 2014, URL: http://www.css.ethz.ch/publications/pdfs/Breaking_the_Cyber-Security_Dilemma_2014.pdf.

Cavelty, M.D. and V. Mauer (eds.) (2010), *The Routledge Handbook of Security Studies*, London: Routledge.

Cavelty, M.D., V. Mauer and Sai Felicia Krishna-Hense (eds) (2007), *Power and Security in the Information Age Investigating the Role of the State in Cyberspace*, London: Ashgate Publishing.

_____ (eds) (2007a), *The Resurgence of the State Trends and Processes in Cyberspace Governance*, London: Ashgate Publishing.

Centeno, C. (2002), "Building Security and Consumer Trust in Internet Payments - The Potential of "Soft" Measures", *Institute for Prospective Technological Studies Directorate General Joint Research Centre European Commission, Background Paper No. 7*, Electronic Payment Systems Observatory (ePSO), Seville, [Online: web], Accessed 20 December 2018, URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.196.2496&rep=rep1&type=pdf>.

Cerf, V. G. (1990), "Requiem for the ARPANET", 28 February 1990, [Online: web], Accessed 20 December 2018, URL: http://www.larryblakeley.com/requiem_for_%20arpanet_vceref.htm.

Cerf, V. G. (2017), "2017 Princeton-Fung Global Forum: Vinton G. Cerf", *Princeton-Fung Global Forum, "Society 3.0+: Can Liberty Survive the Digital Age?"*, 21 March 2017, Berlin.

Charney, S. (2012), "Emerging Cyber-Norms Debate: Advancing International Cyber-Security through Strategy and Partnership", *Europe's World*, Spring, 20: 39.

Christou, G. (2016), *Cybersecurity in the European Union, Resilience and Adaptability in Governance Policy*, UK: Palgrave.

Christou, G. (2017), "The EU's Approach to Cybersecurity", *EU-Japan Security Cooperation online paper*, (Spring/Summer): 1-13, [Online: web], Accessed 20 December 2018, URL: http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf.

Clark, D. (2010), "Characterizing Cyberspace: Past, Present and Future", *MIT, CSAIL, Version-1.2*, 12 March, 2010, [Online: web], Accessed 20 December 2018, URL: https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf.

Clark, D. D. (1988), "The Design Philosophy of the DARPA Internet Protocols", *Computer Communication Review, Originally published in Proc. SIGCOMM '88, Computer Communication Review*, 18(4): 106–114.

Cobb, S. (2016), Data privacy and data protection: US law and legislation white paper, *WeLiveSecurity*, 26 April 2016, [Online: web], Accessed 20 October 2018, URL: <https://www.welivesecurity.com/2016/04/26/data-privacy-data-protection-us-law-legislation-white-paper/>.

Cohen, J.L. (2005), "The Balkans Ten Years After: From Dayton to the Edge of Democracy," *Current History*, 104: 365. [Online: web], Accessed 05 June 2013, URL: http://www.currenthistory.com/pdf_user_files/104_685_365.pdf.

Colón-Fung, I. (2007), "Protecting the New Face of Entrepreneurship: Online Appropriate Dispute Resolution and International Consumer-To-Consumer Online Transactions", *Fordham Journal of Corporate & Financial Law*, 12(1): 233-258.

- Cooper, R. (2000), *Post-Modern State and the World order*, UK: DEMOS.
- Cooper, R. (2003), *The Breaking of Nations. Order and Chaos in the Twenty-First Century*, London: Atlantic Books.
- Copper, F. J. (1975), “The Advantages of A Multipolar International System: An Analysis of Theory And Practice”, *International Studies*, 14(3): 397-415.
- Craze, M. Jack (1997), 'Balls of Missive Ruin: Milton and the Gunpowder Revolution', *The Cambridge Quarterly*, 26(4): 325-343.
- Cummings, M. L. (2017), “Artificial Intelligence and the Future of Warfare”, Chatham House, 26 January, UK, [Online: web], Accessed 17 September, 2018, URL: <https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf>.
- Daalder, I. and Robert, Kagan (2016), “The U.S. can’t afford to end its global leadership role”, Brookings, 25 April, [Online: web], Accessed 20 December 2018, URL: <https://www.brookings.edu/blog/order-from-chaos/2016/04/25/the-u-s-cant-afford-to-end-its-global-leadership-role/>.
- Dellios, Rosita (2004-05), “The Rise of China as a Global Power”, *The Culture Mandala*, 6(2), [Online: web], Accessed 17 September, 2018, URL: <http://www.international-relations.com/CM6-2WB/GlobalChinaWB.htm>.
- Demchak, C. (2010), “Conflicting Policy Presumptions about Cybersecurity: Cyber-Prophets, Priests, Detectives, and Designers, and Strategies for a Cybered World,” *Atlantic Council*, Issue Brief, 12 August 2010, Washington, D.C., [Online: web], Accessed 20 December 2018, URL: http://www.atlanticcouncil.org/images/files/publication_pdfs/403/Demchak-brief.pdf.
- Demchak, C.C. and P.J. Dombrowski (2011), “Rise of a Cybered Westphalian Age”, *Strategic Studies Quarterly*, 5(1): 31–62.
- Deibert, J.R. and R. Rohozinski (2010), “Risking Security: Policies and Paradoxes of Cyberspace Security”, *International Political Sociology*, 4 (1): 15-32.
- Dorenmalen, H.V. (2012), “The Cyber-security Challenge”, *Europe’s World*, Spring 20: 40.
- Denning, D. (2015), “The Rise of Hacktivism”, *Georgetown Journal of International Affairs*, 08 September, [Online: web], Accessed 20 December 2018, URL: <https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism?rq=hacktivism>.
- Derian, J. D. (2009), *Critical Practices in International Theory: Selected Essays*, Routledge: UK.

Dewar, R. S. (2017), *Cyber Security in the European Union: An Historical Institutional Analysis of A 21st Century Security Concern*, PhD Thesis, Scotland: University of Glasgow.

Dittmar, J. E. (2011), "Information Technology and Economic Change: The Impact of the Printing Press", *The Quarterly Journal of Economics*, 126(3): 1133-1172.

Dodge, M. (1999), "The Geographies of Cyberspace", *CASA Working Paper Series*, Paper 8, May, London, [Online: web], Accessed 20 December 2018, URL: <http://discovery.ucl.ac.uk/266/1/cyberspace.pdf>.

Doyle Sir A. C. (1892), *The Adventure of the Copper Beeches*, UK: Happer & Brothers.

e Silva, K. (2013), "Europe's Fragmented Approach Towards Cyber Security", *Internet Policy Review*, 2(4): 1-8.

Edwards, Benjamin, et al. (2017), "Strategic Aspects of Cyberattack, Attribution, and Blame", *PNAS*, 114(11): 2825-2830.

Electronic Privacy Information Center (2015), "The Right to Be Forgotten (Google v. Spain)", EPIC, Washington DC, [Online: web], Accessed 20 December 2018, URL: <https://epic.org/privacy/right-to-be-forgotten/>.

Electronic Privacy Information Center (2018a), "USA Patriot Act", *EPIC*, [Online: web], Accessed 20 October 2018, URL: <https://www.epic.org/privacy/terrorism/usapatriot/>.

Electronic Privacy Information Center (2018b), EU Privacy and Electronic Communications (e-Privacy Directive), *EPIC*, [Online: web], Accessed 20 October 2018, URL: https://epic.org/international/eu_privacy_and_electronic_comm.html.

Engelman, Ryan (2015), "The Second Industrial Revolution, 1870-1914." *US History Scene*, 10 April, [Online: web], Accessed 17 September, 2018, URL: <http://ushistoryscene.com/article/second-industrial-revolution/>.

Eriksson, Johan and Giampiero Giacomello (eds.) (2007), *International Relations and Security in the Digital Age*, Abingdon: Routledge.

