THE EUROPEAN UNION'S POLICY ON CYBER SECURITY, 2003-2012

Dissertation submitted to Jawaharlal Nehru University
in partial fulfilment of the requirements
for the award of the degree of

MASTER OF PHILOSOPHY

JAYADEV PARIDA

CENTRE FOR EUROPEAN STUDIES
SCHOOL OF INTERNARTIONAL STUDIES
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI - 110067
2013

Centre for European Studies
School of International Studies
Jawaharlal Nehru University, New Delhi-110067, India

Tel.: (O) 2670 4148, Fax: 91-11-2674 2592, 2674 1586
Email: cessisjnu@gmail.com

Date: 29.07.2013

DECLARATION

I declare that the dissertation entitled **"The European Union's Policy on Cyber security, 2003-2012"** submitted by me in partial fulfilment of the requirements of the Degree of **Master of Philosophy**, of Jawaharlal Nehru University, is my own work. This dissertation has not been previously submitted for the award of the any degree of this University or any other university.

Jayadev Parida

Mr. Jayadev Parida

CERTIFICATE

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

Prof. R.K. Jain

(Chairperson)

Chairperson
Centre for European Studies
School of International Studies
Jawaharlal Nehru University
New Delhi - 110067

Ummu Salma Bava

Prof. Ummu Salma Bava

(Supervisor)

Professor
Centre for European Studies
School of International Studies
Jawaharlal Nehru University
New Delhi - 110067

This dissertation work dedicated to,
My Grandmother, Parents, Brother, and my idol Himansu Bhusan Nayak

CONTENTS

Acknowledgements

Solitude vivifies; isolation kills. No piece of research can be undertaken in isolation. As I completed my work of dissertation first and foremost I owe my deepest gratitude to my supervisor ***Prof. Ummu Salma Bava*** *for her continuous moral support and guidance in different matters regarding my discussion of the idea of synopsis, research structure and formation of this work. Her immense patience, guidance, motivation, inspiring words and in-depth knowledge in research methodology and security studies have enlightened me exceptionally to accomplish this work. Moreover, she also thought me the value of hard work, discipline and time in life.*

I also extend my gratitude to all faculty members of the Centre for European Studies. I am thankful to staff of the Centre for European Studies (CES), JNU, and Rembrandt Library of the Centre for European Studies helped a lot to provide books specific to my research. I would also like to express my thanks to the Central Library for large online resources which helped me to complete this work.

I would also express my heartiest thanks to my grandmother, father, mother, my little star Appu, my idol and Big B Himhansu, Bhauja, Piusi, Kabi didi, Babuli bhai and Puchulu for standing with me throughout my life. This is the result of their immense support and care that I have reached so far.

I would like to extend my heartiest thanks to my friends – Beesanna, Vineet, Jogendra, Bailochan, Shashi, Dipak, Rishu, Rajnish, Tilak, Chandan, Sunny, Subrat and Arvind. I would like to express my special thanks to Deepak Bhai for his warm support in JNU. I would also like to express my thanks to Sourabh Bhaiya, Jagdish Bhaiya, Pawan Bhaiya, Priya Di, and specially Sonam Di for her help during my work. I would like thanks to my classmates for the time spent with them during the M. Phil course work .I would like to extend my heartiest gratitude to my strengths – Maa, Dugu Didi, Manas, Lopa, Lilly, Anee, Chuin, Prinasi and Nirmal Bhai.

I would like to express thanks to my roommate Mandeep and specially Niraj for his cooperation, I did not feel that I am in a double seated room which helped me to undertake this research in a good environment.

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

Jayadev Parida

List of Tables and Figures

Tables Page Nos.

Figures

List of Acronyms

APT- Advanced Persistence Threat

B2C- Business to Consumer

BiZ- Bosnia and Herzegovina

C*CAT- Cyber-Crime Advisory Tool

CAGR- Compounded Annual Growth rate

CEES- Central Eastern European States

CEO- Chief Executive Officer

CERT- Computer Emergency Response Team

CI- Critical Infrastructure

CII- Critical Information Infrastructure

CIIP- Communication on Critical Information Infrastructure Protection

CSFP- Common Security Foreign Policy

CSSG- Cyber Security Strategy for Germany

CSSSUK- Cyber Security Strategy of United Kingdom

CTOSE- The EU Cyber Tools On-Line Search for Evidence

DDoS- Distributed Denial of Service

DNS- Domain Name System

DoSA- Denial of Service Attack

DRC- Democratic Republic of Congo

DSCI- Data Security Council of India

EC- European Commission

EC- European Community

EC3- European Cybercrime Centre

ECSC- European Coal and Steel Community

ECSM- European Cyber Security Month

ECSS- Estonia Cyber Security Strategy

ECU- European Currency Unit

EFTA- European Free Trade Area

ENISA- European Network and Information Security Agency

ENP- European Neighbourhood Policy

EP- European Parialment

EP3R- European Public-Private Partnership for Resilience

EPC- European Political Community

ESDP- European Security and Defence Policy

ESS- European Security Strategy

EU- European Union

EUCTS- European Union Counter Terrorism Strategy

EUMS- European Union Member States

EURid- European Registry for Internet Domains

EUROPOL- European Police Office

EWI- East West Institute

FWPDNC- The French White Paper on Defence and National Security

G8- Group of Eight

Gen. – General

HTTP- Hypertext Transfer Protocol

ICT- Information and Communications Technology

IMPACT- International Multilateral Partnership Against Cyber Threats

IP address- Internet protocol address

IP- Internet protocol

IPE- International Political Economy

IR- International Relations

IS – International Security

ISDSS- Information Systems Defence and Security Strategy of France

IT- Information Technology

ITU- International Telecommunications Union

JHA- Justice and Home Affairs

JRC- The European Commission's Joint Research Centre

MAT- Mobile Assistance Team

MS- Member States

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

NTS- Non-traditional Security

NTT- Non-traditional Threats

OECD- Organisation for Economic Co-operation and Development

P3R- Prevent Protect Pursue and Respond

PC- Personal Computer

PCS- Personal Communications Services

PPP/P3- Public Private Partnership

SCADA- Supervisory Control and Data Acquisition

SGDSN- General Secretariat for Defence and National Security

SID- Safer Internet Day

SIP- Safer Internet Programme

UKNSS- United Kingdom National Security Strategy

UN- United Nations

UNESCO- United Nations Educational Scientific and Cultural Organisation

UNODC- United Nation Office on Drugs and Crimes

US/USA- United States/ United States of America

USB- Universal Serial Bus

USNSS- United States National Security Strategy

USSR- Union of Soviet Socialist Republics

WMD – Weapons of Mass Destruction

WWW- World Wide Web

XML- Extensible Markup Language

Preface

The dramatic impact of the 9/11 events has shown us the fatal nature of non traditional threats in the beginning of the 21st century. This incident made two things clear: first, the rise of new threats and subsequent complexities on international security realm and second, the scientific technological output out-passes the traditional attributes of geography as a factor in international security. In the realm of digital age both the internet and cyberspace have emerged as the prime means of communication and at the same time a new domain for the activities of the non-state actors.

The synergy between the internet and computer technologies and more broadly the Cyberspace has been emerging as a new area in the field of international security. *Glocalisation* of cyberspace which is shaping and reshaping with time has tremendously impacted our everyday life and equally on the socio-economic-cultural and political sphere.

The present geopolitical scenario is becoming more complicated. The domain of cyberspace is complex, in which identity theft is a reality. Millions of people are entering into it with billions of issues daily. The area of cyberspace is getting vulnerable due to its illegal use, reason behind that its access has become so economical. Identity theft is just the tip of the iceberg. The real threat to cyberspace comes from, such as cyber-crimes, cyber-war, cyber-terror, cyber-espionage. Securing cyberspace has become a much need element for individual well-being as well as for the nation security.

The EU has been putting in enormous efforts to tackle NTT/NTS (non-traditional threats/non-traditional security) at the global level through a multilateral approach. This has justified its role as a prominent actor in the security landscape since 2003 in the field of unconventional security in general and cyber-security in particular. The European Union's adoption of the European Security Strategy in 2003 made it more active in the field of security and crisis management. The EU has identified five major non-traditional threats, such as *terrorism, organised crime, state failure, weapons of mass destruction and climate change* in the ESS 2003. The EU became more resilient towards cyber security after the Estonia cyber-attack.

The Union has drawn the attention towards the criticality of the cyberspace in a more vigilant and lucid manner. In 2008, the review of ESS included cybersecurity as a major threat in the globalised world. 2009 onwards, the Commission has started to protect Europe from cyberattacks and disruptions actively. In November 2011, for the first time, a transatlantic cooperation came in place to accelerate their cybersecurity exercise and the Commission strengthened the European Public Private Partnerships for Resilience in 2012. The Commission (2012) emphases that the "cyber-security is a priority for Europe's welfare and competitiveness" not only developing societies but also the developed societies of the Europe have to control the proliferation of cyber threats before becoming more vulnerable.

The entire research is presented in four chapters. Chapter one deals with the introductory part of the research. It deals with the difference between traditional and non-traditional threats to security in the context of the Cold War and post-Cold War. It will also look at the emergence of the EU as a security actor. Simultaneously, it will analyse *security issues in Europe* during Cold War and post-Cold War.

Chapter two addresses the cyber security issue which is seen as a new emerging threat to international security. It will focus on the discourse of non-traditional threats in the post 9/11 period and the emergence of cyberspace in international relations.

Chapter three deals with the European Union's Approach to Cyber Security is the prime focus of this study and it will analyse approach since 2003-2012. Then chapter give a detailed analyse and evaluate of the EU's mechanism, policies and programmes to tackle the issues like cyber security, freedom of expression, and privacy. Chapter four evaluate the success of the EU policy on cyber-security.

CHAPTER 1

INTRODUCTION

> "(Together, these) world-constructing ideas have created an imperfect present and a future tense with danger. Poverty, oppression, war, misery, death, and disease are the everyday realities of life across swathes of humanity; then add fear, and stir. Debilitating and determining insecurity seem to be in permanent season, and *you and I, him and her, and us and them* will never be what we might become as long as human society, globally, is imprisoned by the regressive ideas that sustain world insecurity. [As you read this book, look forward in anger, but *keep thinking*]" Ken Booth (2007: 11-12).

Background

The geopolitics of the 20th century has undergone many critical changes. On the one hand industrial growth and scientific revolution have paved the way for major economic developments and on the other hand, the rise of nationalism in the first half of the 20th century brought major destruction. In fact, the European landmass had experienced both the positive and negative aspects of the 20th century. Indeed, the consequence of World War II had undermined the major aspects of the European states, viz. political, economic, social and cultural, and the issues of development, stability and security of the region had emerged as the main areas of concern. However, the West European leader initiative for a peace project to secure Europe from new confrontation happened when the two enemies (France and Germany) agreed upon reconciliation and friendship. The great Greek philosopher Heraclitus (500 BC) concluded that "*War is the father of all things*"; quite naturally the World War II turned out to be the father of contemporary European Union and simultaneously Cold War provided substantial inputs for the growth of institutions both horizontally and vertically. And the spill over effects of this process has restored the peace for decades in the European landscape.

But, the legacy of the World War II continued during the Cold War era, where the state was considered as the epicentre of threats, simultaneously, the notion of security had been associated with the core concept of national security (sovereignty, territorial integrity, and independence). During the Cold War, the Westphalian notion of security prevailed from East to West Europe. The end of the Cold War led to a paradigm shift in which the location of threat shifted from traditional to non-traditional threats or to non-military dimensions of security. The peace of the European landmass again came under scrutiny as new threats have emerged in Europe. Perhaps, defusing of the traditional security framework, on the other way round diffuses the core and periphery of the security into new dimensions viz. Civil War, Ethnic Violence, Terrorism and destabilisation in domestic domain.

However, the realm of military security has been diluted by the emphasis on human security in the Post-Cold War period. On the one hand the Balkan conflict and breakup of Yugoslavia following the civil crisis viz. Slovenia (1991), Croatia (1992-1993), Bosnia (1992-1995), Kosovo (1999) brought war back to Europe. On the other hand a decade after the end of the Cold war the landscape of threats became intangible and more vulnerable with the critical blow of 9/11. The major terrorist attack in 2001 in the US has forced the whole world to examine emerging threats like terrorism and organised crime. As far as the volatile nature of non-traditional threats is concerned, it has been significantly impacted through two things viz. newly technologies (Computer and Internet) and scientific development along with it, the non-state actors have been continuously targeting the medium of communication to achieve their goals. In fact, the non-traditional threats have become more acute are proving to be more risk to security of the state and of the people. In the realm of digital age both the internet and cyberspace have emerged as the prime means of communication and at the same time a new domain for the activities of the non-state actors.

This chapter examines the difference between traditional and non-traditional threats to security in the context of the Cold War and post-Cold War. It will also look at the emergence of the EU as a security actor. Simultaneously, it will analyse *security issues in Europe* during Cold War and post-Cold War. The much talked about cyber security which is seen as a new emerging threat to international security will be analysed in chapter two. It will focus on the discourse of non-traditional threats in the post 9/11 period and the emergence of cyberspace in international relations. The European Union's Approach to Cyber Security is the prime focus of this study and it will analyse approach since 2003-2012. The study will also analyse and evaluate the EU's mechanism, policies and programmes to tackle the issues like cyber security, freedom of expression, and privacy. The last chapter will evaluate the success of the EU policy on cyber-security.

1.1. International Security

The paradigm of International Security (IS) has emerged from the classical scholarship of International Relations (IR).In reality, Security Studies as a subject/sub-field of IR was mostly studied after the end of World War II. Moreover, "there is an antecedent literature extending back before the second world war"[1]. Rather going into detail politics of international security, it is necessary to demystify the concept of security. Generally, the image of security has been characterised as being protected or being safe or to be secure from threats. But, indeed, "security is most commonly associated with the alleviation of threats to cherished *values*; especially those which, if left unchecked, threaten to particular referent in the near future. To be clear, although security and survival are often related, they are not synonymous. Whereas survival is an existential condition, security involves the ability to pursue cherished political and social ambitions" (Williams 2008: 5). In fact, in simple terms, security implies freedom from threats and protection of the core values of both human beings and nation-state, security whether it is only security of the state or security of individual or a comprehensive approach which will ensure both the realm, along with other issues. However, the discourse of International security has been mainly and largely divided into two categories viz. Traditional security and Non-traditional security.

From the very first Nation state till now, human race has fought many wars. Although the post Cold War scholars have defined *war* mainly into two categories 'Old war and New war' (Kaldor 2007), whether it is new or old does not matter because untold miseries and human sufferings is the outcome of most wars.

The geostrategic and geopolitical shift in the 20th century has brought focus to three major wars viz. the World War I, the World War II and the Cold War, along with the New Wars (the Balkan Wars in Europe, Civil Wars Ethnic violence and genocide in Africa and Asia) which shift the paradigm of traditional threats into non-traditional security. Indeed, the traditional paradigm of security fundamentally

[1] Which can largely be characterised as war studies, military and grand strategy, and geopolitics. This includes much discussed writers such as Clausewitz, Mahan, Richardson and Haushofer, whose works still remain relevant. However, it is necessary for them to be studied in a time frame work, in this context; it is post war discourse of International Security. (Buzan and Hansen 2009)

focused on territorial (state) security, and states are considered as the prime actor in the international security realm.

1.2. Traditional Security

The discourses of traditional security have primarily been constructed by the realist school, in which they have emphasised upon the national security (sovereignty, territorial integrity and independence) and military capabilities (power to protect the self-interest). However, the intellectual tradition of realist school fundamentally evolved around one out of the many variables i.e. Human Nature. The Hobbesian philosophy has drawn the picture right in this way- human nature is egoistic, brutish, nasty, solitary, poor and they are keenly self-centred. But, the neo-realist Kenneth Waltz has defined realism in a different intellectual paradigm, fundamentally he has taken two considering points to evaluate the realm of in/security at the global level: the nature of Man (good man or bad man) and nature of the societal system i.e. State (good society or bad society). However, through these two assumptions the essence has been drawn, that if both of the nature is positive or only nature of the society is positive, then only the international system (i.e. the third assumption) could work smoothly, otherwise it will lead to 'anarchy' rather than hierarchy.

1.2(a) Realism and International Security

Politics among Nations, power, self-interest and anarchy that is the primary cause of insecurity. There are some new sub-schools of realism that have come up in the landscape of security studies, viz. neo-realism, neo-classical realism, offensive realism, defensive realism, structural realism. But, indeed, all these sub- schools are interlinked with the core scholarship of realist school, as put forwarded by Kenneth Waltz i.e. Man, the State, and the System (international system), similarly the central point of security has been on the role of the state and that the state will ensure the security of other two (Man and International System).