Eriksson, J. and G. Giacomello (2006), "The Information Revolution, Security, and International Relations: (IR) relevant Theory?", *International Political Science Review*, 27 (3): 221-244.

_____ (2007), *International Relations and Security in the Digital Age*, London: Routledge.

EuroWire (2011), "The Growing Pain in EU Cyber Security Policy", *Bertelsmann Foundation, Capitol Hill's Connection to Brussels*, [Online: web], Accessed 05 June 2013, URL: <http://www89.pair.com/bfemail/EuroWire-July2011.pdf>.

Evans, H. and S. T. Mercer (2018), "Privacy Shield on Shaky Ground: What's up with EU-U.S. Data Privacy Regulations", *Lawfare*, 2 September 2018, [Online: web],

Accessed 20 October 2018, URL: <https://www.lawfareblog.com/privacy-shield-shaky-ground-whats-eu-us-data-privacy-regulations>.

Fahey, E. (2014) "EU'S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security", *European Journal of Risk Regulation*, 5(1): 46-60.

Felici M. (eds) (2013), *Cyber Security and Privacy, Trust in the Digital World and Cyber Security and Privacy EU Forum 2013 Brussels*, Belgium, April 18-19, 2013 Revised Selected Papers, Springer, Verlag Berlin Heidelberg.

Filtborg, et al. (2002), "An alternative theoretical approach to EU foreign policy 'network governance' and the case of the Northern Dimension Initiative", *Cooperation and Conflict: Journal of the Nordic International Studies Association*, 37(4): 387-407.

Fox, W.T. R. (1968) "Science, Technology and International Politics", *International Studies Quarterly*, 12(1): 1-15.

Francis, A. K. (2007), *Charles Darwin and the Origin of Species*, Westport: Greenwood Press.

Frum, D. (2014), "The Real Story of How America Became an Economic Superpower", *The Atlantic*, 24 December, [Online: web], Accessed 20 December 2018, URL: <https://www.theatlantic.com/international/archive/2014/12/the-real-story-of-how-america-became-an-economic-superpower/384034/>.

Fuster, G. G. and R. Gellert (2012), "The Fundamental Right of Data Protection in the European Union: in Search Of an Uncharted Right", *International Review of Law, Computers & Technology*, 26 (1): 73-82.

Gady, Franz-Stefan (2012), "U.S.-India Cyber Diplomacy: A Waiting Game", *The National Interest*, 24 October, United States, [Online: web], Accessed 20 December 2018, URL: <http://nationalinterest.org/commentary/us-india-cyber-diplomacy-waiting-game-7662>.

Gady, Franz-Stefan and Greg Austin (2010), "Russia, the United States, and Cyber Diplomacy Opening the Doors", *The East West Institute*, New York, United States, [Online: web], Accessed 20 December 2018, URL: https://www.files.ethz.ch/isn/121211/USRussiaCyber_WEB.pdf.

Garrard, J. and Carol Garrard (2008), *Russian Orthodoxy Resurgent: Faith and Power in the New Russia*, Princeton University Press, US.

George, J. (1989), "International Relations and the Search for Thinking Space: Another View of the Third Debate", *International Studies Quarterly*, 33(3): 269-279.

Gibson, W. (1984), *Neuromancer*, US: Phantasia Press (1986).

Ginsberg, R.H. (1999), “Conceptualizing the European Union as an international actor: Narrowing the theoretical capability–expectations gap”, *Journal of Common Market Studies*, 37(3): 429–454.

Ginsberg, Roy H., and Smith, Michael E (2007), “Understanding the European Union as a global political actor: Theory, practice, and impact”, In: UNSPECIFIED, Montreal, Canada (Unpublished).

Gnesotto, N. (eds) (2004), *EU security and defence policy: the first five years (1999-2004)*, Paris: European Union Institute for Security Studies.

Grauman, B. (2012), “Why the Cyber-revolution still lacks a Global Rulebook”, *Europe’s World*, Spring, 20: 44-45.

Gray, A. (2017), “From early explorers to Trump – a history of the transatlantic relationship”, *World Economic Forum*, 12 January, Switzerland, [Online: web], Accessed 17 September, 2018, URL: <https://www.weforum.org/agenda/2017/01/from-early-explorers-to-trump-a-history-of-the-transatlantic-relationship/>.

Grech, V. (2001), “Publishing on the WWW. Part 5 - A brief history of the Internet and the World Wide Web”, *Images Paediatr Cardiol*, 3(3): 15-2.

Greer, A. and Nathan, Montierth (2017), “How Are US-China Cyber Relations Progressing?”, *The Diplomat*, [Online: web], Accessed 20 December 2018, URL: <https://thediplomat.com/2017/11/how-are-us-china-cyber-relations-progressing/>.

Gregory, F. (2005), “The EU’s Response to 9/11: A Case Study of Institutional Roles and Policy Processes with Special Reference to Issues of Accountability and Human Rights.” *Terrorism and Political Violence*, 17(1–2): 105–23.

Gregory, A. M. and Glance, D. (eds) (2013), *Security and the Networked Society*, Switzerland: Springer.

Greicevci, L. (2011), “EU Actorness in International Affairs: the Case of EULEX Mission in Kosovo”, *Perspectives on European Politics and Society*, 12 (3): 283-303.

Griffin, J.A. (2002), “Privacy and security in the Digital Age”, *IEEE Xplore*, [Online: web], Accessed 17 September, 2018, URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=689168>.

Gunkel, J.D. (2001), *Hacking Cyberspace*, USA: Westview Press.

Morgenthau, Hans J. (1948), *Politics among Nations: The Struggle for Power and Peace*, Alfred A. Knopf: New York.

Harknett, R. J. and James A. Stever (2011), “The New Policy World of Cybersecurity”, *Public Administration Review*, May/June 455-460.

Hansen, L. and H. Nissenbaum (2009), “Digital Disaster, Cyber Security, and the Copenhagen School”, *International Studies Quarterly*, 53 (4): 1155-1175.

Hass, E.B. (1991), *When Knowledge is Power: three models of change in International Organisation*, Berkeley: University of California Press.

Hathaway, E.M. (2012), "Leadership and Responsibility for Cybersecurity", *Georgetown Journal of International Affairs*, Special Issue, 71-80.

Herz, J. H. (1957), "Rise and Demise of the Territorial State", *World Politics*, 9(4): 473-493.

Herzog, Stephen (2011), "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, 4(2): 49-60.

Herzog, S. (2011), "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Response", *Journal of Strategic Security*, 4(2): 49-60.

Huysmans, J. (1998), "Revisiting Copenhagen:: Or, On the Creative Development of a Security Studies Agenda in Europe", *European Journal of International Relations*, 4(4):479–505.

Hsu, D. F. and Dorothy Marinucci (2015), "Cybersecurity: Toward a Secure and Sustainable Cyber Ecosystem", *The IEEE Computer Society*, 12-14.

Huntington, P. S. (1999), "The Lonely Superpower", *Foreign Affairs*. 78(2): 35-49.

Ikenberry, J. G. (2005), "Power and liberal order: America's post-war World Order in Transition", *International Relations of the Asia-Pacific*, 5(2): 133–152.

Ikenberry, John (2008), "The Rise of China and Future of the West", *Foreign Affairs*, 87(1): 23-37.

Intelligence and National Security Alliance (2009), "Addressing Cyber Security through Public-Private Partnership: An Analysis of Existing Models", November, [Online: web], Accessed 20 December 2012, URL: <http://www.insonline.org/CMDDownload.aspx?ContentKey=e1f31be3-e110-41b2-aa0c-966020051f5c&ContentItemKey=161e015c-670f-449a-8753-689cbc3de85e>.