William Wohlforth, has categorised the Realist paradigm into three major sub-sets: '*Groupism, Egoism, and Power-centrism*'[2]. In fact, "realism's most important

[2] Groupism- politics takes place within and between groups. Group solidarity is essential to domestic politics and conflict and cooperation between polities is the essence of international politics. To survive at anything above a subsistence level, people need the cohesion provided by the group solidarity, yet that very same group cohesion generates that potential for conflict with other groups. Today, the most

single argument builds on these assumptions to illuminate a relationship between *political order and security.* If human affairs are indeed characterized by *groupism, egoism and power-centrism,* then politics is likely to be conflictual unless there is some *central authority* to *enforce order.* When no authority exists that can enforce agreements - *in a state of anarchy* – then any actor can resort to force to get what they want. Even if an actor can be fairly sure that no other will take up arms today, there is no guarantee against the possibility that one might so tomorrow. Because no actor can rule out this prospect, all then arm themselves against this contingency. With all if actors could rely on some higher authority to enforce an agreement that can escalate to war in the absence of such authority. The signature realist argument is therefore that *anarchy renders security problematic, potentially conflictual and is a key underlying cause of war*" (Wohlforth 2010: 10). Indeed, the 'struggle for power' in international security landscape has created an anarchical structure and the outcome is insecurity and instability. Likewise, most of the realist thinkers have agreement upon the correlation between power and capabilities which escalates into conflict between or among states. Though 'insecurity is endemic to anarchy' (Cavelty and Mauer 2010: 10), therefore, the structural realist have argued that, a structure is needed to ensure security, which was present during the Cold War i.e. balance of power structure. It follows from that the breakout of the two major World Wars was because there were no balancers, lack of central authority and no order in the system. From the point of Waltz it is clear that, the nature of Man, the State and the System are the prime reasons for the escalation of conflict at the international/global level. The proliferation of war is primarily linked with the core i.e. fear of others, we and they, us and them, indeed, this type paradox along with fear of neighbours, self-interest and *bandwagoning of power* makes things more *conflictual.*

important human groups are nation-states, and the most important source of in-group cohesion is nationalism. Egoism- when individual and group act politically, they are driven principally by narrow self-interest. Although certain conditions can facilitate altruistic behavior, egoism is rooted in human nature. When push comes to shove, and ultimate trade-offs between collective and self-interest must be confronted, egoism tends to trump altruism. Power-centrism- human affairs are always marked by greater inequalities of power in both senses: social influence or control (control over politics) and resources (control over material power). (Cavelty and Mauer 2010)

1.2(b) Liberalism and International Security

In contrast to the realist paradigm, the liberal school, but it has evolved since the First World War. Liberalism dates back to the philosophers Immanuel Kant, Thomas Paine and Woodrow Wilson, who have emphasised upon democracy, peace, constitutional government, open diplomacy. Moreover, Kant's theory of 'Perpetual Peace' and the Fourteen Points of Wilson are some of the well-known scholarship of liberalism. The liberal paradigm has three major hypotheses regarding the system viz. *Democracy, Economic interdependence and International institutions reduce military conflict* (Cavelty and V. Mauer 2010: 26-29).

The liberalists have analysed the security landscape through the realist scholarship (Human nature, nature of the State and international system), moreover, this discourse between two schools has been termed as the 'great debate' in international relations. 'Liberalism is an expansive concept that carries a verity of meaning...'(Cavelty and Mauer 2010: 21), in fact, 'for Doyle, liberalism resembles a family portrait of principles and institutions, recognised by certain characteristics – for example, individual freedom, political participation, private property, and equality of opportunity'(Cavelty and Mauer 2010: 21).

Liberalism have often emphasised the power of human reason and action in which progress, individual liberty, freedom of expression and a peaceful world can be achieved. Liberal scholars have argued that progress is possible; it can be achieved, though it is neither inevitable nor easy.

Human Nature - On the one hand, in *Rights of Man*, Thomas Paine has argued about the 'morning of reason'[3]. Here he has given much emphasis on the relations between the individual and government, but on the other hand Immanuel Kant argued in a different fashion i.e. 'unknown proportions'[4]. In this regard Kant was optimistic about the human reason and the ability to overcome from flux. However, again Kant argued that, to be a good citizen, one has to be good morally

[3] T. Paine 'democratic revolutions would free mankind from [these] corrupting influences and human reason would emerge quickly to transform the world'. (Cavelty and Mauer 2010)

[4] I. Kant has defined human nature as 'mixture of evil and goodness in unknown proportions'. (Cavelty and Mauer 2010)

and the goodness in reason will not come simply, because it needs trails, practice, and instruction to move from one stage to the next.

The State – the liberal paradigm has been literally based upon the democratic peace theory and according to this theory, democratic countries prefer peace rather than war. Paine and Kant both agree that the democratic state may behave more peacefully, e.g. 'Holland and Switzerland [sic] are without wars, foreign and domestic' (Rousseau and Walker 2010: 23). Adding to this, Paine has talked about the tendency of democratic state to 'negotiate the mistake' (Cavelty and V. Mauer 2010: 23). Moreover Kant and Paine have argued that the democracies will spend less money on military expenditure rather than authoritarian regimes, in contrary liberal capitalist country like the US has given emphasis on industrial power for economic growth and national security. Thus, it can be said that the liberal paradigm primarily focuses on the nature of the state and the regimes, which will determine the nature of the system. However, the paradox of democracies is contrary to the view, because at present many democratic countries are allocating higher budgets for military expenditures than other sectors. Indeed, the liberal paradigm has talked about arms reduction, because if a state is well equipped with arms and armaments first it will create a *sphere of suspicion* with the neighbours, second any regime change may lead to proliferation of conflict. Thus, to avoid conflicts states have to control its expenditure and production of militaries.

The System – At systemic level the liberal paradigm has examined the relations between the states and the system i.e. how state interacts with other states in the global/ international level. Moreover, at the system level, liberalists have given much emphasis on trade and economic interdependence. For Paine and Kant it is '*cordialize* mankind and pacific system' (Cavelty and Mauer 2010: 24). Nevertheless, 'trade not only produces wealth, but also reduces conflict by promoting understanding and unveiling the harmony of interests between nations' (Cavelty and Mauer 2010: 24). Unlike other relations trade may possibly lead to peace because 'the *spirit of commerce* sooner or later takes hold on people, and it cannot exist side by side with war' (Cavelty and Mauer 2010: 24) and 'financial power and business interests would reduce war throughout the world' (Cavelty and Mauer 2010: 24). However, though both the schools have a different interpretation of state role, but still they agree upon a common point, 'power and interests'. For realists, power lies on military aspects and interest is mainly linked with national interest, but for liberals, power is mainly linked with finance, economy, trade and interest is business interests

Not only the realists or liberals have talked about security at the global level, there are also many sub-schools of both the paradigms, but the new emerging theoretical idea in international relations have been criticising the old paradigms (realist and liberal) for their one-sided approach towards security, and simultaneously analysing the security aspects in a broader framework. The 'widening and deepening' (Buzan and Hansen 2009: 187) process of security landscape in international realm, has created a new paradigm within the security studies i.e. Non-traditional security.

1.3. Non-traditional Security

Non-traditional threats or unconventional security aspects primarily are the outcome of the post -Westphalia society. Indeed, the twilight of the Cold War brought back a new area into the security discourses. The rise of the critical school and its sub-branches has deconstructed the core concept of security. Literally speaking, a paradigm shift has taken place from national security to human security. 'Human security', has come into the discourses especially by the post-Cold War scholars. However, the prime concern of this scholarship is to create awareness among the global citizens regarding the new vulnerabilities.

Although, realism and liberalism have been engaged with criticising each other, but during this debate, the scholarships of Keohane and Nye have come up with a structural analysis of the international system. In "*Power and Interdependence*" they have focused on non-traditional marketplace. 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 tackle the threats due to uneven nature within it. A single method could not shutout the problems, because the social systems of present society are facing "different issues, different coalitions, (with) different degrees of conflict" (Keohane and Nye 2001: 20).

The 20th century was full of different security challenges and according to J. Mearsheimer 'great powers that shape the international system and fear each other and compete for power' (Mearsheimer 2001) which results in conflicts/wars. On the other hand, diffusion of national security into individual security has made the things more problematic- as Buzan (1983) argued, that 'it (security) is easier to apply to things than to people'. On the other hand the nature of the threats and its degree of impact varies from region to region, from one individual to the other.

'Security is about the identification of *threats* to a particular *referent*, and the formulation of policy responses to those *threats*' (Cavelty and Mauer 2010: 48). It is much easier for the traditionalist scholars to accept it, but when the concept of security is at the crossroads, this particular reference would not be applicable to identify the threats. Certainly, the metaphor of security in the Post-Cold War period has changed.

The end of the Cold War has shown the triumph of capitalist liberal force over others. The illusion of the '*end of history*' as enunciated by Francis Fukuyama (1992) did not last long, because the dawn of the 21st century displayed new problems and threats.

Although, the language has changed along with the perception, but question of security remain unchanged. The rise of new paradigms in international theory landscape changed the approaches of study viz. the English School, the Critical School the Copenhagen School. On the other hand, the international system has shifted into newer discourse viz. '*Core, Periphery, and Semi-periphery*' (Buzan 1991: 432), in which, the core implies the dominant capitalist countries and the periphery are the others (industrially, politically, economically weaker states), and the semi-periphery is situated between these two i.e. the countries mainly trying to join the upper club. Similarly, the world is perceived differently, the issues are different, thus it is necessary to study the realm of security from a different angle.

The landscape of security has changed, it is no more purely state oriented, with end of the Cold War and new influx which have arisen can categorised in 'five sectors of security: *political, military, economic, societal and environmental*' (Buzan 1991: 433).

> "**Military security** concerned with the two-level interplay of the *armed offensive* and *defensive* capabilities of states, and states' perceptions of each other's *intentions*. **Political security** concerned with the *organizational stability of states*, *systems of government*, and the ideologies that give them *legitimacy*. **Economic security** concerned with the *access to the resources, finance and markets necessary to sustain acceptable levels of welfare and state power*. **Societal security** concerned with the *ability of societies to reproduce their traditional patterns of language, culture, association, and religious and national identity and custom within acceptable conditions for evolution*. **Environmental security** concerned with the *maintenance of local and the planetary biosphere as well as the essential support system on which all other human enterprises depend.* 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).

Within a short span of time, global geopolitics and geostrategic(s) have faced two major incidents- '11/9 (1989) and 9/11 (2001)' (Booth 2007: 2). Issues such as climate change, terrorism, civil wars, ethnic violence, political instability, cyber-threats have emerged as new threats now. In a digital age new attacks could be carried out by the non-state actors. Undeniably the incremental assimilation of terrorist groups in the cyberspace is increasing day by day, the reason is that '*who have not travelled overseas to meet terrorist leaders and other militants were able to resort to the internet, a transnational medium of communication that provides an alternative and highly accessible source of foreign influence*'(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, growing infiltration into the cyberspace has been making state and human security more vulnerable.

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 two decades back, but has now come into prominence in the 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 sector have to cooperate in addressing this new threat. Above all, international organisations along with non-sate actors have to work actively in this field because cyberspace is a difficult aspect to put under the jurisdiction of the international law and simultaneously it is free and open place to assemble. However, at present most of the countries have their own policies on cyberspace e.g. South Korea has a heavily censored internet policy.

1.4. Security Dynamism in Europe

"War is the father of all, king of all. Some it makes gods, some it makes men, some it makes slaves, some free." (Heraclitus 500 B.C.)

The European Union is the unique outcome of war; indeed underscores statement of Heraclitus. During the Cold War, ideologically and geopolitically the world was divided into two parts. The European landmass was thinking in a different way to tackle the questions of Peace, development, and containment of Germany. Indeed, two major events have played significant role to achieve this: the reconciliation between France and Germany and the Trans-Atlantic collective defense mechanism (i.e. NATO 1949), simultaneously the West Europeans made all efforts to bring peace back to the Europe. The 'widening and deepening' process of the EU 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.

The European Union's adoption of the European Security Strategy in 2003 made it more active in the field of security and crisis management. However, this also leads to many questions arising on the nature of the EU and the kind of actor it is. The reason behind all such questions is the divergence of security mechanism within the EU on the one hand and NATO's role within Europe on the other hand.

The Aftermath of the World War II had left Europe in terrible condition: the economy had collapsed in many countries (Germany, Italy, France, Eastern Europe and USSR), 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, Marshall Plan as given by the US helped the European reconstruction.

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 nation-states did not engage in any kind of direct war. The end of Cold War brought war back to the heartland.

1.5. The European Union as a Security Actor

> "*Domestic factors* also affect the likelihood of war, and have helped the post-war peace. Most importantly, hyper-nationalism helped the two world wars and the *decline of nationalism in Europe* since 1945 has contributed to the peacefulness of the post-war world" (Mearsheimer 1990: 12)

The last decade of the 20th century has shown pragmatic changes in the security dimension of the European Union and role of its '*actorness*' (Greicevci 2011). The St.Malo summit in 1998 has reshaped the European Union's stand in the global politics, in that summit particularly the British Prime Minister Tony Blair emphasised upon the EU's role in Foreign policy and Security mechanism. Nevertheless, certain conditions have to fulfil to become an actor, thus, the question is, how the European Union is conceptualised as a security actor, it is not a state nor having any sovereignty, rather is it a unique organisation in which 28 countries have given delegated their in different areas power to a mutual authority.

The end of the Cold War and rise of the Balkan Crisis similarly the fall of communism in Central and Eastern Europe and disintegration of USSR have also forced the European's to create their 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.

In fact, the EU first devised a mechanism for ensuring security, developed decision making procedures, and created an institutionalisation security domain. It continued to increase its stake in European security be extending an area of freedom, security 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 Union develops at three levels: an institutionalised security domain (i.e. the CFSP); an 'external anchor' for the periphery (i.e. ENP); and direct military capacity (i.e. ESDP).

> "For instance, ... during the Cold War period, the European Community (EC) abstained from developing any common policies towards its Northern and Eastern periphery owing to the constraints imposed by the bipolarity of the world system. In fact, the 'neutrality' of the European Community in terms of foreign policy lasted more or less until 1992. Then, ... by trumpeting a new Common Foreign and Security Policy (CFSP) for the EU in the Maastricht Treaty (1993), the EU raised expectations for a collective diplomacy. Moreover, in December 1998, France and the United Kingdom released a joint declaration at St. Malo calling for the EU to possess the power of autonomous action and the appropriate military resources, a ground-breaking step forward .... Consequently, this kind of philosophy followed the decision of the Cologne European Council in June 1999 to develop the European Security and Defence Policy as a part of the Common Foreign and Security Policy. In other words, ... the member states decided in Cologne that the Union must have the capacity for autonomous action backed up by credible military force, . . . and the readiness to act in order to respond to international crises" (Greicevci 2011: 284).

Gunner Sjostedt defined actor capability as a 'capacity to behave actively and deliberately in relation to other actors in international system' (Sjostedt 1997: 16). He viewed this capacity primarily as a function of internal resources and internal cohesion. However, Bretherton and Vogler have argued that actorness is constructed through the interplay of both internal and external factors (Bretherton and Vogler 2006:2). According to Reiker (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: first *rights and authorities* – rights and authorities are the capabilities that are supposed be enshrined in formal rules. Second *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. Third type of capacity is *competencies and knowledge* on the part of individuals, professions and institutions. Finally, *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. As March and Olsen argue, '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 emphasis sovereignty or the separation of domestic and foreign affairs. The European Union has become a highly develop 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, we expect to find these capabilities exist, that they are of a certain size and that they increase over time' (Reiker 2009: 703). According to Reiker (2007: 11), "if the EU is indeed a security actor, we would except 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". After examining various policy measures and some empirical data, Reiker posits his argument. First, that the EU has developed a set of formal rights, institutions and rules to regulate this policy area, and that these have increased over time. Second, with the regard to resources (budget, staff and equipment), the overall conclusion is that the EU has limited but increasing resources in this sphere.

The terrorist attack in 2001 on the USA made a drastic change in the geostrategic aspects of non-traditional threats. In fact, to tackle such type of critical occurrences, the USA has come with a new strategy which is the National Security Strategy (NSS), which is emphasises unilateralism, hard power politics and 'pre-emption' (always a part of the US foreign policy). On the other hand, the EU has come with own strategy: the European Security Strategy (ESS 2003) which is based on multilateralism and collective approach to non-traditional threats. It rightly documents that in a globalised world a single state won't be able to tackle the threats alone due to the vagueness and unidentified nature of such a threat, similarly, emergence of new threats (cyber threats) bring more vulnerability to everybody.

1.6. The European Union and Cyber security

Decline of Nationalism - the positive decline of nationalism created a *Sui generis* organisation, whose prime motto is mutual cooperation and common understanding between the members. Both the factors have been playing a significant role to reshape the images of the EU. Unlike the US, the European Union is an emerging security actor which is aiming to address the new security threats. Second, the magnitude of non-traditional threats is unpredictable. The EU has identified five major non-traditional threats, such as terrorism, organised crime, state failure, weapons of mass destruction and climate change in the ESS 2003. Prior to this document there was no such composite policy or document that had cited the non-traditional threats.

The 2008 review of the Security Strategy the European Union brought focus to new threats i.e. Cyber-threats. Cyber-security is also interlinked with the privacy, freedom of expression and the security of critical infrastructure. In 2001, the Council of Europe convention on cyber-crime emphasised the criticality of the cyberspace. Since 2003, incremental growth has taken place in the EU paradigm which shows the ability and capability of an actor in security landscape. But the whole world in general and Europe in particular experienced the vulnerability when anonymous Russian hackers attacked the Estonian Government websites in 2007 continuously for three weeks. The EU has created an agency to fight against cyber-crimes and to strive for Information security in 2004 called the European Network and Information Security Agency (ENISA fully established since September 1, 2005). Recently, 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 cyber-security".

Nonetheless, in virtual world such problems are just like the tip of the iceberg. State and non-sate actors thus have to think and work through a pragmatic approach. In similar way cooperative and composite approach is required by the EU to being an actor in cyber security.

CHAPTER 2

CYBERSPACE AND INTERNATIONL RELATIONS

"Technology is neither good nor evil, nor is it neutral" (Kranzberg's first law of technology 2011).

2.1. Introduction

The dimensions of international politics have changed drastically during the 19th century. The industrial transformation and revolution in the mode of production released huge amounts of new *resources* into the international system. These resources can be viewed as affecting the various aspects of human life, viz. political, social, economic, cultural and ideological. Perhaps, this transformation changed the thinking process of human beings to a great extent which resulted into the rise of 'liberalism, nationalism, racism, scientific-racism, idea of progress, socialism and the counterpoints to liberalism and capitalism' (Buzan 2011). Further, Buzan (2011) has argued that in the 19th century many new phenomena, like nation-sate (state was there for longer time), intergovernmental organisation, international civil society, *international organised non-state entity,* modern cooperation etc came into being. These technocratic revolutions in the socio-economic field encouraged the new process of power accumulation by the nation-states. In the 20th century these industrially modernised powers wanted to get hold of the central position on the one hand and on the other hand nationalism and racism started to make their presence felt more strongly than ever. By the middle of the century, the fear of wars were cleared, but that happened at the cost of 'uneven distribution of power, centralised form power (i.e. [west oriented] military power, economic power, social power, resources and ideas) and huge centralised development in greater inequality' (Buzan 2011). The end of the Cold War transformed geopolitics into a multipolar capitalist structure: rightly argued by Buzan (2011) that we (states) all are capitalist with different connotations as well as in orientations, viz. for the US it is liberal capitalism, for Europe social market capitalism and authoritarian capitalism in Russia and China. In fact, the rise of the new capitalist structure brought more trouble into the society. Buzan (2011) argued that modernity and industrial power has given huge ability to both state and non-state actors to foment trouble. This has become much more diffuse with time:

now however, even *individuals* can command considerable powers of destruction and *small- groups* can do so as well. This is going to be a great change in the political equation which is a *challenge for the states/global society.*

The technological development in the 20th century has brought two new products i.e. the internet and the computer into everyday life and these scientific revolutions have created a new public domain i.e. 'cyberspace'. At present with the advancement of the sophisticated technologies cyberspace is becoming more vulnerable with the progress of time. Cyberspace has been frequently targeted by non-state actors to fulfil their ends. Not only the non-state actors but also individuals and to some extent governments have joined hands to attack states/institutions. These kinds of threats to cyberspace raises the question of its safety and security. The realm of cyber-threats is new but it has as bad an impact as conventional threats do because "*cyber-threats* and other challenges of the *information revolution* [...] and [...] trend of *globalisation*, which ... *weakens the sovereignty and security of the state*" (Eriksson and Giacomello 2006, 2007: 16). Thus, it has become necessary to tackle these unseen threats largely dominating the geopolitics in the post- 9/11 security landscape hidden behind the screens.