Islam, S. (2003), Big Bang Expansion of the European Union, 28 January, Yale Global Online, [Online: web], Accessed 05 June 2013, URL: <http://yaleglobal.yale.edu/content/big-bang-expansion-european-union>.

Jay, R.P. (2014), *Data Protection & Privacy in 26 Jurisdictions Worldwide*, UK: Law Business Research Ltd.

Kaldor, M. (2013), "In Defence of New Wars", *Stability: International Journal of Security and Development*, 2(1): 1-16.

Kaunert, C. and S. Leonard (2012), "Introduction: Supranational Governance and European Union Security after the Lisbon Treaty- Exogenous Shocks, Policy Entrepreneurs and 11 September 2001", *Cooperation and Conflict*, 47(4):417-432.

Kaldor, M. (2004), "Nationalism and Globalisation," *Nations and Nationalism* 10 (1–2): 161–177.

_____ (2007), *New and Old Wars Organised Violence in a Global Era*, 2nd edition, Stanford: Stanford University Press.

Keohane, R.O. and J. Nye (1998), "Power and Interdependence in the Information Age", *Foreign Affairs*, 77(5): 81-94.

_____ (2001), *Power and Interdependence*, 3rd Edition, New York: Longman.

Keukeleire, S. (2003), "The European Union as a diplomatic actor: Internal, traditional, and structural diplomacy", *Diplomacy and Statecraft*, 14(3): 31–56.

Kissinger, H. (2014), *World Order: Reflections on the Character of Nations and the Course of History*, USA: Penguin Press.

Kranzberg, M. (1986), "Technology and History: "Kranzberg's Laws"", *Technology and Culture*, 27(3): 544-560.

Kremer, F. J. and Muller, B. (eds) (2014), *Cyberspace and International Relations: Theory, Prospects and Challenges*, Berlin: Springer.

Kaspersen, A. et al. (2016), "10 trends for the future of warfare", *The World Economic Forum*, 03 November, Switzerland, [Online: web], Accessed 17 September, 2018, URL: <https://www.weforum.org/agenda/2016/11/the-4th-industrial-revolution-and-international-security/>.

Katz, J. E. (1988), "US Telecommunications Privacy Policy: Socio-Political Responses to Technological Ddvances", *Telecommunications Policy*, 12 (4): 353-368.

Kaunert, C and Zwolski, K (2013), *The EU as a Global Security Actor: A Comprehensive Analysis Beyond CFSP and JHA*, Palgrave Macmillan: UK.

Kavanagh, C. (2017), "The United Nations, Cyberspace and International Peace and Security Responding to Complexity in the 21st Century", *The United Nations Institute for Disarmament Research (UNIDIR)*, [Online: web], Accessed 20 December 2018, URL: <http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf>.

Kavalski, E. (2005), *Peace in the Balkans: The Influence of Euro-Atlantice Actors in the Promotion of Security-Community-Relations in Southeastern Europe*, Ph.D. Thesis, UK, Loughborough University.

Keohane, R. and Stanley, Hoffman (eds.), (1991), *The New European Community: Decision Making and Institutional Change*, Boulder: Westview Press.

King, C. (2008), "The Five-Day War Managing Moscow After the Georgia Crisis", *Foreign Affairs*, 87(6): 2-11.

- Kirk, G. (1945), "National Power and Foreign Policy", *Foreign Affairs*, 23(4): 620-626.
- Kleinrock, L. (2010), "An Early History of the Internet", *IEEE Communications Magazine*, (August): 26-36.
- Koltai, R. Steven, (2016), "Brexit and the lessons of history", *Brookings*, 27 June 2016, [Online: web], Accessed 20 December 2017, URL: <https://www.brookings.edu/blog/fixgov/2016/06/27/brexit-and-the-lessons-of-history/>.
- Krauthammer, C. (1990/91), "The Unipolar Moment", *Foreign Affairs*, 70(1): 23-33.
- Kshetri, N. (2010), *The Global Cybercrime Industry*, Berlin: Springer.
- Kshetri, N. (2013), "Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers", *Crime Law Soc Change*, 60:39–65.
- Kulikova, A. (2015), "China-Russia cyber-security pact: Should the US be concerned?", *Russia Direct*, 21 May, Russia, [Online: web], Accessed 20 December 2018, URL: <http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned>.
- Kurbalija, J. (2015), "Different Prefixes, Same Meaning: Cyber, Digital, Net, Online, Virtual, E-", *DiPLO*, 15 April, Geneva, [Online: web], Accessed 20 December 2018, URL: <https://www.diplomacy.edu/blog/different-prefixes-same-meaning-cyber-digital-net-online-virtual-e>.
- Kurbalija, J. and D. MacLean (2007), "Internet Governance", *International Institute for Sustainable Development*, September 2007, Manitoba, [Online: web], Accessed 20 October 2018, URL: https://iisd.org/pdf/2007/igsd_internet_gov.pdf.
- Lake, D. A. (2009), "The State and International Relations", (eds.), in Christian Reus-Smit and Duncan Snidal, *The Oxford Handbook of International Relations*, UK: OUP.
- Lan, T. (2011), "Real Rules for Virtual Space", *Beijing Review*, 54(47):1-2.
- Lane, N. (2008), "US Science and Technology: An Uncoordinated System that Seems to Work", *Technology in Society*, 30(3-4): 248-263.
- Lapid, Y. (1989), "The Third Debate: On the Prospects of International Theory in the Post-Positivist Era", *International Studies Quarterly*, 33(3): 235-254.
- Lallana, E. and M.N. Uy (2003), *The Information Age*, e-ASEAN Task Force and UNDP-APDIP, [Online: web], Accessed 05 May 2013, URL: http://www.unapcict.org/ecohub/resources/the-information-age/at_download/attachment1.
- Lasater, Martin (1984) "UNESCO – Time to Leave", *The Heritage Foundation*, URL - <http://www.heritage.org/report/unesco-time-leave>

Libicki, M. (2007), *Conquest in Cyberspace: National Security and Information Warfare* London: Cambridge University Press.

_____ (2009), “*Cyberdeterrence and Cyberwar*, U.S.: RAND Corporation”.
March, J.G. and J.P. Olsen (1995), *Democratic Governance*, New York: The Free Press.

Leffler, M.P. (1984), “The American Conception of National Security and the Beginnings of the Cold War, 1945-48”, *The American Historical Review*, 89(2): 346-381.

Leitenberg, Milton (2003), “Deaths in Wars and Conflicts in the 20th Century”, *Cornell University, Peace Studies Program, Occasional Paper #29*, [Online: web], Accessed 17 September, 2018, URL: https://www.clingendael.org/sites/default/files/pdfs/20060800_cdsp_occ_leitenberg.pdf.

Leonard, M. (2005), *Why Europe Will Run the 21st Century*, PublicAffairs, US.

Lewis, J. (2018), “Economic Impact of Cybercrime—No Slowing Down”, *Center for Strategic and International Studies*, February, Washington DC, [Online: web], Accessed 20 December 2018, URL: <https://www.csis.org/analysis/economic-impact-cybercrime>.

Lewis, A. J. and Katrina Timlin (2011), “Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organisation”, *The United Nations Institute for Disarmament Research (UNIDIR)*, [Online: web], Accessed 20 December 2018, URL: <http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf>.

Lewis, H. and Cecilia Liao (2014), “Data Nation 2014 Putting Customers First”, *Deloitte*, [Online: web], Accessed 20 December 2018, URL: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/deloitte-analytics/deloitte-uk-data-nation-2014.pdf>.

Lewis, J. A. and Stewart A. Baker (2014), “Net Losses: Estimating the Global Cost of Cybercrime”, *Centre for Strategic and International Studies*, June 2014, [Online: web], Accessed 20 December 2018, URL: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

Lewis, P. et al. (2018), “The Future of the United States and Europe an Irreplaceable Partnership”, *Research Report, Chatham House*, April, UK, [Online: web], Accessed 17 September, 2018, URL: <https://www.chathamhouse.org/sites/default/files/publications/research/2018-04-11-future-united-states-europe-irreplaceable-partnership.pdf>.