2.2. Post 9/11 security discourses

The dramatic impact of the 9/11 events has shown us the fatal nature of non-traditional threats in the beginning of the 21st century. This incident made two things clear: first, the rise of new threats and subsequent complexities on international security realm and second, the scientific technological output out-passes the traditional attributes of geography as a factor in international security. U.S. President Gorge W. Bush said (2003) "the attacks of September the 11th showed our country that vast oceans no longer protect us from danger". In fact, newly invented technologies (i.e. internet and computer) have devalued the strategic location of a state. Simultaneously, the diffusion of modern technologies has brought into focus the role of individuals and smaller groups in the security landscape.

> "[Some commentators in the media, some politicians and members of the public continue to use] 'terrorism' as a synonym for political violence in general, when in reality it is a special form of violence. It is a deliberate attempt by a group or by a government regime to create a climate of extreme fear to intimidate a target social group or a government or a commercial

organisation with the aim of forcing it to change its behaviour" (Cavelty and Mauer 2010: 129).

The world felt terrorism to be the gravest threat to mankind on 'that Tuesday morning 2001', even though it had been present and active prior to that incident. In fact, the post 9/11 scenario reinforced the significance of unconventional threats in the larger picture. However, except the 'war on terror', the 21st century has not experienced any major conventional war but that is just the tip of the iceberg, because on the other hand the world has been hit hard by other calamities, such as hunger, poverty, environmental degradation, natural hazardous, WMD (Weapons of Mass Destruction) pandemics, epidemic and new threats like cyber-threats, which are slowly but steadily affecting human life. In short, the post 9/11 security discourse is more widely and deeply rooted into human behaviour. Therefore, the 'emerging theoretical framework in International security paradigm' termed this discourse as 'Securitization' (Buzan, et al. 1998: 23).

2.3. Securitization

"If we do not tackle this problem[5], everything else will be irrelevant (because we will not be here or will not be free to deal with it in our own way)" (Buzan, et al. 1998: 24)

The concept of 'Securitization' has also been developed by the Copenhagen School. It has in its roots the 'synthesis of Constructivists and Classical Political Realism in its approach to international security' (Williams 2003: 512). In addition, Williams (2003: 511) argued that "the theory of 'securitization' developed by the Copenhagen School provides one of the most innovative, productive yet controversial avenues of research in contemporary security studies". However, 'the securitization concept first entered International Relations vernacular after being outlined by Ole Wæver (1995) in the mid-1990s and received its fullest treatment in the 1998 book *Security: A New Framework for Analysis*' (MacDonald 2003: 566). In fact, the development of "securitization theory has [developed] a broad and powerful research agenda of significance across the field of security [studies], constituting, in the eyes of one supportive commentator, possibly the most thorough and continuous exploration

[5] This problem refers to the existential threat which is presented (or emerging issues) in international security landscape.

of the significance and implications of a *widening security agenda* for security [studies]'' (Huysmans, 1997:186, Williams 2003: 511). The proportional development of this theory though has taken place in the Post-Cold War period, rightly after the First Gulf War (1991) and during the Balkan Crisis (1991-1999). The Post-Cold War period has shown a paradigm shift in the security landscape. Buzan's opines: 'something is designated as an international security issue because it can be argued that some issues are more important than other issues and should take absolute priority' (Buzan, 1998: 24). In fact, international security discourses can be viewed as a debate between two, i.e. 'wide versus narrow'.

> "The 'wide' versus 'narrow' debate grew out of dissatisfaction with the intense narrowing of the field of security [studies] imposed by the military and nuclear obsessions of the Cold War. This dissatisfaction was stimulated first by the rise of the economic and environmental agendas in international relations during the 1970s and 1980s and later by the rise of concerns with identity issues and transnational crime during the 1990s. The issue-driven widening eventually triggered its own reaction, creating a plea for confinement of security [studies] to issues centred on the threat or use of force" (Buzan 1998: 2).

Literally, the emergence of a new spectrum in security realm widens the horizon of security into non-military aspects, and 'that' is what Buzan (1998: 4) pointed out: issues of security have to be understood in broader perspective and it is necessary to '...keep the security agenda open to many different types of threats' and simultaneously 'securitization of those threats' that can be 'non-military as well as military' (Buzan 998: 4).

> "Security" is the move that takes politics beyond the established rules of the game and frames the issues either as a special kind of politics or as above politics. *Securitization can thus be seen as a more extreme version of politicization.* In theory, any public issue can be located on the spectrum ranging from *non-politicized* (meaning the state does not deal with it and it is not in any other way made an issue of public debate and decision) through politicized (meaning the issue is part a of public policy, requiring government decision and resources allocations, or more rarely, some other form of communal governance) to securitized (meaning the issue is presented as an existential threat requiring emergency measures and justifying actions outside the normal bounds of political procedure (Buzan 1998: 23-24).

Securitization scholarship aims to understand "who securitizes (securitizing actor), on what issues (threats), for whom (referent objects), why, with what results, and not the least, under what conditions" (Buzan 1998: 32). However, Buzan and others (1998) have also pointed out that there could be five political zones in which Securitization could take place i.e. *political, military, societal, economic and environmental.*

2.3(a) **Political Security**

"Political security concerned with the organizational stability of states, systems of government and the ideologies that give them legitimacy" (Buzan 1991: 433)

Political security is primarily interlinked with two things viz. *internal legitimacy of political unity* (which relates primarily to ideologies and other constitutive ideas and issues defining the state) and *external recognition of the state* (external legitimacy) (Buzan 1998: 144). According to Buzan (1991: 118ff) "political threats are aimed at the *organisational stability of the state*. Their purpose may range from pressuring the government on a particular policy through overthrowing the government, to fomenting *secessionism* and disrupting the political fabric of the state so as to weaken it prior to a military attack. The idea of the state, particularly its *national identity* and organisational ideology, and the institution which express it are the normal target of political threats. Since the state is an essentially political entity, political threats may be as much feared as military ones. This is particularly so if the target is a weak state" (Buzan, 1998: 142).

> "In the political sector, existential threats are traditionally defined in terms of the constituting principle- sovereignty but sometimes also ideology- of the state. Sovereignty can be existentially threatened by anything that questions recognition, legitimacy or governing authority. Among the ever more interdependent and institutionalized relations characteristic of the West (and increasingly of the international system as a whole) a variety of *supranational referent* objects are also becoming important. The European Union (EU) can be existentially threatened by events that might undo its integration process. International regimes and international society more broadly can be existentially threatened by situations that undermine the rules, norms and institutions that constitute those regimes" (Buzan1998: 22).

In short the securitization has talked about three referent objects in political security: "emerging quasi-superstates such as EU, some of the self-organised stateless societal groups and transnational movements" (Buzan 1998: 145). So far, the first argument can be viewed as a kind of pro-Westphalian notion of 'political security' and much more on the 'identity' base i.e. national identity. But, the latter two (i.e. some of the self-organised stateless societal groups and transnational movements) is significantly emerging spectrum on the security landscape. And when these type of 'objects' (the self-organised, stateless societal groups and transnational movements) entered into cyberspace they made things more vulnerable.

2.3(b) Military Security

"*Military security* is concerned with the two-level interplay of the *armed offensive* and *defensive* capabilities of states and states' perceptions of each other's *intentions*" (Buzan 1991: 433)

The military being exists as an aura in the security realm but it has been firmly institutionalised by the state in the public domain. Thus the state has a central role in military sector and vice versa. In fact, it is the government which illuminates the act on the behalf of the state, rightly pointed out by Buzan that 'political and military sectors are conceptually distinct, the partial interchange-ability of force and consent in the process of government links them together' (Buzan 1998: 52). With exception the armed forces is one of the determining factors for the national security and for international security too, but when it goes into the hands of a corrupt individual or a group (small or big) then the output creates catastrophe in the system. However, "the agenda of military security revolves largely around the states, although as is shown later that other referent objects and securitizing actors are also in play. The main exception to this rule occurs when the state itself either fails to take root or spirals into disintegration. This situation can lead to prolonged periods of primal anarchy, as is currently the case in Afghanistan and various parts of Africa, in which the *state is only a shadow and the reality are the rival warlords and gangs*" (Buzan 1998: 50).

'Military security matters arise primarily out of the *internal and external* processes'- 'internal and external' are referring to the traditional approach to national security, in which the military (i.e. army) is most commonly used for internal security (to maintain peace in domestic affairs) and external security (for war and territorial expansion), but in preset times that concept is being studied in a wider fashion, but the rise of *non-military threats to their existence, such as migrants or rival ideology* transcend the vulnerability in the global level (Buzan et al. 1998: 52). In fact, linear approach to territorial security became very wide in the Post-Cold War geopolitics. Thus, it became necessary to securitize the military sector, because, "... information revolution changes military affairs. It [which] refers to the strategic, operational and tactical consequences of the marriage of systems that collect, process, and communication information with those that apply military force, seeking to transform armed forces and war fighting by digitising the *battlespace* and adopting new doctrine and organisational forms " (Cavelty 2002: 86). In fact, "... military (security) relation [....] has its own distinctive logic and technological imperative, but it does not operate in isolation. The entire interplay of military capabilities between states is deeply conditioned by political relations. At the interstate level ... [that] is primarily about the way in which states equipped themselves to use force and how their behaviour in this regard is interpreted and responded to by other states (Buzan et al. 1998: 52).

However, military implies the capability and capacity of a state, but in the present scenario with the impact of globalisation other sector like economic capability and modernised soft skills of a state are showcasing their influence on state capability and military has become a less determining factor nowadays. On the other hand, ad hoc position of non-state actors, regime change (internal and external), *regional security complexes* (Buzan and Waever 2003) and threat provoking issues in domestic affairs never let the military agenda to go down. The Post-Cold War scenario has already experienced the rise of non-state actors using force as evidenced in Afghanistan. Likewise, in contemporary international system new sophisticated threats i.e. Cyber-threats have taken their position in the public domain. The increasing proliferation into the cyberspace has enhanced focus on issues like critical infrastructure, security of arms and arsenals, private security etc.

2.3(c) Economic Security

"*Economic security* is concerned with the *access to the resources, finance and markets necessary to sustain acceptable levels of welfare and state power*" (Buzan 1991: 433)

International political economics have been discussed by three major schools of thought: 'the *Mercantilists and neo-mercantilists, the liberals, and the socialists'* (Buzan et al. 1998: 95-96). Economic relations are the dominant determining factor both in the national and the international system. It is largely interlinked with politics and military security aspects. In the contemporary international system, due to dominance of the liberal paradigm 'discourse on economic security centres on concerns about *instability and inequality*'[6] (Buzan et al. 1998: 97).

However, economic security has heavily relied on the state's ability to maintain independent capability to mobilise its military, resources, market, information and currency. As far as securitization of the economic field is concerned only two sorts of securitizing logic can usually attempt to evaluate firms to the status of referent objects.

> "The first is local and concerns the immediate effect on individuals and towns when a firm goes under. Individuals, trade unions, city governments and local political representatives of the national government may all attempt to save the company by casting its demise in security terms. The second type of securitizing logic is national and involves the government's attitude toward the place of a firm in the state's industrial base. For example, if the government is committed to a high degree of self-reliance for military mobilization, this argument may widely cover firms as diverse as boot markers, shipyards and electronics. Here the securitizing actor may be the firm itself (pleading fie subsidies or government orders) or a trade union or local elected government official (concerned about jobs), or it may be the state acting pre-emptively in pursuit of its own sense of military security" (Buzan et al. 1998: 100).

The present digital world has been frequently targeted by '*Trojan Horses and new Robin Hoods*' that is the reason why economic sector needs to be securitized. Indian Telecom Minister Kapil Sibal (2013) has given emphasis on both cyber

[6] Instability raises questions about the relative economic decline of the U.S as a hegemon and about the domestic and international management problems arising from the increasing integration and liberalization of the world economy. Inequality raises questions domestically about the role of the state and internationally about the disadvantaged economic position of most of the Third World states (Buzan et al. 1998: 97).

security and economic security, in his opinion "cyber security is critical for economic security and any failure to ensure cyber security will lead to economic destabilisation" (The Hindu 2013: 1). Problems in the military and the political sector may not have huge geopolitical impact but in the era of 'complex interdependence' (Keohane and Nye 2001) turbulence in economic sector might pull down the growth of many states.

2.3(d) Societal Security

"Societal security is concerned with the ability of societies to reproduce their traditional patterns of language, culture, association and religious and national identity and custom within acceptable conditions for evolution" (Buzan 1991: 433)

In the field of international security (IS), societal system has a bigger role to play, though in the larger paradigm it is the state that plays the role. In short, society and state both are complementary and supplementary to each other. In the words of Buzan et al (1998) "The state and society 'of the same people' are two different things.... State is based on fixed territory and formal membership, whereas societal integration is a much varied phenomenon-possibly occurring at both smaller and larger scales and sometimes even transcending the spatial dimension altogether" (Buzan et al. 1998: 119). As far as International security is concerned 'national security has been the established key concept for the entire area of security affairs, but paradoxically, there has been little reflection on the nation as a security unit. The focus has been on the political, institutional unit-the state, and accordingly on the political and military sectors. If one zooms in on to the nation another sector enters the picture- the societal one. Societal security is closely related to, but nonetheless distinct from political security which is about the organisational stability of states, systems of government and ideologies that governments have and legitimacy of the states' (Buzan et al. 1998: 119).

Buzan et al. (1998: 119) have pointed that 'society is about identity, the self-conception of communities and of individuals identifying themselves as members of a community. These identities are distinct from, although often entangled with, the explicitly political organisations concerned with government'. Identities play the most common and most vital role in the societal system, and societal security could be understood as 'identity security' (Buzan et al. 1998: 120). Undeniably, the fabric of a state lies under the stability of the societal system because only a domestically sound country can play a significant role in the security marketplace that is the reason it needs to be securitized.

> In the social sector, as we have defined it, the referent object is large scale collective identities that can function independent of the state, such as nations and religions. Given the particular nature of this type of referent object, it is extremely difficult to established hard boundaries that differentiate existential from lesser threats. Collective identities naturally evolve and change in response to internal and external developments. Such changes may be seen as invasive or heretical and their sources pointed to as existential threats, or they may be accepted as part of the evolution of identity. Given the conservative nature of "identity", it is always possible to paint challenges and changes as threat to identity, because "we will no longer be us" no longer the way we were or the way we ought to be to be true to our "identity". Thus, whether migrants or rival identities are securitized depends upon whether the holders of the collective identity take a relatively closed-minded or a relatively open-minded view of how their identity is constituted and maintained. The abilities to maintain and reproduced a language, a set of behavioural customs, or a conception of ethnic purity can all be cast is terms of survival. (Buzan, et al. 1998: 22).

There are misunderstandings about the term societal, '*societal security and social security*'[7], both the term though look the same but the approach is different altogether. The domain of societal security is very wide in nature. Thus, one lens cannot be applicable to visualise the whole spectrum of issues. Therefore, it needs a 'different security agenda, different areas and regions' (Buzan et al. 1998: 121). Likewise, there are certain common issues which can be viewed as threats to societal security, such as '*migration*[8], *horizontal competition*[9], *vertical competition*[10] *and*

[7] First, societal security is not the same as social security. Social security is about individuals and is largely economic. Societal security is about collectives and their identity. Empirical links will often exist when the social conditions for individual's life influences processes of collective identification (Waever et al. 1993). The concept of societal security, however, refers not to this individual level and to mainly economic phenomena but to the level of collective identities and actions taken to defend such "we identities". Second, a problem with societal is that the related term society is often used to designate the wider but more vague *state population*, which may refer to a group that does not always carry an identity. In this terminology Sudanese society, for example, is that population contained by the Sudanese state but which is composed with many societal units (e.g. Arabs and black Africans). This is not our use of societal; we use societal for communities with which one identifies (Buzan et al. 1998: 120)

[8] Migration- X people are being overrun or diluted by influxes of Y people; the X community will not be what it used to be, because other will make up the population; X identity is being changed by a shift in the composition of the population (e.g. Chinese migration into Tibet, Russian migration into Estonia) (Buzan et al. 1998: 121).

[9] Horizontal competition-although it is still X people living here, they will change their ways because of the overriding cultural and linguistic influence from the neighbouring culture Y (e.g. Quebecois'

possible fourth one is depopulation[11]' (Buzan et al. 1998: 121). Some battles of societal security are fought in the hearts and minds of the individuals (Buzan et al. 1998: 122). The concepts like 'we, us and them' (Buzan et al. 1998: 123-124) have a major stake in the field of societal security. Societal security, in short, "signifies the ability of an identity community to survive... [it] has an objective and a subjective dimension. Objectively, it pertains to the preservation of societal markers i.e. language and customs; subjectively, it entails to community's survival as a locus of identification for its members" (Theiler 2010: 106). In addition Buzan et al. (1998: 124) have argued that 'media and religion' also play a vital role in the spectrum of societal security. In fact, these two are soft and can influence human being on the emotional level. However, diffuse of new technologies and use of cyberspace also signifying the importance of societal security in security landscape.