Lieberthal, K. and Peter W. Singer (2012), "Cybersecurity and U.S.-China Relations", Brookings, February 2012, [Online: web], Accessed 20 December 2018, URL: https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf.

Long, W.R.M., et al. (2017), "United Kingdom", in Raul, A.C. (eds.), *The Privacy, Data Protection and cybersecurity Law Review*, Fourth Edition, United Kingdom: Law Business Research Ltd.

Lundin, Erik Lars (2012), "From a European Security Strategy to a European Global Strategy: Take II: Policy options", Occasional Papers No - 13, *The Swedish Institute of International Affairs*, 21 December 2012.

Lynn III, F. W (2010), "Defending a New Domain the Pentagons's Cyberstrategy", *Foreign Affairs*, 89(5): 97-108.

Ma, J. (2016), "Cybermatics for Cyberization towards Cyber-Enabled Hyper Worlds", *4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, Oxford: 85-86.

Manners, I. (2002), "European [security] Union: from existential threat to ontological security", Copenhagen: Copenhagen Peace Research Institute, [Online: web], Accessed 17 September, 2018, URL: https://static-curis.ku.dk/portal/files/172360381/Ian_Manners_European_security_Union_from_existential_threat_to_ontological_security_COPRI_5_2002.pdf.

Manners, I. (2006), "European Union 'Normative Power' and the Security Challenge", *European Security*, 15(4): 405-421.

Mantelero, A. (2013), "The EU Proposal for a General Data Protection Regulation and, the roots of the 'right to be forgotten'", *Computer Law & Security Review*, 29 (3): 229-235.

Maruel, M. E. (2010), *China in 21st Century: China's Cyberwarfare Capability*, New York: Nova Science Publishers.

Matthews, J. T. (1989), "Redefining Security", *Foreign Affairs*, 68(2): 162 – 177.

Mayer, Maximilian, et al. (eds.) (2014), *The Global Politics of Science and Technology: An Introduction – Vol. 1*, Heidelberg: Springer.

McCormick, Thomas J. (1997), "The Promises and Perils of American Hegemony", *Revue Française d'Études Américaines*, 72: 81-90.

Moga, L.T. (2009), "The Contribution of the Neofunctionalist and Intergovernmentalist Theories to the Evolution of the European Integration Process", *Journal of Alternative Perspectives in the Social Sciences*, 1(3): 796-807.

Mearsheimer, J.J. (1990), "Back to the Future: Instability in Europe after the Cold War", *International Security*, 15 (1): 5-56.

_____ (2000), *The Tragedy of Great Power Politics*, New York: Norton.

Moore, G. (1965), "Cramming More Components onto Integrated Circuits", *Electronics*, April: 114-117, reprinted 1998.

Mutimer, D. (2010), "Critical Security Studies", in Myrian D. Cavelti and Victor Mauer (eds.), *The Routledge Handbook of Security Studies*, London: Routledge.

Mohan, R. C. (2014), "Towards International Treaty on Cybersecurity: A Bilateral Dialogue Between India and the US", in Samir Saran et al. (eds.) *Indo-US Cooperation on Internet Governance and Cybersecurity*, Observer Research Foundation, New Delhi.

Montalbano, E. (2011), "U.S., Russia Forge Cybersecurity Pact", *Dark Reading*, 7 July, [Online: web], Accessed 20 December 2018, URL: <https://www.darkreading.com/risk-management/us-russia-forge-cybersecurity-pact/d/d-id/1098871>.

Moret, E. and Patryk, P. (2017), "The EU Cyber Diplomacy Toolbox: towards a Cyber Sanctions Regime?", *European Union Institute for Security Studies*, July 2017, [Online: web], Accessed 20 October 2018, URL: <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf>.

Mundie, Craig (2014), "Privacy Pragmatism Focus on Data Use, Not Data Collection", *Foreign Affairs*, (March/April): 28-38, [Online: web], Accessed 20 December 2018, URL: <https://www.foreignaffairs.com/articles/2014-02-12/privacy-pragmatism>.

Naughton, J. (2016), "The evolution of the Internet: from military experiment to General Purpose Technology", *Journal of Cyber Policy*, 1(1): 5-28.

Navarria, Giovanni (2016), "How the Internet was born: from the ARPANET to the Internet", *The Conversation*, Melbourne, 03 November 2016.

Newman, E. (2004), "The 'New Wars' Debate: A Historical Perspective Is Needed", *Security Dialogue*, 35(2): 173-189.

Newman, H. L. (2017), "The US Gives Cyber Command the Status It Deserves", *Wired*, 19 August, [Online: web], Accessed 20 December 2018, URL: <https://www.wired.com/story/cyber-command-elevated/>.

Newman, M. (2006), "Internet Use 1990", *SASI Group*, University of Sheffield and University of Michigan, [Online: web], Accessed 20 December 2018, URL: http://www.worldmapper.org/posters/worldmapper_map335_ver5.pdf.

- Newmeyer, K. P. (2012), "Who Should Lead U.S. Cybersecurity Efforts?", *PRISM Security Studies Journal*, 3(2): 115-126.
- Nojeim, G.T. (2010), "Cybersecurity and Freedom on the Internet", *Journal of National Security Law & Policy*, 4(119): 119-137.
- Nye, J. (1974), "Multinationals: The Game and the Rules: Multinational Corporations in World Politics", *Foreign Affairs*, 53(1): 153-175.
- Nye, J. (2006), "Transformational Leadership and U.S. Grand Strategy", *Foreign Affairs*, 85(4): 139-148.
- Nye, J. (2011), "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly*, 5 (4): 18-38.
- Novosti, R. (2007), "Estonia has no Evidence of Kremlin Involvement in Cyber Attacks", 6 September, [Online: web], Accessed 05 June 2013, URL: <http://en.rian.ru/world/20070906/76959190.html>.
- Østerud, Øyvind (2011), "State formation", In Dirk Berg-Schlosser; Leonardo Morlino (eds.), *International Encyclopedia of Political Science*, UK: Sage Publications, Chapter, Vol.8.: 2507 - 2512.
- O'Rourke, C. and A. Kerr (2017), "Privacy Shields for Whom? Key Actors and Privacy Discourses on Twitter and in Newspapers", *Westminster Papers in Communication and Culture*, 12(3): 21-36.
- Parida, J. (2017), "A Stronger Data Protection Regime for a Better Digital India", *Liberal Studies*, 2(1): 95-107.
- Patrick, S.M. (2015), Obama's National Security Strategy: New Framework, Same Policies, Council on Foreign Relations, 06 February, New York, [Online: web], Accessed 20 December 2018, URL: <https://www.cfr.org/blog/obamas-national-security-strategy-new-framework-same-policies>.
- Paul, T.V. and John A. Hall (1999), *International Order and the Future of World Politics*, CUP, US.
- Piris, Jean-Claude and Giorgio M. (1998), "The Amsterdam Treaty: Overview and Institutional Aspects", *Fordham International Law Journal*, 22(6): 32-47.
- Pohle, J. and, Luciano Morganti (2012), "The Internet Corporation for Assigned Names and Numbers (ICANN): Origins, Stakes and Tensions", *Revue française d'études américaines*, 134(4): 29-46.
- Pollitt, M. M. (1998), "Cyberterrorism – fact or fancy?", *FBI Laboratory 935, Pennsylvania Ave. NW*, Washington, DC, [Online: web], Accessed 05 May 2013, URL: <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>.

Ponemon Institute (2013), “2013 Cost of Data Breach Study: Global Analysis”, *Symantec*, May 2013, [Online: web], Accessed 20 December 2018, URL: <https://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf>.