2.3(e) Environmental Security

"*Environmental security* is concerned with the *maintenance of local and the planetary biosphere as well as the essential support system on which all other human enterprises depend*" (Buzan 1991: 433)

The discourse on environmental security has manifested only since the United Nation Convention on the Human Environment in 1972 at Stockholm and scholars of environmental security have termed it as 'ultimate security' (Buzan et al. 1998: 71); 'a real security threat' (Biswas 2011: 11); 'Coming Anarchy'(Robert Kaplan's 1994) etc. The concept of environmental security basically evolved around the two basic

fear of Anglophone Canada and more generally, Canadian fears of Americanization) (Buzan et al. 1998: 121).

[10] Vertical competition- people will stop seeing themselves as X because there is either an integration project (e.g. Yugoslavia, the EU) or a secessionist "regionalist" project (e.g. Québec, Catalonia, Kurdistan) that pulls them toward either wider or narrow identities. Whereas one of these projects is centripetal and the other centrifugal, they are both instance of vertical competition in the sense that the struggle is over how wide the circles should be drawn or rather-since there are always numerous concentric circles of identity-to which to give the main emphasis (Buzan et al. 1998: 121).

[11] Depopulation- whether by plague, war, famine, natural catastrophe or policies of extermination. Depopulation threatens identity by threatening its carriers, but it is not specifically a part of the societal sector's logic of identity, except perhaps in case where extermination policies are motivated by the desire to eliminate an identity and extreme cases-such as AIDS in Uganda-where quantity turns into quality. As with unemployment and crime these are threats primarily to individuals (threats in society); only if they threaten the breakdown of society do they become societal security issues (Buzan et al. 1998: 121).

agendas: 'scientific and the political agenda'[12] (Buzan et al. 1998: 71). As far as the security of the environment is concerned, sustainability and resources management are critical issues in the context of other geopolitical issues. In fact, the understanding of the environmental security is two-fold viz. the theoretical developments of the concept of security and environmental changes and livelihood (Biswas 2011: 1). But, Dalby (2008) argued that 'the poor is hungry due to lack of food, not because of poverty…. [and] there is a clear geopolitical divide between the South (those are in direct danger of both environmentally and politically) and the North (the prosperous populations)' (Williams 2008: 262). Deudney (1999) emphasises that the "environmental threats tend to be diffused, indirect and international, originated both inside and outside of the state" (Williams 2008: 266). Unlike other threats, environmental has a long term impact on human life.

> "…the political agenda reflects the overall degree of politicization and securitization (as contrasted with private securitizing and desecuritizing moves). The two agenda overlap in the media and in public debates. Ultimately, the scientific agenda underpins securitizing moves, whereas the political agenda is about three areas: (1) state and public awareness of issues on the scientific agenda (how much of the scientific agenda is recognised by policymakers, their electorates, and their intermediaries-the press); (2) the acceptance of political responsibility for dealing with issues; and (3) the political management questions that arise: problems of international cooperation and institutionalisation in particular regime formation, the effectiveness of unilateral national initiatives, distribution of costs and benefits, free-rider dilemmas, problems of enforcement and so forth" (Buzan et al. 1998: 72).

Thus, environmental security has acquired a variety of issues within its paradigm viz. disruption of ecosystem, energy problems, population problems, food problems, economic problems and civil strife (Buzan et al. 1998: 74-75). Simultaneously, the environment covers everyone, from the 'northern elite, middle class to the Amazon Indian' (Buzan et al. 1998: 76). In fact, the impact of environmental disaster not only hampered the humankind but it also equally damaged

[12] The scientific agenda is typically embedded in the (mainly natural) sciences and nongovernmental activity. It is constructed outside the core politics, mainly by scientist and research institutions, and offers a list if environmental problems that already or potentially hamper the evolution of present civilizations. The political agenda is essentially governmental and intergovernmental. It consists of the public decision-making process and public policies that address how to deal with environmental concerns.

the other components of the ecosystem, like the animals and various other species (i.e. living on land and water both).

> In the environmental sector, the range of possible referent objects is very large, ranging from relatively concrete things, such as the survival of individual species (tigers, whales, humankind) or types of habitat (rain forests, lakes), to much fuzzier larger-scale issues, such as maintenance of planetary climate and biosphere within the narrow band human that beings have come to consider to be normal during their few thousand years of civilization. Underlying many of these referent objects are baseline concerns about the relationship between the human species and the rest of the biosphere and whether that relationship can be sustained without risking a collapse of the achieved levels of the civilization, a wholesale disruption of the planet's biological legacy or both. The interplay among all of these factors is immensely complicated. At either the macro or the micro extreme are some clear cases of existential threat (the survival of species, the survival of human civilization) that can be securitized. In between, somewhat as in the economic sector, lies a huge mass of problems that are more difficult, although not impossible, to construct in existential terms. (Buzan 1998: 22)

However, the discourse on environmental security is varied in nature and that needs a greater cooperation between the governments, private sectors, NGOs, and Civil societies. Present scenario securitisation of cyberspace is much needed assets for environmental security and vice versa, the reason is growing dependency on nuclear technology and ICTs brings new vulnerability to everybody.

2.4. International Relations and Information and Communication Technology (ICT)

"This primer on the *information age*, as well as the other primers in this series on the *Information Economy, Society and Polity*, is an act of imagination and affirmation of a future that is being shaped by *information and communication technologies* (ICTs)" (Lallana and Uy 2003: 5).

The linkages between IR and ITC have a great impact on the geopolitics of human history. Undeniably, technocratic revolution has introduced many new phenomena to the world around us, but it has a dark side as well. Leaving aside the negative aspects, rest shows that we have entered into the landscape of the information age, technically called the digital world where information floats easily and smoothly from one part of the world to the other. The initial development in the domain that ushered in the age of ICT can be traced back to the invention of the Telephone by Alexander Graham Bell in 1875.

> "Technological breakthroughs have revolutionized communications and the spread of information. In 1875, for example, the invention of the telephone breached distance through sound. Between 1910 and 1920, the first AM radio stations began to broadcast sound. By the 1940s television was broadcasting both sound and visuals to a vast public (Lallana and Uy 2003: 5).

Human entrepreneurship and enterprise has added a new paradigm to the landscape of international relations i.e. Information and Communication Technology (ICT). Particularly, this term is a combination of three words: Information, Communication and Technology but in simple terms ICT refers to a broad field encompassing computers, communications equipment and the services associated with them. It includes the telephone, cellular networks, satellite communication, broadcasting media and other forms of communication (Lallana and Uy 2003: 7). Subsequent developments in the field of ICT created a new concept called *digital world*, this word will be used often in this study because cyberspace is a part of digital world and vice versa. A digital world is a world united by one language; a world where people from across continents share ideas with one another and work together to build projects and ideas (Lallana and Uy 2003: 6).

Further, Lallana and Uy (2003: 7) have argued that the ICT revolution and the digital revolution are two different revolutions occurring in different times. The essence of their argument is that the revolution in ICT took place in 1875 when first telephone was invented by the A. G. Bell, but the process of digitisation came into being during 1960s (1961 to be precise, when the first digital carrier system was installed). Digital revolution from the 1970s to the 1990s had a spill-over effect on national security and international relations. A new era of technology competition began in the realm of international politics on October 4, 1957, the day when USSR (present Russia) launched its first satellite Sputnik-1 into the space. It was the period of the Cold War. Space-race between the two rivals (US and USSR) was at its extreme. Such a revolution brought new developments i.e. internet, computer and related issues into the security landscape. Technology has transformed everyday life. Although the computer was invented in 1943, it was with the invention of the microprocessor in 1970, that it became available to general public. Coming back to the digital world, one fact is clear that things get much easier to be done. In fact, sophisticated advancement of present technologies is enhancing the significance of the digital world. Thus, at a technological level all kinds of computers, equipment and appliances are interconnected and functioning as one unit. Such digitisation helps computers to play movies and tune in to television on the one hand and on the other some modern homes allow a person to control the central lighting and air-conditioning remotely through computers. These are just some of the features of a digital world (Lallana and Uy 2003: 6). This physicality of the digital world has given a new domain to human activities. As far as international security is concerned it has been profoundly impacted by the digital revolution.

2.5. International Security and Cyberspace

In contemporary geopolitics, revolution in the domain of ICT brought up new issues relating to the Cyberspace, Cyber threats, Cyber-crime, Cybersecurity digital age, information age and so on. Emergence of such a jargon in the realm of international security is a proof in itself that non-traditional threats have been increasing in their importance. Let us take the case of cyberspace first, we will come back to the relation between the international security and cyberspace later.

2.5(a) What is Cyberspace?

The word Cyberspace was first used as a matrix in the fictional work of William Gibson in 1982- a short story 'Burning Chrome', to refer to a computer generated virtual reality. The term became popular in 1984, after its use in Gibson's novel Neuromancer. Etymologically, cyberspace is a compound term and the origin of the first word *'cyber'* can be traced to the Greek word *kybernetes*, which means pilot, governor and ruler. The root '*cyber*' is also related to '*cyborg*'- a term that refers to a human-machine synthesis created by connecting the human body to advanced high-tech devices[13]. But the word cyberspace was made widely popular by the computer professionals. It was defined in a different way by Bruce Sterling (1994): "Cyberspace is the 'place' where a telephone conversation appears to occur. Not inside actual phone, the plastic device on your desk. Not inside the other person's

[13] Vassilys Fourkas, what is 'Cyberspace'? http://www.waccglobal.org/en/20043-communication-rights-an-unfinished-agenda/495-What-is-cyberspace.html (accessed 15/01/2013)

phone, in some other city. The *place between* the phones. The indefinite place out there, where the two of you, two human beings, actually meet and communicate"[14]. Further argues that in the past twenty years, this electrical 'space' which was once thin and dark and one-dimensional, little more than a narrow speaking-tube stretching from phone to phone, has flung itself open like a gigantic jack in the box. Light has flooded upon it, the eerie light of the glowing computer screen. This dark electric netherworld has become a vast flowering electronic landscape. Since the 1960s, the world of the telephone has cross-bred itself with computers and television, and though there is still no substance to cyberspace, nothing you can handle, it has a strange kind of physicality now. It makes good sense today to talk of cyberspace as a place all on its own (Sterling 1994). Sometime question arises how it emerged as a domain and what are its components. In short, cyber-ecosystem has some basic components. First, and most importantly, it is a communication network that is organised transnational(ly) and not through the institutional structures of the state system. Second, and closely related, cyberspace is operated as a mix of public and private networks. Third, unlike other domains, such as the sea, land, air or space, cyberspace is a human-made domain in constant flux based on the ingenuity and participation of users themselves. Fourth, cyberspace is comprised of both a material and a virtual realm; a space of things and ideas structure and content (Deibert and Rohozinski 2010: 16).

During, the 1950s and the 1960s much development took place in the field of internet and computer technology. Although Charles Babbage is considered the father of computer, but it was the German civil engineer Konrad Zuse who in 1941 gave a new shape to the modern computer. The commencement of the *space race* between the two rivals gave internet to the marketplace, but during that time it was mostly used for military purpose, research and for some institutional work. During the period of 1989-1991 a revolutionary innovation, the WWW and HTTP[15] came in the field of internet through the scholarship of Tim Berners Lee which immensely amplify the spread of internet and computer technology all over the human landmass. Perhaps, these revolutionary developments gave a physical shape to cyberspace.

[14] Bruce Sterling, Introduction to the Hacker Crackdown: Law and Disorder on the Electronic Frontier http://ebooks.adelaide.edu.au/s/sterling/bruce/hacker/complete.html (accessed 07/04/2013).

[15] WWW and HTTP means World Wide Web and hypertext transfer protocol respectively.

In fact, cyberspace has emerged as the fifth domain of human activities after land, water, air and space. UNESCO declares that the right to assemble in cyberspace comes under the Article 19 of the Declaration of Human Rights. Indeed, the accessibility to cyberspace is very important because, "*today there are five billion mobile phone users and two billion internet users. As a consequence of the proliferation of these and other data-producing devices and sensors, there are more transistors on our planet than grains of rice*" (Harry Van Dorenmalen 2012). The complex interdependency in cyberspace makes it more vulnerable because of its soft nature and ease of access, and this makes it difficult in identifying where the threats to it originate form, i.e. whether it is a state or a non-state actor.

Coming to the international security landscape, new security threat offer a challenge to IR theory. From the beginning of the Cold War till now technological breakthroughs have been gradually transforming the nation-states. Diffusion of technology in a globalised world has also fragmented the landscape of security into various dimensions. Particularly, 9/11 was a critical event and is one of the focal points of that fragmentation. On the other hand emerging threats are in a new arena point to threat like in a cyber-age, digital age information age. Looking at the statement of Harry Van Dorenmalen (the chairman of IBM Europe) that '*there are more transistors on our planet than grains of rice*', one cannot do anything but realise that it is true and at the same time it is the reason behind the vulnerability of the cyberspace. In fact, cyberspace is a double-edged sword so it should be used carefully. Take for instance the rise of the *Arab Spring* in 2010-2011 against the authoritarian regimes of Arab world and later the dramatic death of Colonel Gaddafi, here cyberspace played a vital role in people's assertion of their individual liberty. In an incident in 2007 the *DDoS attack*[16] on Estonian government websites by an

[16] In a distributed denial-of-service (DDoS) attack, an attacker may use a computer to attack another computer. By taking advantage of the security vulnerabilities or weaknesses, an attacker could take control of a computer. He or she could then force the computer to send huge amounts of data to a website or send spams to particular email addresses. The attack is "distributed" because the attacker is using multiple computers to launch the *denial-of-service attack*. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting a computer and its network connection, or the computers and network of the sites one is trying to use, an attacker may be able to prevent that person from accessing emails, websites, online accounts (banking, etc.) or other services that rely on the affected computer.
http://www.us-cert.gov/ncas/tips/ST04-015 (accessed 10/05/2013).

anonymous hacker from Russia hampered individual liberty. Such types of attacks create new challenges in the realm of international security and that is the reason why in this digital world protection of cyberspace is emerging as a major issue for states.

2.6. Issues in Cyberspace

Information wants to be free [....] and the nascent world of cyberspace is full of sysadmins, teachers, trainers, cybrarians, netgurus, and various species of cybernetic activists (Sterling 1994).

Since more than two decades the synergy between the internet and computer technologies and more broadly the Cyberspace has been emerging as a new area in the field of international security. *Glocalisation* of cyberspace has tremendously impacted our everyday life and equally on the socio-economic-cultural and political sphere, shaping and reshaping with time. The Canadian cyber-specialist Rafal Rohozinski said that 'the poor and developing countries are changing the culture of cyberspace'. For instance, in Kenya 99 per cent of the new internet connections are by young people using mobile phones (Grauman 2012). In India, in 2012 (the issue of Northeast Indians and their safety in Bangalore as well other parts of the India) the integrity of the country was shaken through the misuse of cyberspace by miscreants. After that incident, a security analyst commented the Major (Gen.) Ashok Mehta said (in a discussion on Defence Watch 2012) that it was the first organised abuse of cyberspace against India. A country including its armed forces has to be prepared to protect the cyberspace while *balancing the freedom of speech* with the need to *maintain peace and harmony* essential for *internal stability and national security.* In that discussion the CEO of DSCI Dr. Kmalesh Bajaj argued that the 'internet which grew purely as an attacking domain is now encompassing every aspects our life. We cannot conceive life without internet, because from defence application to governance to daily shopping and so on, internet has a significant application. And the platforms which are used to deliver such applications are vulnerable to attacks. Their vulnerabilities lie in the basic software and in getting more proliferate because we are making these applications available on a platform which is more vulnerable. Today there are 100 million users. With 500 million Smartphones connected to the cyberspace the vulnerability of applications increases as it is proliferating into the Smartphones, so the space itself is becoming more prone to attacks'.

In fact, in the international security landscape during the period from 1989-1991 had a great significance. During this period end of the Cold War and the subsequent geopolitical changes led to a new era of freedom of expression and freedom to access to information. It was possible only for two reasons: the success of European peace project (EU) side by side with the process of globalisation helped to erase the miseries from Central and Eastern Europe. It gave a breakthrough for the rise of information age and cyberspace. The free flow of information from one corner to other helped to develop good relations between the states which could not be achieved through traditional diplomacy.

The scholarship of securitization has primarily based themselves on the issues of *identity*, whether it is political, social, national and cultural or any other form. The present geopolitical scenario is becoming more complicated. The domain of cyberspace is complex, in which identity theft is a reality. Millions of people are entering into it with billions of issues daily. The area of cyberspace is getting vulnerable due to its illegal use, reason behind that is access to it has become so economical. Identity theft is just the tip of the iceberg. The real threat to cyberspace comes from, like cyber-crimes, cyber-war, cyber-terror, cyber-doom. Cyberspace has thus also become securitised.

2.6(a) Cyber-crime

Conventional crimes such as arson, burglary, and murder are mainly against individuals and their property. Unlike conventional crime, Cyber-crime is more unique and sophisticated in nature. There are three factors which have made its structure so complicated. They are technology and skill-intensiveness, a higher degree of globalisation than the conventional crimes and the newness (Kshetri 2010: 35). Kshetri (2010: 35-36) has argued that technological skills and its linkages with globalisation have increased the power of cyber-criminals manifold. Secondly, the *newness* with and within it which in other way influences the law enforcement mechanisms and simultaneously leaves loopholes in the laws and the system to commit and get away with such (cyber)crimes.

> [...] [Due to] newness of cybercrimes, law-enforcement authorities across the world are relatively inexperienced to deal with these crimes [and the]

> implication of newness is that the legal system is not well-developed to deal with cybercrimes. [In fact] the traditional model of law enforcement is a compilation of past practices that have been deemed effective in dealing with the phenomena it confronts. The model's general strategy, the reactive approach, is one that has been in use since antiquity. [Therefore] first, principles of law need rethinking in [terms of] the cyberspace, [Because] still another dimension of newness is a lack of previously developed mechanisms and established codes, policies and procedures. These factors are likely to result in much less guilt in cybercrimes compared to conventional crimes (Kshetri 2010: 35-36).

Indeed, in international security landscape for the first time a major cyber-attack took place in 1990 all over the USA. Today, when technology has grown by leaps and bounds since that incident 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 to do so primarily to fulfil the economic temptation[17] 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 and malwares. Such attacks have acquired a new dimensions altogether, for example, the Stuxnet. In fact, the scholars termed this new act as *cyber-war* or *cyber-warfare.*

2.6(b) Cyber-war/ Cyber-warfare

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[18]. The term cyber war/cyber-warfare was first used by the Richard A. Clarke in his book *Cyber War* in 2010. Most of the scholars have taken it as mainly a political action of

[17] Offences are most imminent if their technological viability coincides with a high level of economic temptation to break the rules [...]. People can perceive the criminal law system as legitimate and fair, accept the legitimacy of anti-cybercrime norms and internalize them, but may violate them when they have a powerful temptation [...] (Kshetri 2010: 36).
[18] War in the fifth domain, http://www.economist.com/node/16478792 , (accessed 13/02/2013).

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 has linked threats to politics, defence, economics, information, privacy etcetera. Both are supplementary and complementary to each other. But, cyber-warfare is newer and more harmful. In fact, after the three major incidents: Estonia 2007, Georgia 2008 and Stuxnet[19] (it was a highly sophisticated worm/malware which first came to the marketplace in June 2010) and attack on Iranian nuclear projects in Natanz has shown how disastrous the new (cyber) warfare can be. It is believed that both Russia (in Estonia 2007 and Georgia 2008) and the US have indulged in such attacks. 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 fought at any but the virtual domain.

Scholars like Richardson have argued that in the age of Stuxnet cyberspace has become more vulnerable and cyber-warfare more fierce. After it was detected in Iran, that Stuxnet is one of the most sophisticated and highly systemised malware which can move into thousands of computers without the knowledge of the user. Second, it has some kind of identity passport (when a new software is installed or seeks entry to a programme, the program generally asks for an identity) through which it can enter into any Windows operating system. Third, it will not spare a single photo or an Mp3 from being corrupt. Fourth, an individual or a nation-state can set a specific target for Stuxnet to attack (technically the code of the computer) and due to its sophistication it moves automatically until it reaches that particular system. Last but not the least, it can be transferred through a flash drive or a USB to a computer and then let loose to find its target. As far as conventional warfare is concerned it can be seen or adjudged through the landscape of International Humanitarian Law but due to lack of policies and law enforcement mechanism for cyberspace both on

[19] Randy Abrams, (A researcher with ESET, A privately held security firm that has studied Stuxnet) said that, Stuxnet Virus is malware that attacks widely used industrial control systems built by the German firm, Siemens AG. The Company says the malware was initially distributed via an infected USB Thumb drive memory device or devices, exploiting vulnerabilities in the Microsoft Windows Operating system. Such Systems are used to monitor automated plants- from food and chemical facilities to power generators. Analysts Said attackers may have chosen to spread the malicious software via a thumb drive because many SCADA (Supervisory Control And Data Acquisition) Systems are not connected to the Internet, But do have USB ports. Once the worm infects a system, it quickly sets up communications with a remote server computer that can be used to steal proprietary corporate data or take control of the SCADA system (Richardson 2011: 9). It has been believed that it is one of the US-Israel joint venture to produce this virus to defect the Iranian nuclear project.

humanitarian and legal grounds illicit users of cyber domain find it easy to commit such acts. Simultaneously, there are still some differences between the public and the private stakeholders regarding the reality of cyber-warfare. In fact, Computer programmes like Stuxnet are weapon of cyber-warfare and are very much real.

However, when questions for the protection of the critical Infrastructure and the fear of cyber-terror arises, scholars like Lallana and Uy (2010: 28) say that cyber-terrorism is a *narrow concept* but on the other hand we cannot deny the ability of terrorist groups to manipulate it.

2.6(c) Critical Infrastructure and Cyber-terrorism

Contemporary politics relies heavily on the functioning of critical infrastructures like water supply, electricity, telecommunications and especially the underlying information and communication systems. Defence, energy and transport too are crucial sectors. 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.

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 in Cyberterrorism – fact and fancy? 1998).

Pollitt (1998) has argued that "computers control power delivery, communications, aviation, and financial services. They (computers) are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable - to the effects of poor design and insufficient quality control, to accident and perhaps most alarmingly, to deliberate attack. 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" Cavelty (2010: 182). The technological dependency and its nature of vulnerability could create some terrifying situations. Eventually, the "problem with the use of the term 'cyber-terrorism' in this discourse is that the term has become totally bereft of meaning by the frequent evocation in the media for attacks of any kind with the help of computers which is exacerbated by similar use of the term by government officials" (Cavelty 2010: 182).

The rise of vulnerability in the cyber domain could lead to a catastrophe, therefore, cyberspace has to be secured. Although, the discourse on cyber-security originated late in the 1980s in the U.S but it got the geopolitical momentum largely a decade or so. Information revolution and deep rooted dependency and influence of ICTs into all spheres of human life have left gaps for such vulnerabilities, which are technically called risks (Cavelty 2010: 180).

2.7. Cyber-security

''Cyber security", a concept that arrived on the post-Cold War agenda in response to a mixture of technological innovations and changing geopolitical conditions (Hansen and Nissenbaum 2009: 1155).

It is noteworthy that we are at the crossroads of the ICTs revolution because the socio-economic, cultural and political milieu has transformed drastically from the industrial revolution till now. On the other hand the domain of cyberspace is vulnerable and in due course of time its vulnerability may increase. Scholars have argued that the cyberspace is becoming more vulnerable because the domain itself is prone to threats. There is a certain identifying terminology to refer to its vulnerability, viz. crime in cyberspace, cyber-terrorism and cyber-war on one hand, privacy and freedom of expression and more often protection of critical infrastructures on the other. Particularly in all those sectors ICTs have been playing a bigger role. From a geopolitical angle there are huge differences, for a country like China it is information security for others it is cyber-security, and in the individual level it is computer security, internet security. On the other hand, many debates have been taking place in public domain to address this situation. But, the undeniable fact is that cyberspace has great opportunities as well as great vulnerabilities (Nye 2011). To combat cyber-threats nation-states need to stand at a vantage point to create a strategy because it is politically very important but is a highly technical area at the same time. Lallana and Uy (2003: 29) opine: '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".

In the cyber domain largely there are two types of inhabitants: peaceful users and illicit users. The ICT facts and figure 2011 shows that 35 percent of people use internet all over the world and among them nearly 50 percent are from the younger generations, i.e. bellow the age of 25. Thus, the threats to cyberspace come from 'some' within this 35 percent, but all the users have to face the consequences. Individuals of different ages with different motive and different requirement enter into the cyber domain. If we keep traditional security out of the discussion even then there is a huge space for cyber-threats to build a *threat cluster* (Cavelty 2010: 180) because the leadership is fumbling around with the difficulty(ies) in balancing parallel demands: economic recovery and growth vis-à-vis national security and infrastructure protection. "This 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).

> 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". Unlike atoms, human adversaries are purposeful and intelligent. Mountains and oceans are hard to move but portions of cyberspace can be turned on and off at the click of a mouse. It is

> cheaper and quicker to move electrons across the globe than to move large ships long distances through the friction of salt water. The costs of developing multiple carrier taskforces and submarine fleets create enormous barriers to entry and make it possible to speak of U.S. naval dominance. In contrast, the barriers to entry in the cyber-domain are so low that non-state actors and small states can play significant roles at low levels of cost. (Nye 2011)

Securing cyberspace has become a much need element for individual well-being as well as for the nation security. Indeed, it was the U.S which started internet and later globalised it but now the U.S has become the main victim of cyber-attacks. 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)

However, the debate which was confined to computer scientists in the 1990s now is getting a geopolitical momentum. The cyberspace and its security are not the only threats to the national security but companies and corporations. This is the reason for huge debates and discussions that have been put forward on the platform of joint ventures i.e. PPP (Public Private Partnership)

2.7(a) Public-Private Partnership

Public-private notion is little different, here public means UN and other National Governments, International Organisations and private includes the non-governmental organisations (INGOs, TNGOs) Corporate sector (TNCs and MNCs), and various Institutions. Though the horizon of cyberspace is very wide, thus, to secure it from threats both public and private institutions have to put forward their efforts. Indeed, "we individuals, business and government organisation are all at risk to the prolific threats impacting our networks" (INSA 2009: 4). In the words of Scott Charney (2012) "*private sector must have a seat at the table [...] (it) owns the majority of today's global networks ... governments are the primary actors in international negotiations [...] (private sector) can contribute considerable operational experience to help inform these discussions*".

However, cyber threats have to be addressed in a structured way because the '*cyberspace ecosystem*' (Scott Charney 2012) is directly or indirectly consists of Internet, Telecommunications, and Computer networks. Nevertheless, as paradigm shift is concerned "*In the industrial age, power was generally based on physical might; in the digital age, power is derived from information, knowledge, and communications*" (Charney 2012: 39). Indeed, Cyber-security is no longer pure computer security, because it has much implication on health, education, economy, and politics of the State and illicit use of cyberspace could lead to denial of the services. However, at present both the government as well as the private stakeholder at the crossroads of cyberspace and getting more dependent on "ICT applications, such as e-government, e-commerce, e-education, e-health and e-environment" and e-election too. This is the main reason why the Estonian Government suffered a lot during the massive attack in 2007. To tackle this type of situation "development of domestic legislation to eliminate safe havens for criminal misuse of technologies, [...] improving law enforcement, [...] improving information exchange, [...] and public awareness" [(UNGA 55/63) ITU2011a: 183] has to improve their level of action and "there must be no safe havens for those who abuse information technologies" [(G8 1999) ITU 2011a: 176].

In 2008 International Telecommunications Union (ITU) stated that Cybersecurity is one of the profound challenges of our time and likewise in 2011 ITU pointed out that cybercrime is a major challenge, especially for developing countries. And the offences basically based upon four aspects "offences against the confidentiality, integrity, and availability of computer data and system; computer related offence; content related offence; and copyright related offence" (ITU 2011a). Thus, "we need a balanced view that recognises that there is a cyber-threat, but neither under-estimate nor over-hype the problem" (Giampaolo Di Paola 2012: 58) because, "internet (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 mitigate the threats no matter how they emerged and through whatever source (economic reason or political reason or social reason or else).

2.8. Conclusion

"If you shut down the Internet today you would shut down our economy. That's both the good news and the bad news", according to Julius Genachowski (2012), Chairman of the Federal Communications Commission.

Cyber-threats are asymmetric threats to national security, which has innumerable ways to impact the security landscape. Cyber-crime is mainly an economic crime in the respect that the victim has to face financial loses. Many kinds of incidents have taken place, for example, account forgery, credit card hacking, money laundering. It is not a single individual act rather it is a group act. 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, for example, the attack on Iran which was to destabilise the nuclear plant. The differences rose between the western governments and the Iranian government. There were the triangular fears of regime change, nuclear capability and linkages with terrorist groups which resulted in such an attack. Sometimes an attack has links with some ideological motives which was the case of such attacks on Estonia and Georgia. Cyber-terrorism although is yet to make a radical geopolitical appearance, but undeniably, different terrorist organisations are active in the cyber domain to fulfil their goals, such as new recruitment, fund raising, online training and so on. It seeks to harm all the aspects of a nation state, viz. political, social, economic, and ideological, and establish its main motive which is to create their own domain and cause destruction to others.

Other than these, there are other online threats such as child abuse (child pornography) illegal and illicit materials such as videos, images, hate speeches to disturb the peace and tranquillity of the society etcetera. On the one hand protection of critical infrastructure for growth and sustainability of a nation cannot be ignored while on the other hand the well-being of the citizens is of paramount importance.

The traditional schools of IR theories have remained silent about the non-traditional threats. The securitization (Copenhagen school) has some implications on the non- traditional threats like cyber-security. They argued "*Cyber security is not left to the liberal market, but implies a complex constellation of public-private responsibility and governmental authority. [...] (It) is the linkage between ''networks'' and ''individual'' and human collective referent objects*" (Hansen and Nissenbaum 2009: 1162). Likewise, they have looked upon some aspects *Hypersecuritisation, Everyday security practice, Cyber-securitizations, Technification*, (Hansen and Nissenbaum 2009) which is in their language *the specific grammar of the cyber security sector* (Hansen and Nissenbaum 2009: 1163) The basic assumption of securitization is who securitizes, what issue and for whom. Here in the landscape of cyber-security state, international organisations as well as private institutions are the securitizing actors.

The issue is the protection of cyberspace which includes the two way strategy: first, security of national assets and second the safety of privacy and freedom of expression. Freedom of expression is a very important reason why cyberspace needs to be securitized. Cyberspace is for everyone (i.e. the state, individuals and groups) because cyberspace is a place by the people for the people and of the people. 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'.

The essence is that the nation-states, international organisations, private institutions and individuals (i.e. IT experts and academicians) have to cooperate to address these new threats. Although cyber-threats yet has not made a significant appearance but most of the things which are interconnected to it have huge implications for physical world, which make it a major threat. Nye argued that the cyber-realm is a combination of physical world and virtual world in this real world. The U.S Defence Secretary Leon E. Panetta said that United State may have to face situations like a *Cyber Pearl Harbour* and it is the responsibility of both the Government and Business institutions to work for digital security. In these two statements one thing worth noting is that cyber-threats pose a great danger to the human world. Hence, a new active co-operation has to be forged at the earliest between and among the stake-holders to be ready in case of an attack. All stake-holders in the Cyber-domain thus need to have a proactive rather than a reactive approach. For instance, in the U.S there are the unilateral policies and programs for cyber-security in place, but on the other hand the European Union has been putting in enormous efforts to tackle NTT/NTS (non-traditional threats/non-traditional security) at the global level through a multilateral approach. This has justified its role as a prominent actor in the security landscape since 2003 in the field of unconventional security in general and cyber-security in particular.

CHAPTER 3

THE EUROPEAN UNION'S APPROACH TO CYBER SECURITY

> Modern societies confront a myriad of risks that threaten the *economic prosperity*, undermine the safety and *security of citizens* and cause significant *disruption to society and politics*. These risks range from empowered and *militant non-state actors* to *technological and human-made processes*, such as *environmental degradation and global warming*. Risk mitigation has become a routine phenomenon of good public policy (Deibert and Rohozinski 2010: 15).

3.1. Introduction

The European landmass had suffered badly due to two World Wars and which also brought to focus the security of the region. The end of the Second World War (1939-1945) brought in many problems, but not without glimpses of prospects for the Europeans. Those prospects emerged as peace dividends at the time when the *Cold War was increasingly evident* (Bretherton and Vogler 2006: 3). The rebirth of peace processes in Western Europe lead to a generis identity which resulted in a spill-over effect in all dimensions: economical, social, political, and cultural and moreover in the military affairs of Europe. These developments had taken place through the impact of two *major factors* (a) supports from the US (b) and the willingness for peace from the (Western) Europeans. The process sought to create economic cooperation and to harmonise the war industry (i.e. Coal and Steel which had played a pivotal role in the war), and the reconstruction of peace in the continent. In 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. Later the vertical and horizontal development viz. Maastricht Treaty in 1992, Amsterdam Treaty in 1997, Nice Treaty 2001 and eventually the Lisbon Treaty in 2009 have given completeness to the Union in the policy and the structural landscape signified security and foreign policy as an important aspect of the Union (i.e. Common Foreign and Security Policy). In fact, during 1951-1990, the European Community grew tremendously and went on to establish itself as a *global economic actor* (Bava 2007: 99). In 1992 the Maastricht treaty entered into force and that put in play a new paradigm in Europe. However, the European Union (EU), it took more than a decade to assume the status of a full-fledged actor in the security landscape. The Amsterdam

Treaty initiated a process of 'communitarising' 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. Subsequently, there has been 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). But, the Security Strategy (ESS 2003) indeed has provided the Union with the needed impetus to tackle the geopolitical turmoil. In fact, a review of that document had appeared in 2008, in which cyber-crime had been added as an emerging threat to national security. Thereafter, many developments have taken place in the EU to tackle this new threat. Before going into a detailed analysis of the EU's policy on Cyber-security, it is necessary to briefly outline the contexts because it made the EU to take a proactive move in the security landscape.

3.1(a) The Return of War to Europe and its impact on the European Union

The formation of the European Union (EU) and the incremental growth 'turned the swords into ploughshares'. But, the end of Cold War had paved the way for the rise of new threats. During the dissolution of Yugoslavia and the subsequent wars during 1991-1995, "the Western Balkan states became Europe's *Achilles' heels*, revealing the EU's inability to act decisively in periods of crisis. The EU neither played a critical role in the bloody ethnic conflicts in the former Yugoslavia nor succeeded in mobilizing the international community before the upsurge of the Kosovo crisis. However, 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). *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' (Cohen 2005: 365).*

Undeniably, the EU had failed to tackle the situation, but that crisis had proved to be a roller coaster for the Europeans and for the Union too. 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). In fact, the consequences had paved the way for the Union to assume a new identity of the EU's role in Crisis management and Conflict resolution and emergence of the EU as a security actor. Although, the EU has been performing well in the field of crisis management and in resolving conflicts, there is a debate to identify the nature of the Union in the realm of security. Bava (2007) argued that the role of the EU as a security actor is far from easy. On the other hand, Kaunert raised the question that whether the European Union is a weak security actor or an increasingly significant security actor (Kaunert and Leonard 2012: 418), because in the landscape of (security and) foreign policy, capability and capacity of states influence global politics. In other words, the state and all the power it has influence the desired outcomes, especially in the realm of military security, in the form of military power. Second comes the definitional problems with the EU itself (Bava 2007: 98).

> If the state is the template of actions to judge how effective a security actor it is, then the EU does not fit into this category. The EU defies definition. It is Intergovernmental and supranational and almost state like. The major difference is that it is almost alike but not a state and so it is not a unified single actor like a state. (Bava 2007: 98).