Ponemon Institute (2014), “2014 Cost of Cyber Crime Study: United States”, *Hewlett-Packard*, 09 October, 2014, [Online: web], Accessed 20 December 2018, URL: https://ssl.www8.hp.com/us/en/ssl/leadgen/document_download.html?objid=4AA5-5208ENW.

Ponemon Institute (2015), “2015 Cost of Cyber Crime Study: United States”, *Hewlett-Packard*, October 2015, [Online: web], Accessed 20 December 2018, URL: http://img.delivery.net/cm50content/hp/hosted-files/2015_US_CCC_FINAL_4.pdf.

Ponemon Institute (2017), “2017 Cost of Cyber Crime Study”, *Accenture*, [Online: web], Accessed 20 December 2018, URL: https://www.accenture.com/t20170926T072837Z__w__us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

Porteous, H. (2010), “Cybersecurity and Intelligence: The US Approach”, *Parliamentary Information and Research Service*, PRB 09-26E, 8 February, [Online: web], Accessed 20 December 2018, URL: <https://lop.parl.ca/Content/LOP/ResearchPublications/prb0926-e.pdf>.

RAND (2018), “Paul Baran and the Origins of the Internet”, RAND, US, [Online: web], Accessed 17 September, 2018, URL: <https://www.rand.org/about/history/baran.html>.

Raul, A.C. (2017), *The Privacy, Data Protection and cybersecurity Law Review*, Fourth Edition, United Kingdom: Law Business Research Ltd.

Richardson, J. (2011), “Stuxnet as Cyber-warfare Distinction and Proportionality on the Cyber Battlefield”, *The John Marshall Journal of Information Technology & Privacy Law*, 29(1): 1-28.

Rieker, P. (2007), *The EU as a Security Actor: the Development of Political and Administrative Capabilities*, Working Paper: 725, Oslo: Norwegian Institute of International Affairs.

_____ (2009), “The EU – a Capable Security Actor? Developing Administrative Capabilities”, *Journal of European Integration*, 31(6): 703-719, [Online: web], Accessed on 12 April 2017, URL: <http://dx.doi.org/10.1080/07036330903274599>.

Risse-Kappen, Thomas (1997), *Cooperation among Democracies The European Influence on U.S. Foreign Policy*, USA: Princeton University Press.

Robinson, N. (2013), "Cybersecurity Strategies Raise Hopes of International Cooperation", *RAND Review*, 37(1): 20-21 [Online: web], Accessed 30 January 2015, URL: http://www.rand.org/content/dam/rand/pubs/corporate_pubs/CP000/CP22-2013-06/RAND_CP22-2013-06.pdf.

Rosenzweig, P. (2013), *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*, The Changing Face of War James Jay Carafano, Series Editor, USA: Praeger Publishers.

Rousseau, D.L. and T.C. Walker (2010), "Liberalism", in Myrian D. Cavelti and Victor Mauer (eds.), *The Routledge Handbook of Security Studies*, London: Routledge.

Russ, K. (2008), "Cyber War I: Estonia Attacked from Russia," Published in *European Affairs* 9 (1-2) (Winter/Spring 2008), [Online: web], Accessed 05 May 2018, URL: <http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html>.

Reding, V. (2012), "The European data protection framework for the twenty-first century", *International Data Privacy Law*, 2(3): 119-129.

Renard, Thomas (2014), "The European Union: A New Security Actor?", *European University Institute, Robert Schuman Centre for Advanced Studies, Global Governance Programme*, EUI Working Paper RSCAS 2014/45, Italy, [Online: web], Accessed 17 September, 2018, URL: http://cadmus.eui.eu/bitstream/handle/1814/31267/RSCAS%202014_45.pdf?sequence=1&isAllowed=y.

Rieker, P. (2007), "The EU as a Security Actor: The development of political and administrative capabilities", *Norwegian Institute of International Affairs*, [725] Working Paper, [Online: web], Accessed 20 December 2018, URL: https://www.files.ethz.ch/isn/46168/725_EU_Security_Actor.pdf.

_____ (2009), "The EU — A Capable Security Actor? Developing Administrative Capabilities", *European Integration*, 31(6): 703-719.

Rifkin, J (2011), *The Third Industrial Revolution; How Lateral Power is Transforming Energy, the Economy, and the World*, United Kingdom: Palgrave Macmillan.

Rosenzweig, Paul (2013), *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*, USA: Paeger.

Roskin, Michael (1974), "From Pearl Harbor to Vietnam: Shifting Generational Paradigms and Foreign Policy", *Political Science Quarterly*, 89(3): 563-588.

Sandler, Todd and Justin George (2016), "Military Expenditure Trends for 1960–2014 and What They Reveal", *Global Policy*, 7(2): 174-184.

Sterling, B. (1994), *Introduction to the Hacker Crackdown: Law and Disorder on the Electronic Frontier*, [Online: web], Accessed 05 May 2013, URL: <http://ebooks.adelaide.edu.au/s/sterling/bruce/hacker/complete.html>.

Stratford, J.S. and J. Stratford (1998), “Data Protection and Privacy in the United States and Europe”, *IASSIST Quarterly*, Fall: 17-20, [Online: web], Accessed 12 February 2015, URL: <http://www.iassistdata.org/downloads/iqv01223stratford.pdf>.

Saran, S. et al. (2014), *Indo-UU Cooperation on Internet Governance and Cybersecurity*, Observer Research Foundation, New Delhi.

Sarkesian, C. Sam, et.al. (2008), *US National Security: Policymakers, Processes & Politics*, 4th Edition Lynne Rienner Publishers: USA.

Sbragia, M. A. (1993), “The European Community: A Balancing Act”, *Publius: The Journal of Federalism*, 23(3): 23–38.

Schwab, Klaus (2016), “The Fourth Industrial Revolution: what it means, how to respond”, *World Economic Forum*, 14 Jan 2016, Switzerland, [Online: web], Accessed 20 December 2018, URL: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>.

Scott, H. W. (2016), “The U.S.-China Cyber Agreement: A Good First Step”, *RAND*, California, United States, 01 August, [Online: web], Accessed 20 December 2018, URL: <https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>.

Scott, H. W. et al. (2016), “Getting to Yes with China in Cyberspace”, *RAND*, California, United States, [Online: web], Accessed 20 December 2018, URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf.

Segal, A. (2013), “The Code Not Taken: China, the United States, and the Future Of Cyber Espionage”, *Bulletin of the Atomic Scientists*, 69(5): 38-45.

Sharikov, Pavel (2013), “U.S.-Russia Relations in the Sphere of Information Security”, *Carnegie Endowment for International Peace*, 01 November, Washington D.C., [Online: web], Accessed 20 December 2018, URL: <http://carnegieendowment.org/2013/11/01/u.s.-russia-relations-in-sphere-of-information-security-pub-63163>.

Shears, M. (2014), “Snowden and the Politics of Internet Governance”, *Center for Democracy & Technology*, 21 February 2014, Washington DC, [Online: web], Accessed 20 October 2018, URL: <https://cdt.org/blog/snowden-and-the-politics-of-internet-governance/>.

Sindjoun, L. (2001), “Transformation of International Relations— between Change and Continuity: Introduction”, *International Political Science Review*, 22 (3): 219–228.