In fact, such debates arose due to the incapability of the EU made evident during the Balkan crisis. Balkan states have both geopolitical and strategic implications on the Union's fabric. Thus, any problem in this region will impact the EU as well. In Turhan's view, any regional conflict in the Balkans, known as the "*backyard of Europe*," would not only allow the countries to drift into turmoil, but would also threaten the security of Europe (Turhan 2011: 4). The Balkan nations became more important especially after the last two enlargements of the EU in 2004 and 2007 when the EU frontiers were extended to the East, and with the new Union of 28, moved closer to the countries of the Western Balkans (Berbec 2010 ,Turhan 2011: 4). Global geopolitics has taken a major shift during the period 1989-1999 i.e. the end of the Cold War and the disintegration of the USSR, and the diffusing of threats brought the attention towards the non-military dimensions of security.

3.2. <u>Non-traditional Threats and the EU Approach in the post 9/11 Period</u>

Within the overarching Cold War framework, there was a *well-defined and identifiable threat to the European security landscape* (Bava 2007: 99). But, the end of the Cold War paved the way for new threats to emerged in the Europe. In the words of Turhan (2011: 12), '*Open status issues with serious problems* in institutional, political and economic spheres', viz. "constitutional uncertainty, the weak state syndrome, poor business environment, high rates of unemployment and on the other hand, peace building, stability and transparency in government, extremism and ultra-nationalism, organized crime and corruption and poverty are the key issues that not only the Western Balkans but also the EU has to tackle [during the enlargement process]" (Biscop 2004: 9). Unconventional threats have manifested their geopolitical appearance in a dramatic way.

Kofi Annan (2005) has given a candid opinion regarding the non-traditional threats to security:

> "Ask a New York investment banker who walks past Ground Zero every day on her way to work what today's biggest threat is. Then ask an illiterate 12-year-old orphan in Malawi who lost his parents to AIDS. You will get two very different answers. Invite an Indonesian fisherman mourning the loss of his entire family and the destruction of his village from the recent devastating tsunami to tell you what he fears most. Then ask a villager in Darfur, stalked by murderous militias and fearful of bombing raids. Their answers, too, are likely to diverge".

A major incident took place on September 11, 2001, which worked in two ways: first, it shifted the US priorities and also influenced the logic of the EU enlargement momentum. Along with the war on terrorism, the crises and wars in Afghanistan and Iraq inevitably turned US concerns to other regions and gave the EU an opportunity to take more initiative in the Balkans. Thus, it is not wrong to view that in the transatlantic rivalry between Europe and America, the Balkans had become one of the most important arenas in which European potential was manifested (Turhan 2011: 8). Second, 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. Such divergence had originated between the Atlantic allies due to the overwhelming unilateral approach of the US towards the issues which did not go down well with the Europeans. Thus, in 2003 the European Union came with its brand new Security Strategy to tackle the unconventional threats.

3.3. European Security Strategy and Subsequent Developments, 2003-2008

Europe has never been so prosperous, so secure or so free. The violence of the first half of the 20th Century has given way to a period of peace and stability unprecedented in European history (ESS 2003: 1).

A wide range of geopolitical turbulence, exogenous shocks (Kaunert and Leonard 2012) and incremental growths in the EU had lead to new security paradigm for the region, which was clearly outlined in the 2003 security strategy - A Secure Europe in a Better World. Going back to the Cold War politics, the security of the region was overseen by the North Atlantic Treaty Organisation. The cooperation between the NATO and the EU continued till the Berlin plus Agreement. But, after that, the EU also pushed itself as a security player in the global politics. But, the state of affairs is paradoxical, on the one hand the EU is not a state rather an outcome of mutual cooperation between states and on the other hand, it is "separable, but not separate" (Schmidt 2000) from the NATO because most of the countries are members of both the organisations. Eventually, the ESS has underpinned the fact that "the world is full of new dangers and opportunities" (ESS 2003: 14), therefore, it is needed to have multilateral approach to tackle the new threats. In fact, the ESS (European

Security Strategy-2003) was aiming to frame a pan-European mechanism with global applicability. In addition, the geopolitics of 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). The incident of 9/11 has 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, because *security* is a desirable condition for *development.* The ESS in 2003 has pointed out five key threats:

> "*Terrorism, Proliferation of Weapons of Mass Destruction, Regional Conflicts, State Failure and Organised Crime*" (ESS 2003).

But the strategy has been criticised by various scholars as well as from the EU-sceptics:

> A true European Union foreign policy would require a more strategic outlook to realize that potential. The elaboration of a European security strategy (ESS) in 2003 was an important step in that regard, *but creating a strategy document is not the same as having a strategy.* 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. It is much more than just a document; it is a process that seeks to negotiate the limits of what the polity can agree on, to smooth out the most logically incompatible edges of that consensus, and to produce a document that can command widespread respect and agreement. The resulting strategy document, even if it gets the headlines, is the least important part of that process—it is the result of a political negotiation, not the impetus for a strategic change. The ESS was not created through such a political process; rather the ESS process was *heavily centralized in the staff of the EU's High Representative for the Common Foreign and Security Policy,* Javier Solana. Indeed, the European Union lacks the institutional infrastructure to carry out such a process. (Bindi 2010, Shapiro and Bindi. 2010: 343).

Though, there are differences within the ESS but still it has some justifiable objectivity which bolsters its significance in the 21st century. The ESS has briefly outlined three techniques to tackle the non-traditional threats: first, *identify the threats*; second, have a *strategic objective* of addressing the(those) threats through the international order based on effective multilateralism, simultaneously building security in [our] neighbourhood (which was latter manifested in the EU Neighbourhood Policy). Last but not the least, *implementing policy* in a proactive way, viz. in a more active, more capable and more coherent manner. The ESS also emphasises 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) Therefore, we need to develop a *strategic culture* that fosters early, rapid and when necessary, robust intervention (ESS 2003: 11). In fact, in 2005 the European Union has taken a *de facto* approach to tackle the problem of terrorism, i.e. the European Union Counter Terrorism Strategy, which has aimed to act with various institutions of Europe as well as in the global level. It has identified four major methods to stop the acts of the terrorist organisations. Those methods are the 'P3R', viz. Prevent, Protect, Pursue and Respond (EUCTS 2005: 3).

> "Prevent- to prevent people turning to terrorism by tackling the factors or root cause which can lead to radicalisation and recruitment, in Europe and internationally. Protect- the citizens and the infrastructure and reduce our vulnerability to attacks, through improved security of borders, transport and critical infrastructure. Pursue- to pursue and investigate terrorist attacks across borders and globally; to impede planning, travel, and communications; to disrupt support networks; to cut off funding and access to attack materials and bring terrorists to justice. Respond- to prepare ourselves, in the spirit of solidarity, to manage and minimise the consequences of a terrorist attack, by improving capabilities to deal with: the aftermath; the co-ordination of the response; and the needs of victims" (EUCTS 2005: 3).

However, in 2001, the Council of Europe convention on cyber crime emphasised the criticality of the cyberspace and rise of vulnerability in the cyberspace. It contains 48 articles on the subject of response to cybercrime, but unlike the ESS as well as the other policies of the EU, they have identified the nature of the unconventional threats but they failed to address the danger (i.e. Cyber-threats) poses. There had been some reasons for the Europeans to do so. First, the EU adopted the ESS prior to the Big Bang enlargement (Islam 2003) (i.e. 2004 Enlargement and latter 2007 and 2013 enlargements). After 2004, enlargement two famous comments have appeared, one from the Danish Prime Minister Anders Fogh Rasmussen, that "A new Europe is being born" and other one from the German Foreign Minister Joschka Fischer, that the EU's big bang expansion "the definite end of the Cold War" (Islam 2003). Second, at present the stakes of the Europeans in the Cyberspace is comparatively higher than 2000-2004 (see Table -1), and simultaneously, the vulnerability is also much higher. Third, during that period 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 crisis were the prime areas of concern.

In fact, the European Union had taken one important stand in 2004 which was to build a wide network EU security agency, i.e. The European Network and The Information Security Agency which came into force in September 1, 2005. The tables clearly indicates that there has been a dramatic change in the proportional growth rate (i.e. individual penetration in to the cyber domain) from 2003 to 2012, and most of the country's growth rate has doubled in 2012 in contrast to 2003 and mainly the smaller economy states have registered much higher growth than the major economies. On the other hand major economies of the Union are presently have more share than the United States. (See Table- 1 and Table 2)

Table 1 EU Member States Percentage of Individuals using the Internet

Country Name	Year												
	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Austria	33.73	39.19	36.56	42.70	54.28	58.00	63.60	69.37	72.87	73.45	75.17	79.80	81.00
Belgium	29.43	31.29	46.33	49.97	53.86	55.82	59.72	64.44	66.00	70.00	75.00	78.00	82.00
Bulgaria	5.37	7.61	9.08	12.04	18.13	19.97	27.09	33.64	39.67	45.00	46.23	51.00	55.15
Croatia	6.64	11.56	17.76	22.75	30.91	33.14	37.98	41.44	44.24	50.58	56.55	59.64	63.00
Cyprus	15.26	18.82	28.32	30.09	33.83	32.81	35.83	40.77	42.31	49.81	52.99	57.68	61.00
Czech Republic	9.78	14.70	23.93	34.30	35.50	35.27	47.93	51.93	62.97	64.43	68.82	72.97	75.00
Denmark	39.17	42.96	64.25	76.26	80.93	82.74	86.65	85.03	85.02	86.84	88.72	90.00	93.00
Estonia	28.58	31.53	41.52	45.32	53.20	61.45	63.51	66.19	70.58	72.50	74.10	76.50	79.00
Finland	37.25	43.11	62.43	69.22	72.39	74.48	79.66	80.78	83.67	82.49	86.89	89.37	91.00
France	14.31	26.33	30.18	36.14	39.15	42.87	46.87	66.09	70.68	71.58	80.10	79.58	83.00
Germany	30.22	31.65	48.82	55.90	64.73	68.71	72.16	75.16	78.00	79.00	82.00	83.00	84.00
Greece	9.14	10.94	14.67	17.80	21.42	24.00	32.25	35.88	38.20	42.40	44.40	53.00	56.00
Hungary	7.00	14.53	16.67	21.63	27.74	38.97	47.06	53.30	61.00	62.00	65.00	70.00	72.00
Ireland	17.85	23.14	25.85	34.31	36.99	41.61	54.82	60.55	65.34	67.38	69.85	76.82	79.00
Italy	23.11	27.22	28.04	29.04	33.24	35.00	37.99	40.79	44.53	48.83	53.68	56.80	58.00
Latvia	6.32	7.22	21.94	26.98	38.58	46.00	53.63	59.17	63.41	66.84	68.42	71.68	74.00
Lithuania	6.43	7.18	17.69	25.91	31.23	36.22	43.90	49.90	55.22	59.76	62.12	65.05	68.00

Luxembourg	22.89	36.16	39.84	54.55	65.88	70.00	72.51	78.92	82.23	87.31	90.62	90.89	92.00
Malta	13.11	17.88	28.92	31.64	34.62	41.24	40.41	46.90	50.08	58.86	63.00	69.22	70.00
Netherlands	43.98	49.37	61.29	64.35	68.52	81.00	83.70	85.82	87.42	89.63	90.72	92.30	93.00
Poland	7.29	9.90	21.15	24.87	32.53	38.81	44.58	48.60	53.13	58.97	62.32	64.88	65.00
Portugal	16.43	18.09	19.37	29.67	31.78	34.99	38.01	42.09	44.13	48.27	53.30	57.76	64.00
Romania	3.61	4.54	6.58	8.90	15.00	21.50	24.66	28.30	32.42	36.60	39.93	44.02	50.00
Slovakia	9.43	12.53	40.14	43.04	52.89	55.19	56.08	61.80	66.05	70.00	75.71	74.44	80.00
Slovenia	15.11	30.18	27.84	31.85	40.81	46.81	54.01	56.74	58.00	64.00	70.00	69.00	70.00
Spain	13.62	18.15	20.39	39.93	44.01	47.88	50.37	55.11	59.60	62.40	65.80	67.60	72.00
Sweden	45.69	51.77	70.57	79.13	83.89	84.83	87.76	82.01	90.00	91.00	90.00	94.00	94.00
United Kingdom	26.82	33.48	56.48	64.82	65.61	70.00	68.82	75.09	78.39	83.56	85.00	86.84	87.02

Comparing with the US

Table 2 Percentage of Individuals using the Internet in the US

Country Name	Year												
	2000	2001	2003	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
United States	43.08	49.08	58.79	61.70	64.76	67.97	68.93	75.00	74.00	71.00	74.00	77.86	81.03

Source: ITU, Percentage of Individuals Using Internet. (http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls)

Prior to the Budapest convention on cybercrime in 2001, some kind of a *de facto* debate on cyber-security had taken place within the EU framework, 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 emphasised 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 ECUS 200 billion by the year 2000. 86 million people were connected to the Internet worldwide by the end of 1996, and by 2000, this is expected to reach 250 million individuals" (European Commission 1997). This is based on a four pronged agenda:

> First, widespread affordable access to the infrastructure, products and services needed for electronic commerce must be provided through secure and easy-to-use technologies and services and reliable, high-capacity telecommunications networks. Second, a coherent regulatory structure within the EU, based on Single Market principles, must be ensured. Third, a favourable business environment must be fostered by promoting relevant skills and raising awareness. Fourth, there must be a compatible and coherent regulatory framework at the global level (European Commission 1997).

Quite naturally, it is an obvious fact for an economic power like the EU to think in terms of economic security in the realm of virtual world. In 2000, David Byrne, the European Commissioner for the Health and Consumer Protection emphasised that B2C (business to consumer) 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 citizen's to be concern about in the cyberspace and their economic interests as consumers. Use of the Internet for gathering information, education and for e-mails at present far outweighs its use as a transactional medium. We 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), but the vulnerability in the virtual domain creates problems for all. Hence, it is a matter of security and confidentiality. Thus, to address the vulnerabilities the Commission has found out three remedies, viz. prevention of the problems, alternative disputes resolution system and help of the courts which is the last resort (Byrne 2000: 3-6).

However, the review of the ESS has brought some changes as well as gave a composite shape to the ESS. 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 has brought in some more threats into the European frame work, viz. "*illegal immigration, piracy, Information Security and ecological problems*". Moreover, it has given a specific place to *cyber security,* which was added to the security strategy 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).

It is quite obvious that the EU has added cyber-security in the agenda, because the review report came after the major attack in Estonia and equally after the Central Eastern enlargements (in 2003 to 2007). The report has underlined some important areas and mechanism to fight against cyber-crime, viz. comprehensive EU approach, awareness both globally and locally, and international cooperation. In fact, since 2008 the debate on cyber-security has been vigorous in European countries. There are some identifiable reasons for this, Europe was seen lagging behind the United States in terms of Internet use, especially in the residential and SME markets prior to 2003 (Liikanen 2000: 5, ITC facts and figures 2009). But since 2003 a revolutionary shift has taken place in terms of Europeans (i.e. EU) accessibility to the internet (see table-1 and table-2), and that resulted after 2009 while the EU got its top position in the cyber-usage (ITC facts and figures 2010, 2011b, 2013). In fact, ITC facts and figures 2011 show that the Europeans have more stakeholders compared to others in the cyber-ecosystem with an average of almost 90'000 bit/s of bandwidth per user in Europe compared to the US with an average of 30'000-33'000 bit/s and 20'00 bit/s per user in Africa. Simultaneously, Europe leads in broadband connectivity, with fixed and mobile-broadband penetration reaching 26 percent and 54 percent, respectively. Recently released data from ITU shows that:

> "Over 2.7 billion people are using the Internet, which corresponds to 39 per cent of the world's population. In the developing world, 31 per cent of the population is online, compared with 77 per cent in the developed world. *Europe is the region with the highest Internet penetration rate in the world* (75 per cent), followed by the Americas (61 per cent) In Africa, 16 per cent of people are using the Internet – only half the penetration rate of Asia and the Pacific. In 2013, 41 per cent of the world's households are connected to the Internet. Half of them are in the developing world, where household Internet penetration has reached 28 per cent. In the developed world, 78 per cent of all households are connected to the Internet. Europe and Africa are the regions with the highest and the lowest levels of household Internet penetration respectively: 77 per cent in Europe compared with 7 per cent in Africa" (ICT facts and figures 2013).

Table 3 Growth Rate of Mobile Broadband

Regions			
	Subscriptions (million)	Penetration (percentage)	CAGR (2010-2013) (Percentage)
Americans	460	48	28
Europe	422	68	33
CIS	129	46	27
Arab States	71	19	55
Africa	93	11	82
Asia Pacific	895	22	45

Source: ITU World Telecommunication /ICT Indicators database/ICT facts and Figures 2013[20].

If we compare the three tables, one fact becomes clear that Europe in general and EU in particular has been increasing its stake in the cyberspace compared to other regions. According to Table-3 three, in contrast to the developed countries, the developing world has been acquiring more places in the virtual world: Africa has the highest CAGR (82%). But, as far as bandwidth and the price of the internet is concerned there is a huge *digital divide*[21][22] between the regions. Whereas the Europe has to pay less with high speed (i.e. minimum 10Mbit/s), on the contrary Africa has to pay more with low bandwidth (i.e. least 2Mbit/s) (ICT fact and figures 2011, 2013). For cyber-security *per se,* the Union has been working proactively after the Estonian incident. In fact, it is worthwhile to have a look on the Estonian incident because it is technically an eye-opener for the EU to formulate and implement policies to mitigate problems in the cyberspace. Simultaneously societal security has been scrutinised which in the other way lead to the backlash.

3.4. <u>The Cyber Attack on Estonian</u>

The Estonian Cyber-attack took place in 2007 allegedly by some Russian hackers (believed[23]). Later investigations have found some rationale for such an action by the Russians. First, Estonia was a satellite country of former USSR, but after the disintegration it had joined both the NATO and the EU. Simultaneously, it implemented policies designed to minimise the Russian influences in Estonia (Herzog 2011: 50). Second among the reasons is the augmented ethnic tension between the two groups, i.e. the Estonians and the Russian minorities. Last but not the least, was the action of Estonian Government on April 30, 2007, to move 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 comprised 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 ethnic identity. As Mary Kaldor (2004) and David Szakonyi (2007) argued, a perceived attack on the identity of a subordinate group is

[21] The gulf between those who have ready access to computers and the Internet, and those who do not. http://oxforddictionaries.com/definition/english/digital-divide, (09/07/2013).