- Sjöstedt, G. (1977), *The External Role of the European Community*, London: Saxon House.
- Smith, B. (2018), “34 companies stand up for cybersecurity with a tech accord, Microsoft”, 17 April, [Online: web], Accessed 20 December 2018, URL: <https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/>.
- Smith, M. (2013), “The Myth of American Isolationism: Commerce, Diplomacy, and Military Affairs in the Early Republic”, *SPECIAL REPORT No 134, The Heritage Foundation*, Washington, DC, 9 September, [Online: web], Accessed 20 December 2018, URL: http://thf_media.s3.amazonaws.com/2013/pdf/SR134.pdf.
- Storper, M. and Richard Walker (1989), *The Capitalist Imperative: Territory, Technology and Industrial Growth*, US: Wiley-Blackwell.
- Stuart, D. (2017), “The National Security Act of 1947”, *Oxford Bibliographies*, [Online: web], Accessed 20 December 2018, URL: <http://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0102.xml>.
- Swartz, J. (2008), “Cybercriminals can’t get away with what they used to”, *US Today*, 17 November, [Online: web], Accessed 20 December 2018, URL: <http://www.usatodayeducate.com/wp-content/uploads/09-10Cyber6.pdf>.
- Solms, Rossouw von and Johan van Niekerk (2013), “From information security to cyber security”, *Computers & Security*, 38: 97-102.
- Taddicken, M. (2014), “The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure”, *Journal of Computer-Mediated Communication*, 19: 248-273.
- Tamkin, E. (2017), “10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?”, *Foreign Policy*, 27 April, [Online: web], Accessed 20 October 2018, URL: <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/>.
- Tansill, C.C. (1952), *Back Door to War: The Roosevelt Foreign Policy 1933-1941*, Chicago: Henry Regnery Company.
- Teeter, P. and Jörgen, S. (2017), “Cracking the enigma of asset bubbles with narratives”, *Strategic Organization*, 15(1): 91-99.
- Thimm, J. (2014), “Inseparable, but Not Equal Assessing U.S.–EU Relations in the Wake of the NSA Surveillance Affair”, *SWP Comments*, January, Berlin, [Online: web], Accessed 2 February 2015, URL: http://www.swp-berlin.org/fileadmin/contents/products/comments/2014C04_tmm.pdf.

Tikk, E. (2011), "Ten Rules for Cyber-security", *Survival: Global Politics and Strategy*, 53(3): 119-132.

Turhan, S.F. (2011), "The Europeanization of the Western Balkans: Is it Just a Dream?", *SETA, Brief No: 54*, June, Washington DC, [Online: web], Accessed 10 May 2018, URL: http://www.setadc.org/pdfs/SETA_Policy_Brief_No_54_Western_Balkans_Fatma_Turhan.pdf.

Theoharis, A. (1972), "Roosevelt and Truman on Yalta: The Origins of the Cold War". *Political Science Quarterly*, 87(2): 210-241.

Ullman, Richard H. (1983), "Redefining Security", *International Security*, 8(1): 129-153.

Walt, S. M. (1991), "The Renaissance of Security Studies", *International Studies Quarterly*, 35(2): 211-239.

Walters, R. (2014), "Cyber Attacks on U.S. Companies in 2014", *The Heritage Foundation*, 7 October, [Online: web], Accessed 20 December 2018, URL: http://www.heritage.org/defense/report/cyber-attacks-us-companies-2014#_ftn1.

_____ (2015), "Cyber Attacks on U.S. Companies Since November 2014", *The Heritage Foundation*, 18 November, [Online: web], Accessed 20 December 2018, URL: http://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014#_ftn1.

Waltz, K.N. (1959), *Man, the State, And War*, New York: Columbia University Press.

_____ (1964), "The Stability of a Bipolar World", *Daedalus*, 93(3): 881-909.

_____ (1979), *Theory of International Politics*, California: Addison-Wesley Publishing.

_____ (1993), "The Emerging Structure of International Politics", *International Security*, 18(2): pp. 44-79.

Weber, C. (2005), *International Relations Theory a Critical Introduction*, New York: Routledge.

Williams, M.C. (2003), "Words, Images, Enemies: Securitization and International Politics", *International Studies Quarterly* 47: 511-531.

Williams, P.D. (eds) (2008), *Security Studies an Introduction*, London: Routledge.

Wikinson, P. (2010), "Terrorism", in Myrian D. Caveltly and Victor Mauer (eds.), *The Routledge Handbook of Security Studies*, London: Routledge.

Wohlforth, W. C. (2010), "Realism and Security Studies", in Myrian D. Cavelty and Victor Mauer (eds.), *The Routledge Handbook of Security Studies*, London: Routledge.

Wei, Y. (2016), "China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty", *Henry M. Jackson School of International Studies*, 21 June, USA, [Online: web], Accessed 20 December 2018, URL: <https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/>.

Weinberg, J. (2011), "Governments, Privatization, and Privatization: ICANN and the GAC", *Michigan Telecommunications and Technology Law Review*, 18(1): 189-218.

Weiss, Charles (2005), "Science and Technology and International Relations", *Technology in Society*, 27(3): 295-313.

Weiss, M. A. and Kristin, Archick (2016), "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield", *Congressional Research Service*, 7-5700, R44257, 19 May, Washington DC, [Online: web], Accessed 17 September, 2018, URL: <https://fas.org/sgp/crs/misc/R44257.pdf>.

Wickett, X (2018), "Transatlantic Relations Converging or Diverging?", *Chatham House Report*, January 2018, Great Britain, [Online: web], Accessed 17 September, 2018, URL: <https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-18-transatlantic-relations-converging-diverging-wickett-final.pdf>.

Wieczorkowsk, J. and Przemysław Polak (2014), "Big data: Three-aspect Approach", *Online Journal of Applied Knowledge Management*, 2(2): 182-196.

Williams, M. (2017), "Data protection in the US vs Europe: what businesses need to know", *Pensar*, 29 August 2017, [Online: web], Accessed 20 October 2018, URL: <https://www.pensar.co.uk/blog/data-protection-in-the-us-vs-europe>.

Wolfers, A. (1952), "National Security as an Ambiguous Symbol", *Political Science Quarterly*, 67(4): 481-502.

Wouters, J.& Frederik Naert, (2003), "The European Union and 'September 11'", *Institute for International Law Working Paper No 40*, January 2003, Faculty of Law, K.U. Leuven, [Online: web], Accessed 20 December 2018, URL: <https://www.law.kuleuven.be/iir/nl/onderzoek/working-papers/WP40e.pdf>.

Wright, D. and Reinhard Kreissl (2013), "European responses to the Snowden revelations: A discussion Paper", *Increasing Resilience in Surveillance Societies*, December, [Online: web], Accessed 20 December 2018, URL: http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf.

Wueest, Candid (2016), "Financial threats 2015", *The Symantec*, 22 March, [Online: web], Accessed 20 December 2018, URL: <https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/financial-threats-15-en.pdf>.

Young, W.J. and J. Kent (2013), *International Relations since 1945: A Global History*, Second Edition, UK: Oxford University Press.

Zielonka, Jan (2008), "Europe as a global actor: empire by example?", *International Affairs*, 84 (3): 471-484.

Zwolski, K. (2009), "The European Union as a Security Actor: Moving Beyond the Second Pillar", *Journal of Contemporary European Research*, 5(1): 82-96.

Media and Internet Sources

Beattie, Andrew (2004), "Market Crashes: The Dotcom Crash (2000-2002)", *Investopedia*, New York City, 07 January 2004.

Bryan-Low, C. (2005), "In Eastern Europe, A Gumshoe Chases Internet Villains", *The Wall Street Journal*, US, 01 September 2005.

Bumiller E. and T. Shanker (2012), Panetta Warns of Dire Threat of Cyberattack on U.S., *The New York Times*, [Online: web], Accessed 10 January 2018, URL: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.

Burson Cohn & Wolfe (2019), "Twiplomacy Study 2018", 10 July 2018, [Online: web], Accessed 03 January 2019, URL: <https://twiplomacy.com/blog/twiplomacy-study-2018/>.

Cook, James (2014) "FBI Director: China Has Hacked Every Big US Company," *Business Insider*, New York, 06 October, 2014.

Croft, A. (2013), "EU threatens to suspend data-sharing with U.S. over spy reports", *The Reuters*, London, 5 July 2013.

Dobbs, M. (2012), "The Price of a 50-Year Myth", *The New York Times*, US, 15 October 2012.

GIP Digital Watch (2018), "UN GGE", [Online: web], Accessed 03 January 2019, URL: <https://dig.watch/processes/ungge>.

EurActiv (2013) "US data scandal deepens EU-US divide on privacy", *The EurActiv*, London, 10 June 2013.

Fidler, S. (2014), "Rise of the U.S.", 100 Years Legacies, *The Wall Street Journal*, New York City, [Online: web], Accessed 20 December 2018, URL: <http://online.wsj.com/ww1/rise-of-the-us>.

Fourkas Vassily, (N.D.), “What is ‘Cyberspace?’”, [Online: web], Accessed 05 May 2018, URL: <http://www.waccglobal.org/en/20043-communication-rights-an-unfinished-agenda/495-What-is-cyberspace.html>.

Gardner, Frank (2013), “How do terrorists communicate?”, *The BBC*, UK, 2 November 2013.

Graham, Luke (2017), “Cybercrime costs the global economy \$450 billion: CEO”, *The CNBC*, US, 7 February 2017.

Grantforward (2017), “Defense Advanced Research Projects Agency”, 22 June 2017, [Online: web], Accessed 10 June 2018, URL: <https://www.grantforward.com/sponsor/detail/defense-advanced-research-projects-agency-7166>.

HackDomian.com (2012), 2012 Cyber Attacks Statistics, [Online: web], Accessed 10 June 2018, URL: <http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/>.

Hamblen, M. (1999), “Clinton commits \$1.46B to fight Cyberterrorism”, *CNN*, Atlanta, 26 January 1999.

Helft, Miguel and C. C. Miller (2011), “1986 Privacy Law Is Outrun by the Web”, *The New York Times*, San Francisco, 9 January 2011.

Heller, N. (2017), “Estonia, the Digital Republic”, *The New Yorker*, New York City, 18 December 2017.

Hoyng, H. (2014), “WWI and America's Rise as a Superpower”, *The Spiegel*, Hamburg, 24 January 2014.

James, J. (2017), “Data Never Sleeps 5.0”, *The Domo, Inc.*, American Fork, US, 25 July 2017.

James, J. (2018), “Data Never Sleeps 6.0”, *The Domo, Inc.*, American Fork, US, 5 June 2018.

Jeong, S. (2018), “The Supreme Court fight over Microsoft’s foreign servers is over”, *The Verge*, New York City, 5 April 2018.

Krauthammer, C. (1990), “The Unipolar Moment”, *The Washington Post*, United States of America, July 20 1990.

Library of Congress (2009), “European Union Signing of Agreement on Social Networking”, 18 February, GLM, [Online: web], Accessed 20 October 2018, URL: http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205401014_text.

Landay, J. (2018), “U.S. Intel Chief Warns of Devastating Cyber Threat to U.S. Infrastructure”, *The Reuters*, London, 13 July 2018.

Levs, J. and C. E. Shoichet (2013), “Europe furious, 'shocked' by report of U.S. spying”, *The CNN*, Atlanta, 1 July 2013.

Internet Live Stats, (2018) [Online: web] Accessed on 30 June 2018, URL: <http://www.internetworldstats.com/europa.htm>.

Leyden, J. (2003), “EU Develops Cyber Crime Forensics Standards”, *The Register*, London, 27 October 2003.

Live Internet Stats (2019), [Online: web], Accessed 03 January 2019, URL: <http://www.internetlivestats.com/>.

Lohrmann, D. (2017), “The dramatic rise in hacktivism”, *TechCrunch*, Bay Area, United States, 22 February 2017.

Mala, E. and J. David Goodman (2011), “At Least 80 Dead in Norway Shooting”, *The New York Times*, New York City, 22 July 2011.

Markoff, J. and A. E. Kramer (2009), “U.S. and Russia Differ on a Treaty for Cyberspace”, *The New York Times*, San Francisco, 27 June 2009.

Marr, B. (2018), How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read, *Forbes*, US, 21 May 2018.

McDowell, M. (2013), *Security Tip (ST 04-015) Understanding Denial -of -Service attacks*, [Online: web], Accessed 05 June 2018, URL: <http://www.us-cert.gov/ncas/tips/ST04-015>.

Microsoft (2016), “A Digital Geneva Convention to Protect Cyberspace”, *Microsoft Policy Papers*, [Online: web], Accessed 20 December 2018, URL: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH>.

MIT Technology Review (2018), “France has Launched a Global Cyber Arms Pact — but the US, Russia, and China haven’t signed”, Cambridge, *MIT Technology Review*, 13 November 2018.

Moscaritolo, A. (2010), “Prison sentence for RBS hacker suspended in Russia”, *SCMacazine*, New York, 09 September 2010.

Murphy, K. (2014), “We Want Privacy, but Can’t Stop Sharing”, *The New York Times*, New York City, 4 October 2014.

Murphy, M. (2010), “Cyber War: War in the fifth domain”, *the Economist*, [Online: web], Accessed 13 February 2013, URL: <http://www.economist.com/node/16478792>.

Novinite.com (2006), “Thousands of .eu Domain Names Suspended”, 25 July, Sofia, [Online: web], Accessed 05 June 2018, URL: http://www.novinite.com/view_news.php?id=67035.

Nakashima, E. (2013), “U.S. and Russia Sign Pact to Create Communication Link on Cyber Security”, *The Washington Post*, United States of America, 17 June 2013.

Nakashima, E. and Andrea Peterson (2014), “Cybercrime and espionage costs \$445 billion annually”, *The Washington Post*, United States of America, 9 June 2014.

Nakashima, E. and William W. (2014), “U.S. Announces First Charges against Foreign Country in Connection With Cyberspying”, *The Washington Post*, United States of America, 19 May 2014.

Nielsen, N. (2013), “EU Asks for Answers on UK Snooping Programme”, *the Euobserver*, Brussels, 26 June 2013.

Nuwer, Rachel (2017), What if the Internet Stopped for a Day?, *The BBC*, UK, 7 February 2017.

Nye, J. (2011), *Cyberspace Wars*, the opinion page, the New York Times, 27, Feb, 2011, [Online: web], Accessed 05 June 2013, URL: <http://www.nytimes.com/2011/02/28/opinion/28iht-ednye28.html>.

Peterson, A. (2015) “OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times As Many As Previously Thought”, *The Washington Post*, United States of America, 23 September 2015.

Phillips, L (2011), “EU Institutions Hit by 'Major' Cyber Attack Ahead of Summit”, *Euobserver*, Brussels, 23 March 2011.

Repères (2011), “World War II Casualties”, Centre européen Robert Schuman, France, [Online: web], Accessed 17 September, 2018, URL: <http://www.centre-robert-schuman.org/userfiles/files/REPERES%20%E2%80%93%20module%201-2-0%20-%20explanatory%20notes%20%E2%80%93%20World%20War%20II%20casualties%20%E2%80%93%20EN.pdf>.

Rosen, Stephen Peter (2015), “How America Can Balance China’s Rising Power in Asia”, *The Wall Street Journal*, US, June 1 2015.

Sandvick (2016), “Why did the Congress of Vienna fail to stop future European wars?”, *dailyhistory.org*, 3 October, [Online: web], Accessed 17 September, 2018, URL: <https://dailyhistoryblog.com/2016/10/03/why-did-the-congress-of-vienna-fail-to-stop-future-european-wars/>.

Statista (2018), “Number of Cyber Security Incident Reports by Federal Agencies in the United States from FY 2006 to 2016”, [Online: web], Accessed 20 December 2018, URL: <https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/>.

Singh, Shalini (2013), “Cyber security Plan to Cover military, Govt. and Business Assets”, *The Hindu*, New Delhi, 2 July 2013.