[22] A term used to describe the discrepancy between people who have access to and the resources to use new information and communication tools, such as the Internet, and people who do not have the resources and access to the technology. The term also describes the discrepancy between those who have the skills, knowledge and abilities to use the technologies and those who do not. The digital divide can exist between those living in rural areas and those living in urban areas, between the educated and uneducated, between economic classes, and on a global scale between more and less industrially developed nations, http://www.webopedia.com/TERM/D/digital_divide.html, (accessed 09/07/2013)

[23] Estonian officials like Foreign Minister Urmas Paet quickly accused Russia of perpetrating the attacks but European Commission and NATO technical experts were unable to find credible evidence of Kremlin's participation in the DDoS strikes (http://en.rian.ru/world/20070906/76959190.html, (accessed 05/06/2013).

likely to provoke a nationalist backlash, as occurred in Estonia. In addition to rioting and violence from April 27 to May 18, 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).

After the major attack in 2007, the Estonian government came up with many preventive measures, such as "Cyber Security Strategy for 2008–2013, Knowledge-based Estonia- Estonian Research and Development Strategy 2007–2013 and 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 emphasised two things: protection of national resources simultaneous with the accomplishment of taking the fight against cyber crime to the international/global level. "The asymmetrical threat posed by cyber attacks and the inherent vulnerabilities of cyberspace constitute a serious security risk confronting all nations. [...], (so it) needs to be addressed at the global level". "[...] such attacks pose a threat to the *international security.* It reached new heights in 2007 owing to the first-ever co-ordinated cyber attack against [...] Estonia [...]. The recurrence and growing incidence of cyber attacks indicate *the start of a new era in which the security of cyberspace acquires a global dimension* and the protection of critical information systems must be elevated, in terms of national security, on par with traditional defence interests"(Estonia cyber security strategy 2008). Indeed, the government of Estonia has focused on four major areas - "application of a graduated *system of security measures in Estonia*; development of (its) expertise and *high awareness of information security* to the highest standard of excellence; development of an appropriate regulatory and *legal framework* to support the secure and seamless operability of information systems; promoting international co-operation aimed at *strengthening global cyber security*" (ECSS 2008: 3).

The asymmetric attacks on the Estonian government have created a spill over effect on policy formations of the EU and the member states. The strategy of the French government is very clear: "(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". Likewise every nation should develop the "*capability of public authorities and the [...] society to respond to a major crisis and rapidly restore normal functioning*" (Information Systems Defence and Security Strategy 2011). To ensure security in cyberspace, the French strategy focused on seven areas of action. They are: "*anticipate and analyse; detect, alert and respond; enhance and perpetuate our scientific, technical, industrial and human capabilities; protect the information system of the state and the operators of critical infrastructure; Adapt French legislation; Develop our international collaborations; Communicate to inform and convince*" (ISDSS 2011: 5). Though the Cyber-war is a major worry of the marketplace, "(the) White Paper develops a two-prong strategy: on the one hand, a new concept of cyber-defence, organised in depth and coordinated by a new Security of Information Systems Agency under the purview of the General Secretariat for Defence and National Security (SGDSN); on the other hand, the establishment of an offensive cyber-war capability, part of which will come under the Joint Staff and the other part will be developed within specialised services" (FWPDNC 2007: 12)to become a world power in cyber-defence.

Each country has its own way to define cyber security. In the same way, Germany mainly focused on the protection of critical infrastructure as a major concern of the cyber security mechanism. Because "*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*" (NSCIP 2009: 4). Protection of critical infrastructure is one way forward towards cyber security. Thus, "Germany has, both nationally and internationally, actively addressed matters of critical infrastructure protection" (NSCIP 2009: 3). It sees the "immediate neighbours; the European Union; the G 8 nations; and the NATO" as the major and easily accessible partners in the international level (Cyber Security Strategy for Germany 2011: 5). They have pointed out that "the availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace have become vital questions of the 21st century" and "the break-down of information infrastructures or serious cyber attacks may have a considerable negative impact on the performance of technology, businesses and the administration and hence on Germany's social lifelines" (CSSG 2011: 2). However, CSSG (2011:2) "ensuring cyber security has turned into a central challenge for the state, business and society both at national and international level".

The new millennium has brought with it many threats. Thus, "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 more vulnerable than in 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 attacks is diffused, it challenges the government to protect the freedom and prosperity. Simultaneously, they have to take important steps with the private sector to fight against cyber security. However, the main aim of the UK is to give its citizens a "safe, secure and resilient cyber space" (CSSSUK 2009: 3), and on other hand it has to seize the opportunities to catch the criminals and terrorists.

3.5. The European Union's approach to Cyber Security

> "*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. Even national borders may hinder us more than protect us against challenges which are global in nature and which require responses that are coordinated across sectors, organizations and national borders. The leading roles that information technologies play in modern society have made cyber security essential to the worldwide economy*" (EU cyber-cooperation: the digital frontline 2012: 4).

Ernest B. Hass (1991) has emphasised upon three modes of changes which often come in the life span of an organisation(s) (i.e. international organisation). Those models are: *incremental growth, turbulent non-growth and model of learning (managed interdependence)* (Hass 1991: 92). In this scholarship, the European Union has a precise place whereupon Hass argued that the EU has left its footprints on these three models and has proven to be successful institutions as well as a role model for other international organisations. Since the Euro crisis occurred, many comments have been made regarding the future of the EU, but undoubtedly it can be said that the EU will survive and revive its glory. However, in the era of digital technology, the EU has to take some major steps to reconstruct its image, i.e. multilateral and proactive approach towards threats. Briefly, in the digital realm things shifted smoothly in a greater speed, which is the reason why international actors must act accordingly. Otherwise the new policies would be lacking the tooth to tackle new threats.

The European Union has emerged as a prominent actor in the cyber-domain in terms of E-commerce, connectivity, services, securitization, bandwidth and so on. In addition, the Union is also well aware about the problems confronting the cyberspace:

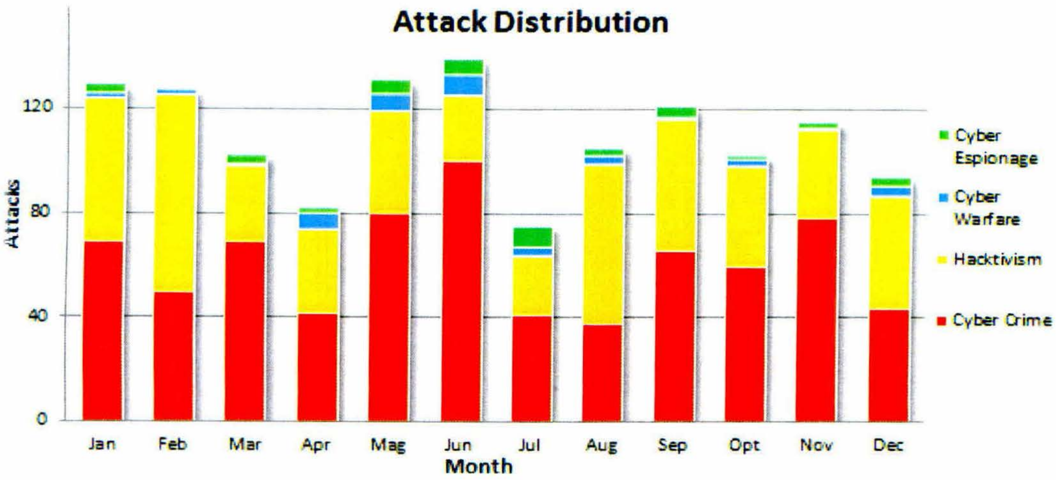
> Information and Communication Technologies (ICT) (i.e. Cyberspace) have provided countless benefits to citizens, businesses and governments, and have reinvented Europe's society and economy. The future of such technologies holds a double edged sword: greater benefits and inevitably, new threats. Very few of us are in a position to appreciate the magnitude of the damaging activities that occur online every day, yet all of us depend inextricably on cyber-space and the multi-dimensional facets it entails. The number and sophistication of cyber-attacks affecting public and private information systems has increased dramatically over the last year, and is expected to continue to grow at a fast pace (EU cyber cooperation: the digital frontline 2012: 4).

'Four decades ago, the Pentagon created the Internet, and today, by most accounts, the United States remains the leading country in both its military and societal use. At the same time, however, because of *greater dependence on networked computers and communication*, the United States is *more vulnerable to attack* than many other countries, and *the cyber domain has become a major source of insecurity*' (Nye 2011: 20). Likewise, the same holds true for the EU in the recent period, the reason is its rising dependency and unpredictable nature of the cyberspace.

3.5(a) Cyber-threats to EU

There are a huge number of attacks that have taken place in the landmass of the EU, and the new technical coinages, such as Cyber-Espionage, Cyber-warfare, Hacktivism, and cyber-crime and so on are increasingly becoming the most talked about terms in the security domain. (More details see Figure-1 and Table-3).

Figure 1: Attack Distribution data for 2012



Sources: EU cyber-cooperation: the digital frontline (ENISA 2012: 11).

Figure 1 shows how different types of cyber-attacks have evolved throughout 2012. It is clear from this data that the majority of attacks fall into the category of cybercrime or hacktivism. In addition, there is a huge number of cases of misuse of the '.eu' domain that have been registered. That has also hampered the safety and security of the EU member states.

> *"Thousands of .eu Domain Names Suspended*
>
> *The European Internet domain name authority, EURid charged with fraud 400 registrars, EU observer reported. EURid suspended 74, 000 .eu domain names, as a result of a thorough system check. The review detected a small number of companies, that had registered several hundred(s) (of) fake others, thus manipulating the system and easily grabbing additional domain names. Their intention was to resell them at a higher price, which is a serious breach with the registrar's contract. The domain name authority has already suspended a number of domains because their owners were unable to prove that they live within the EU. Court proceedings are set to begin in October in Brussels, and EURid hopes that the 74, 000 names laid aside will be made available again for registration by the end of the year. Although EURid announced its 2 millionth .eu registration a few months ago, now they*

fear that the misuse of their services may lower the value of .eu domain names" (Novinite.com 2006).

However, such cases underpin the importance of the cyber-security for the EU and vice versa. To tackle the complex nature of the cyber-attacks, the Union has indentified and defined various terms related to cyber-attacks. Though, these terms have already been defined in the second chapter but here they are being defined again in accordance with the EU's perceptions of these terms. They are as follows:

Table 4 EU definition of Cyber-attacks

Concepts	Definition and explanation
Cybercrime	[Because] cybercrime covers such a broad scope of criminal activities, it is difficult to produce a single definition. Whether using a computer as a tool or as a target, criminality is increasingly present in cyberspace. On the internet the time and place of the crime do not have the same significance as in the physical world. If I am phishing, I can take money illegally from a person's bank account at any place in the world and at any time. This also means that I may find myself in different legal systems. It may be impossible for the prosecution authorities in country A to arrest a criminal in country B. Cybercrime often also allows organised crime to scale up its illegal operations
Cyber espionage	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. In 2012, European security researchers reported that a cyber espionage virus found on personal computers in several countries in the Middle East was designed to eavesdrop on financial transactions and perhaps disable industrial control systems. Researchers at Kaspersky

	Lab, a Russian IT security company in Moscow, identified the surveillance virus, dubbed Gauss, on PCs in Lebanon and other countries in the region and remarked that it appears to have been developed by the same team or 'factory' that built the Stuxnet and Flame computer viruses
Cyber warfare	In the past, troops from opposing countries confronted each other on a battlefield, and the "rules" for warfare were written if not always followed. Nowadays, the line between a soldier, a terrorist and a criminal is often a very blurry one. With Internet technology it is possible for an individual, group or state to carry out remotely controlled, often covert, cyber-attacks on the critical infrastructures of a state. When used as a preventive mechanism, cyber counter-intelligence's role is to identify, penetrate, or neutralize foreign operations that use cyber means as an offensive capability. This includes foreign intelligence service collection efforts, which use traditional methods to measure cyber capabilities and intentions. U.S. Defence Secretary Leon Panetta went as far as saying: "A cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11. Such a destructive cyber terrorist attack could paralyze the nation"
Flame malware	Flame, also known as Flamer, sKyWIper, and Skywiper, is a modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system. The program is being used for targeted cyber espionage in the Middle Eastern countries. Its discovery was announced on 28th May 2012 by MAHER, Center of Iranian National Computer Emergency Response Team (CERT), Kaspersky Lab and CrySyS Lab of the Budapest University of Technology and Economics. The last of these stated in its report that it "is certainly the most sophisticated malware we encountered during our practice; arguably, it is the most complex malware ever

	found". A variant, Miniflamer is even more specialised and tightly targeted, and, as far as is known, has only been used against 10s or 100s of PCs
Hacktivists	'Hacktivists', such as Anonymous, have carried out cyber-attacks against a number of EU Member States' government websites. The group is also thought to be responsible for cyber-attacks on the Pentagon and the News Corp media group, and has also threatened to destroy Facebook. In late May 2012 alleged Anonymous members claimed responsibility for taking down a website about genetically modified crops. In early September 2012 they claimed responsibility for taking down GoDaddy's Domain Name Servers, affecting small businesses around the globe. The evolution of online protest in the name of "e-Democracy" is taking cyber threats to a brand new level: a prolific and potentially uncontainable one. Over the past year, hacktivists have been conducting large-scale exploits to infiltrate law enforcement agencies and major companies, and steal sensitive data "for the purposes of embarrassing or damaging" these organizations, according to Ed Skoudis, founder and chief security consultant at In Guardians a vendor-independent Information security consultancy.
Shamoon	The virus is being used for cyber espionage in the energy sector. Its discovery was announced on 16 August 2012 by Symantec, Kaspersky Lab, and Seculert. Similarities have been highlighted by Kaspersky Lab and Seculert between Shamoon and the Flame malware. The virus has been noted as unique for exhibiting differing behaviour from other malware cyber espionage attacks. Shamoon is capable of spreading to other computers on the network through the exploitation of shared hard drives. Once a system is infected, the virus continues to compile a list of files from specific locations on the system, erasing and then sending information about these files back to

	the attacker. Finally, the virus will overwrite the master boot record of the system to prevent it from booting. 30,000 computers were affected in Saudi Arabia's state oil company and a Qatari gas firm, as Shamoon wiped files replacing them with images of a burning American flag.

Sources: EU cyber-cooperation: the digital frontline (ENISA 2012: 6-7 and 11-12).

These terms denote what is just the tip of the iceberg. A huge number of virues, malwares and agents of cyber-warfare are produced in the marketpalce everyday. They are capable of breaking into nations, individuals, and organistions through all barriers and barricades of protection. Thus, cyber-security has emerged as a mutifaceted term in the landscape of security. The EU defines it as:

> Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems and the totality of transmitted and/or stored information in the cyber environment. This refers to the protection of information, information systems, infrastructure and the applications that run on top of it from those threats that are associated with a globally connected environment (EU cyber-cooperation: the digital frontline 2012: 6).

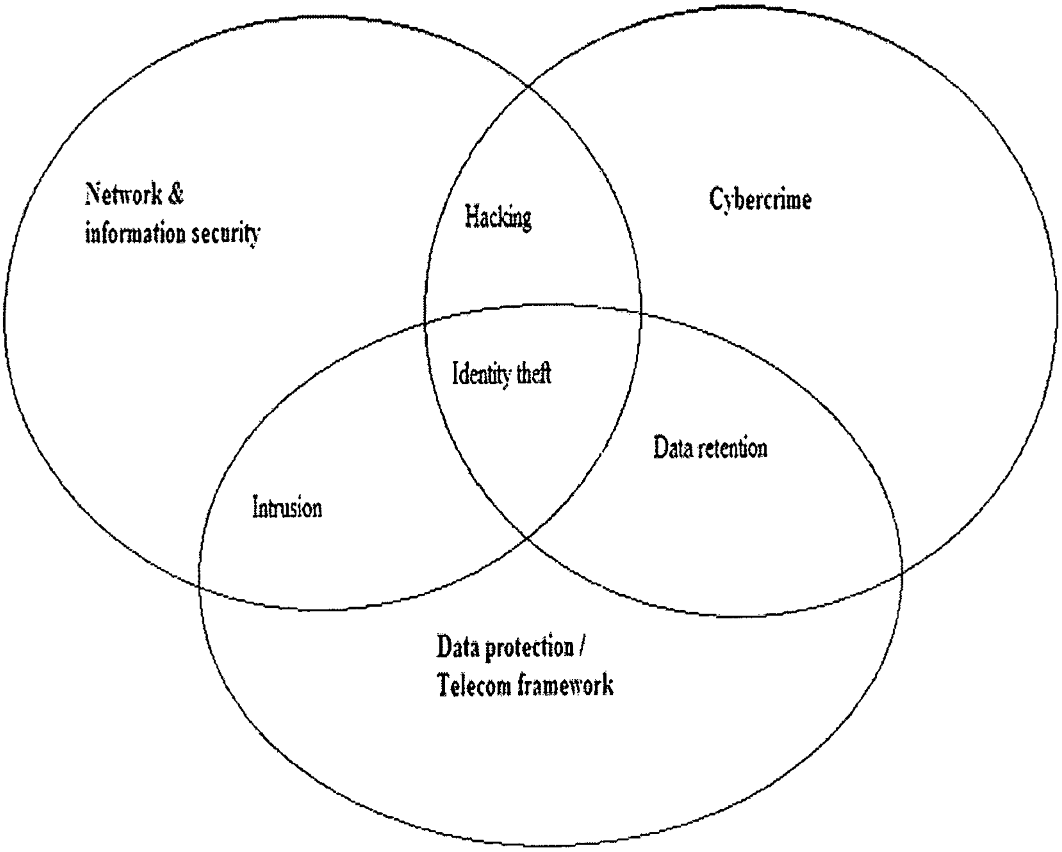
Undeniably, cybersecurity has emerged as the prime agenda in the realm of security of the European Union, which needs to be analysied. Cybersapce per se had emerged as a business domain for the Union but it later got a new mometum towards security landscape of EU.