Summers, D.J. (2014), "Fighting in the cyber trenches", *The Fortune*, the New York City, 13 October 2014.

SlidePlyer (2018), [Online: web], Accessed 03 December 2018, URL: <https://slideplayer.com/slide/10254426/>.

Symantec (2018), "Internet Security Threat Report", Symantec, Volume 23, [Online: web], Accessed 03 January 2019, URL: http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_.

Richwine, L. (2014), "Cyber attack could cost Sony studio as much as \$100 million", *The Reuters*, UK, 10 December 2014.

Roser, M. and Mohamed Nagdy (2017), "Military Spending", *OurWorldInData.org*, [Online: web], Accessed 17 September, 2018, URL: <https://ourworldindata.org/military-spending>.

Techopedia (2018), Data Packet, Techopedia, Live Internet Stats, [Online: web], Accessed 03 January 2019, URL: <https://www.techopedia.com/definition/6751/data-packet>.

TechTerms.com, (2013), "*Malware*", [Online: web], Accessed 05 April 2013, URL: <http://www.techterms.com/definition/malware>.

Times Higher Education (2003), "EU Project Develops Computer Forensic Tools to Fight Cybercrime", *THE*, 31 October, Brussels, [Online: web], Accessed 18 March 2018, URL: <http://www.timeshighereducation.co.uk/180751.article>.

The BBC (2011), "Southampton cocaine haul 'worth up to £300m'", *The BBC*, UK, 3 August 2011.

The BBC, (2006), "Thousands of EU net names frozen", *The BBC*, UK, 26 July 2006.

The Economist, (2010), "War in the fifth domain", *The Economist*, London, 1 July 2010.

The Economist (2012), "A Third Industrial Revolution", 21 April 2012, [Online: web], Accessed 17 September, 2018, URL: <http://www.economist.com/node/21552901>.

The Fortune (2018), "These 3 Countries Pose the Biggest Cyber Threats, U.S. Officials Say", *The Fortune*, the New York City, 26 July 2018.

The Guardian (2015), "What is 'safe harbour' and why did the EUCJ just declare it invalid?", *The Guardian*, London, 6 October 2015.

The Guardian, (2000), “The Rise and Rise of Microsoft”, *The Guardian*, London, 15 January 2000.

The Indian Express (2016), “India’s internet freedom on the decline: Report”, *The Indian Express*, New Delhi, 15 November 2016.

The New York Times (1999), "To Paris, U.S. Looks Like a 'Hyperpower'" *The New York Times*, San Francisco, 5 February 1999.

The Nobel Prize (2012), The Nobel Peace Prize 2012 was awarded to European Union, The Nobel Prize, [Online: web], Accessed 17 September, 2018, URL: <https://www.nobelprize.org/prizes/peace/2012/summary/>.

The Reuters (2012), “White House Lobbies for Cybersecurity Bill amid Worries It May Stall”, *The Reuters*, UK, 02 August 2012.

The Reuters (2013), “U.S. PRISM spying programme rattles EU lawmakers”, *The Reuters*, UK, 11 June 2012.

The Spiegel (2013), “Transfers from Germany Aid US Surveillance”, *The Spiegel*, Hamburg, 05 August 2013.

The Statista, (2018), Consumer loss through cyber crime worldwide in 2017, by victim country (in billion U.S. dollars), The Statista, Germany, [Online: web], Accessed 03 January 2019, URL: <https://www.statista.com/statistics/799875/countries-with-the-largest-losses-through-cybercrime/>

The Sydney Morning Herald (2007), “Estonia urges firm EU, NATO response to new form of warfare: cyber-attacks”, *The Sydney Morning Herald*, Australia, 16 May 2007.

The Wall Street Journal (2013) “Should the U.S. Adopt European-Style Data-Privacy Protections?” *The Wall Street Journal*, US, 10 March 2013.

The Wired (2012), “The Decades That Invented the Future, Part 9: 1981-1990”, 21 December, [Online: web], Accessed 17 September, 2018, URL: <https://www.wired.com/2012/12/the-decades-that-invented-the-future-part-8-1981-1990/>.

Thomas, Jo (1985), “Britain Confirms its Plan to Quit a ‘harmfully politicalized’ UNESCO”, *The New York Times*, URL - <http://www.nytimes.com/1985/12/06/world/britain-confirms-its-plan-to-quit-a-harmfully-politicalized-unesco.html>.

Tyson, Neil deGrasse (2013), “Don't Sit around Waiting for a Sputnik Moment”, Big Think, You Tube, 1 May, [Online: web], Accessed 17 September, 2018, URL: <https://www.youtube.com/watch?v=h2M3uURGW0M>.

Tzu, Sun (1913), “*The Art of War*”, Translated by Lionel Giles, [Online: web], Accessed 04 July 2018, URL: <http://www.chinapage.com/sunzi-e.html>.

Westby, J. (2016), “7 Days before Obama Gives Away Internet & National Security”, *Forbes*, New York City, 24 September 2016.

YouTube (2011), “Stuxnet *Virus*”, [Online: web], Accessed 06 October 2018, URL: <http://www.youtube.com/watch?v=SAy46DhWW8Y>.

YouTube (2019), [Online: web], Accessed 03 January 2019, URL: <https://www.youtube.com/yt/press/statistics.html>.

VeriSign, Inc (2019), “Domain Name System”, [Online: web], Accessed 03 January 2019, URL: https://www.verisign.com/en_IN/website-presence/online/domain-name-system/index.xhtml.

Zetter, K. (2016), “That Insane, \$81m Bangladesh Bank Heist? Here's What We Know”, *The Wired*, California, 17 May 2016.

Annex 1: List of Experts Interviewed and Institutions visited during the Field Work from 01 November 2016 – 19 July 2017

S.N.	Name of the Expert	Affiliation	Date	Consent*	
				YES	NO
1	Dr.Alexander Klimburg	The Hague Centre for Strategic Studies, The Hague	28.02.2017	Yes	-
2	Prof. Dr. Volker Roth	Institute of Computer Science, FU Berlin	03.03.2017	Yes	-
3	Dr. Myriam Dunn Cavelty	Center for Security Studies, ETH Zurich	13.03.2017	Yes	-
4	Dr. Roxana Radu	Geneva Internet Platform, Geneva	13.03.2017	Yes	-
5	Dr. Julia Pohle	WZB, Berlin	23.03.2017	Yes	-
6	Dr. Hannes Ebert	German Institute of Global and Area Studies, Berlin	27.04.2017	Yes	
7	Ms. Isabel Skierka	The Digital Society Institute at ESMT, Berlin	16.05.2017	Yes	
8	Mr. Mirko Hohmann	Global Public Policy Institute, Berlin	17.05.2017	Yes	-
9	Dr. Ben Wagner	SWP, Berlin	16.06.2017	Yes	-
10	Dr. Annegret Bendiek	SWP, Berlin	21.06.2017	-	No
11	Dr. Matthias Schulze	SWP, Berlin	21.06.2017	-	No
12	Dr. Ingo Peters	Center for Transnational Relations, Foreign and Security Policy, Otto-Suhr-Institute for Political Science, Freie Universität Berlin	26.06.2017	Yes	-
13	Dr Sandro Gaycken	The Digital Society Institute at ESMT, Berlin	05.07.2017	Yes	
14	Dr. Robert Scott Dewar	Center for Security Studies, ETH Zurich	07.07.2017	Yes	-
15	Mr. Ahlefeldt Johanne	PKGr, SPD, Berlin	12.07.2017	Yes	
16	Ms. Gail Kent	Facebook, UK	03.09.2017	Yes	-

*Consent release form was given to each expert before the interview, so that their name and views could be quoted in the research. However, some experts did not want to be explicitly named but were willing to share their opinion and expertise on the topic. Thus the confidentiality of the person has been maintained.