3.5(b) EU and Cybersecurity

"Cybercrime hides behind our computer screens and in the wires of global communication networks and services" (The European Research Commissioner Philippe Busquin 2003)

The European Union paved the way for mass movement in cyberspace at the end of the1990s, which was largely for better accessibility, consumerism and to open the market through internet. Likewise, protection of the internet-ecosystem and promotion of business was the prime agenda, and that was the reason the Union implemented a policy in 2000 to speed up the E-commerce and consumerism (see 3.3). In 2001 the Commission adopted a new policy to tackle the risks of the digital realm, i.e. '*Network and Information Security: Proposal for a European Policy Approach*'. In fact, it has outlined the importance of security for ICT and vice versa, and on other hand it also illustrates the correlation between the telecommunications, cyber-crime and data protection. The diagram bellow shows the interrelation between the policy sectors of these three.

Figure 2.2: The correlation between the telecommunications, cyber-crime and data protection



Sources: Network and Information Security: Proposal for a European Policy Approach, (Commission of the European Communities 2001: 3).

The Commission has argued that security is a key priority as well as challenge for the policy makers. Conversely, adoption of adequate policy response is becoming an increasingly complex task. It also advocates for various things, viz. rising awareness; strengthening the cooperation between the Union and the MS to fight against cyber-risks and on the other hand to develop the credibility of the CERTs, 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).

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. To tackle such kind of scams the European Commission's Joint Research Centre (JRC) has developed 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 identify, secure, integrate and present electronic evidence on on-line criminal offences. It meets the challenge of clearly establishing what happens during an e-crime, or even during a simple online transaction. 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. In fact, 'this project enables the EU in collecting, analysing, storing and presenting electronic evidence against claims of fraudulent transactions, computer hacking and viruses, as well as other high tech crimes' (THE 2003). Four kinds of law enforcing mechanisms have been developed under this project, viz. *Cyber-Crime Advisory Tool (C*CAT), legal advisor, XML-based specification and demonstrator* for the protection of the cyber-ecosystem of the EU. The Commission has proposed to establish a pan-European network security agency called the European Network and Information Security Agency (ENISA) (see 3.5c further information). Prior to the establishment of the ENISA there was the e-Europe strategy from 1998 to 2002. It was basically an EU wide telecommunications policy.

> "[It was a successful] telecommunications policy which has created essential conditions for an inclusive information society in Europe: First, EU businesses and citizens must have access to a world class, seamless communication infrastructure.... [Simultaneously to formulate a] knowledge based economy. Second, EU businesses - in particular SMEs - and citizens must enjoy affordable access to the Internet... [Equally that will mitigate the] digital divide between the info-rich and the info-poor. To achieve this, e-Europe fully integrates two key commitments: Achieve greater competition in local access networks by the end of 2000 and create a fully integrated and liberalised telecoms market by the end of 2001" (Liikanen 2000: 2).

This policy has paved the way for three things, viz. adopting the framework, boosting internet penetration, securing user rights and privacy (Liikanen 2000: 5-6). Subsequently, in 2002, the Commission endorsed the e-Europe 2005 at the Sevilla Summit (it is the successor of the e-Europe 2002). This has largely covered the EU level mechanisms to assist member states in raising awareness on security issues and simultaneously securing the exchanges of information between the public services. It also gave an overall picture of cyber-security (Liikanen 2003: 2). The e-Europe 2005 has aims to improve the benchmark of *Modern Online Public Services,* viz. e-governance, e-learning, e-health, dynamic e-business, secure information infrastructure and wide broadband accessibility by the end of 2005. Mid-term review of this strategy came in 2004. It added two new things to it: security (i.e. to reduce the fear among the citizens in online buying) and e-inclusion[24]. Viviane Reding (2003: 2) argued in favour of the Union and the influence that the Internet Governance and the Internet have in today's world and of the need for common understandings between the main stakeholders. In particular, Europe agreed on the need for ensuring better and active participation of all parts of the world in decisions on crucial issues: the domain name system, IP addresses, further DNS issues or security problems (spam, spy ware, etc.). It is indeed fully legitimate that governments want to ensure that appropriate answers are given to the issues of cyber-crime, SPAM, intellectual property rights and development objectives. Furthermore, it is in everybody's interest that all countries in the world feel committed to common basic principles on the

[24] E-inclusion is a horizontal concern for all areas of *e*Europe 2005. In particular, a greater focus is needed on the establishment of European network accessibility standards, on web accessibility initiative (WAI) guidelines and common labelling for accessible web pages. Multi-platform access (via PC, digital TV, 3rd generation mobile telephones, etc.) must be promoted to improve accessibility for excluded groups and disadvantaged regions

Internet, and there should be a room for better exploitation of the potential of public–private partnership in the Internet governance (Reding 2005: 2).

In 2005 the Commission came with a new strategy, the *'i2010 – 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 into the threshold. It is the successor of both the e-Europe 2002 and the e-Europe 2005, and an integral part of the Europe 2020. It contains three major objectives:

> Objective 1: A Single European Information Space offering affordable and secure high bandwidth communications, rich and diverse content and digital services. Objective 2: World class performance in research and innovation in ICT by closing the gap with Europe's leading competitors. Objective 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 underpinned the need of 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.

> Speed: faster broadband services in Europe to deliver rich content such as high definition video. Rich content: increased legal and economic certainty to encourage new services and on-line content. Interoperability: enhancing devices and platforms that "talk to one another" and services that are portable from platform to platform. Security: making internet safer from fraudsters, harmful content and technology failures to increase trust amongst investors and consumers (Commission of the European Communities 2005: 4-5).

It has added more tooth to the Lisbon strategy 2000. In 2006, the Union formally came 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.

The first half of 2007 turned out to be a shocking period for the European Union, with the massive cyber-problem in Estonia. The EU came out of its comfort zone to secure the cyberspace in a pragmatic manner and "*To improve and facilitate coordination and cooperation between cyber crime units, other relevant authorities and other experts in the European Union; to develop a coherent EU policy framework on the fight against cyber crime; to raise awareness of costs and dangers posed by cyber crime*" (European Commission 2007b). A large number of patch work viz. allocation of fund for freedom, justice and security for the time period 2007-2013, this fund will be expense on three grounds: security and safe guarding liberties, fundamental rights and justice, and solidarity and management of migration flows (European Commission 2007a) was carried out in the Union to tackle the disastrous nature of cyber-crimes. In the context of European security, Franco Frattini, the European Commissioner responsible for justice, freedom and security, said that "the changing nature of security threats requires a strong public-private dialogue in security research and innovation" (Frattini 2007).

The European Union became more resilient after the Estonia cyber-attack. In 2007, the Union has drawn the attention towards the criticality of the cyberspace in a more vigilant and lucid manner. The Commission defined cyber-crime as such:

> "the term cyber-crime is applied to three categories of criminal activities: traditional forms of crime such as fraud or forgery, though in a cyber crime context relates specifically to crimes committed over electronic communication networks and information systems (hereafter: electronic networks); publication of illegal content over electronic media (i.e. child sexual abuse material or incitement to racial hatred); crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking" (Commission of the European Communities 2007: 2).

In November 15-16, 2007 the EC organised an EU level expert meeting to fight against cyber-crime. The main motive of this gathering was to adopt a general 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. The meeting consisted of three sessions, whereupon issues, such as promoting member states' best practices in combating cyber crime and identifying actions required to improve *cross-border law enforcement cooperation* were discussed. Both the second and third sessions, also attended by private sector and international stakeholders, examined in detail the extent to which common principles of public private cooperation and private sector coordination are essential in tackling issues as different as on-line sexual abuse of children and attacks against information systems (European Commission 2007c). In fact, the Commission wanted to develop the cross border-cooperation to fight against the cyber-crime. The Commission also identified eight major areas of the problem:

> "growing vulnerability to cyber crime risks for society, business and citizens; An increased frequency and sophistication of cyber crime offences; A lack of a coherent EU-level policy and legislation for the fight against cyber crime; Specific difficulties in operational law enforcement cooperation regarding cyber crime, due to the cross-border character of this type of crime, the potential great distance between the crime perpetrator and the crime victim and the extreme speed with which crimes can be committed; A need to develop competence and technical tools (training and research); The lack of a functional structure for cooperation between important stakeholders in the public and the private sector; Unclear system of responsibilities and liabilities for the security of applications as well as for computer soft- and hardware; The lack of awareness among consumers and others of the risks emanating from cyber crime" (Commission of the European Communities 2007: 2).

Connect with Respect (i.e. Safer Internet Day), a project in which 30 European countries are a part of, is co-funded by the European Union and celebrated in more than 70 countries. In 2009, through this programme the Union brought a new policy for the protection of the online-child rights. The main aim was to empower teenagers to deal with potential risks they may face while they are online, like cyber-bullying, revealing of personal information, etc. The Commission through an agreement tied up with 17 leading web firms[25] to improve the security and safety of the teenagers who use social networking sites (European Commission 2009a). The Commission also agreed with the growing importance of the social networking sites because it has turned into a social and economic phenomenon, attracting 41.7 million regular users in Europe, and changing the way we interact with each other on the Web. The use of social networks has grown over the past year by 35% in Europe and is expected to

[25] These include Arto, Bebo, Dailymotion, Facebook, Giovani.it, Google/YouTube, Hyves, Microsoft Europe, Myspace, Nasza-klaza.pl, Netlog, One.lt, Skyrock, StudiVZ, Sulake/Habbo Hotel, Yahoo!Europe, and Zap.lu.

grow to 107.4 million users by 2012[26] which is more than double. This also prevents the underage-child, i.e. bellow age 13 to have access to social networking sites. On the other hand the agreement also ensured that private profiles of bellow18 users should not be searchable. It is one of the concrete moves in this direction. However, in March 2009, The Commission adopted a resolution on Critical Information Infrastructure Protection: '*Protecting Europe from large scale cyber-attacks and cyber disruptions: enhancing preparedness, security and resilience*' setting out a plan (the 'CIIP action plan') to strengthen the security and resilience of vital ICT infrastructures. In fact, the aim was to stimulate and support the development of a high level of preparedness, security and resilience capabilities both at national and the European level. This approach was broadly endorsed by the Council in 2009. The CIIP action plan outlined five pillars: preparedness and prevention; detection and response; mitigation and recovery; international cooperation and criteria for European Critical Infrastructures in the field of ICT. It sets out the work to be done under each pillar by the Commission, the Member States and/or industry, with the support of the European Network and Information Security Agency (ENISA) (European Commission 2009, 2011).

3.5(c) The EU's Strategy for Cyber Security

Since 1997 to till the attack on Estonia, the Union had formulated many policies without experiencing any vulnerability, but in 2007-08 a series of incidents[27] took place within as well at the doorsteps of the EU which turned the Union's priority towards becoming more resilient towards cybersecurity issues. In 2008, the review of ESS included cybersecurity as a major threat in the globalised world. 2009 onwards, the Commission has started to protect Europe from cyberattacks and disruptions actively. In this regard the Commissioner for Information Society and Media Viviane Reding said:

> The Information Society brings us countless new opportunities and it is our duty to ensure that it develops on a solid and sustainable base. 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

[26] http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205401014_text, (accessed 20/10/2012)

[27] The series of incident is referring to the Cyber-attack on Estonia 2007, Lithuania 2008, and Georgia 2008.

> critical information infrastructures. There must be no weak links in Europe's cybersecurity (European Commission 2009b)

She also 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). In fact, one month long internet interruption in Europe or US would mean economic losses of at least 150 billion euros (Reding 2009). All together the Union needs a 'Mister Cybersecurity' like 'Mister Foreign Affairs', a security tsar 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). In her speech in 2009 she argued that future's internet must preserve openness, with right governance principles alongside wide internet availability, security and investment in research and innovation (Reding 2009).

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, Europe of justice, Europe that protects, Access to Europe, Europe of solidarity and Europe in a globalised world. This strategy has aimed to protect the rights and promote justice among the Europeans both vertically and horizontally[28] 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 immorality[29]), and the promotion of EU solidarity and single policy approach simultaneously in the global level. This strategy termed cyber crime as a new modern crime, and it 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

[28]Rights of the children, minority groups and victim of violence; simultaneously promotion of democracy and justice in the landmass.

[29] Sexual abuse, child pornography, sexual exploitation of children.

same time it insisted that both the Union and the MS develop transparency in tackling the criticality of cybercrime.

The Union hosted the EU-US summit 2010 in Lisbon, whereupon both global powers with their high representatives discussed various issues, such as global economy, terrorism, energy security, environmental issues and bilateral-ties inter alia with cybersecurity. In the discussion they portrayed cyber-attacks as a global threat which cannot be tackle single headedly. The transatlantic relationship is irreplaceable and acting together, the European Union and the United States can be a formidable force for good in the world (ESS 2003: 13). A large amount of cyber-exercise took place in 2010, such as the formation of the Digital Agenda for Europe (DAE), empowerment of ENISA and building an atmosphere of trust within and outside the landmass to fight against Cybercrime and so on. Digital Agenda for Europe is a pan-European digital policy which aims to stimulate the accessibility and to make Europe a powerhouse of smart, sustainable and inclusive growth on the global stage. It has 104 actions and seven pillars: Digital single market; interoperability and standards; trust and security, fast and ultra fast internet access; research and innovation; enhancing digital literacy, skills and inclusion; ICT-enabled benefits for EU society. Neelie Kroes is the present commissioner for digital agenda.

In 2011 the EC adopted a new strategy on Critical Information Infrastructure Protection. The main aim of the report was to deal with the critical cyber threats on CII and secure the infrastructure from being harmed. The report was entitled '*Achievements and next steps: towards global cyber-security*'. This report can be considered basically as the successor of the 2009 policy of the Commission. It also outlined the critical and global nature of cyber-threats. This policy gave a way forward to stimulate global cooperation because 'a single handed European approach is not sufficient to address the challenges ahead' (European commission 2011c). In fact, the challenges ahead are neither specific to the European Union, nor can they be overcome by the EU on its own. The pervasiveness of ICT and of the Internet allows more efficient and effective economic communication, coordination and cooperation among stakeholders, which results in a vibrant ecosystem of innovation in all fields of life. However, *threats can now 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 ICT. Widespread and massive use of ICT by all segments of society has increased the risk of vulnerability to a greater extent. Thus, the global community needs to devise strategies to prevent, counter, mitigate and react to these risks appropriately and effectively (European Commission 2011a: 4). The Commission also underlined the growing importance of cyber-warfare and cyber-terrorism as an evolving threat scenario in the marketplace. This document emphasised on a two-fold approach, viz. promotion of principles for the resilience and stability of the internet; pan European cyber-mechanism on the one side, and on the other, building strategic international partnership (i.e. US and G8) inter alia with the European coordinated efforts in the international fora and discussions on enhancing the security and resilience of Internet (European Commission 2011a: 6).

In the second half of 2011, two major incidents took place in Europe, viz. the devastating terrorist attack on Norway in July by a right-wing extremist organisation and in August public authorities of the UK seized 1.2 tonnes of cocaine in a record haul. Therefore, the Commission drew major attention towards the Internal Security, and envisaged EU's need for better tools to fight crime, terrorism and extremism along with cyber-crime (European Commission 2011c: 1). Across the EU, cyber attacks increasingly wreak havoc on public and private computer systems. These are stark reminders of the importance of taking actions to counter threats to internal security (EC 2011c). In this regard Cecilia Malmström, the EU Commissioner for Home Affairs said: "The attacks in Norway earlier this year made it strikingly clear that our societies are facing security threats that are growing in scale and sophistication. No single member state can respond to these threats on its own – we have to work together to achieve our security objectives, and to respond in an effective way to the concerns European citizens are expressing about their security" (EC 2011c). The Commission also made a statement that the recent developments in the EU's neighbourhood, including the overwhelmingly positive democratic developments of the Arab Spring, had created considerable revolution movements by the people which in turn could put pressure on the EU's external border, and in some cases, could create conditions for increased criminal activities (EC 2011c).

In November 2011, for the first time, a transatlantic cooperation came in place to accelerate their cybersecurity exercise. It was held in Brussels, 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" (EC 2011b), using simulated cyber-crisis scenarios were conducted to explore how the EU and US would come together and cooperate in the event of a cyber-attack on their critical information infrastructures (ENISA 2011). Example of co-operation like the 'Cyber Atlantic 2011' was one of the commitments on cybersecurity by the two Atlantic friends during their last summit in 2010, whereupon they had agreed to establish an EU-US working group on cybersecurity and cyber-crime. It has a four point agenda: cyber-incident management, public-private partnerships, raising awareness and fighting cybercrime.

So far the developments in the field of cybersecurity were only across the EU but for the first time it moved towards other side of the Atlantic. It was obvious for both the partners – EU and US to take such joint action to securing the digital realm.

The Commission strengthened the EP3R[30] in 2012, which was a part of the 2009 strategy to protect critical information infrastructure. Its other core institutions (those fighting for cyber-security and resilience) i.e. ENISA, EUCERT, DAE, and EUROPOL were also fortified. On 30th January, 2012 Neelie Kroes the Vice-President of the European Commission responsible for the Digital Agenda, in her speech emphasised upon public-private co-operation in cyber-security. She said that the transformative change in the digital realm (i.e. internet) 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, if the Internet is not secured, nothing will be. The digital ecosystem boosts productivity, drives innovation and stimulates growth and high-quality jobs. In future, it will not just be a tool for social interaction and economic transaction but will encompass more and more services, health and social care, education, transport and energy grids (Kroes 2012). Therefore, a resilient and smooth Internet is essential to a stable and growing economy. At the same time, threats are growing. Number of attacks is going up and the attacks have become more

[30] European Public Private Partnerships for Resilience

frequent and more serious. Anyone can be an attacker, from those doing it for publicity or notoriety, to those involved in organised crime, spying or outright warfare (Kroes 2012). Thus, "we all need to take responsibility of dealing with this issue and to act strategically, to give it attention at the most senior level and to work together. That includes the public and private sectors co-operating" (Kroes 2012). The private sector owns or controls the majority of ICT infrastructure and is home to nearly all the ICT expertise. No plan for cyber security can ignore this fact. Sometimes we need to share information on threats, on risks, on vulnerabilities, "sometimes that information is sensitive... But, we need to be able to exchange good practices and provide each other with solutions" (Kroes 2012: 2). Kroes (2012) mainly emphasises on three major aspects to strengthen and fortify the EP3R: exchange and act on information about the cyber-incidents and cyber-attacks; stimulating efforts from private sectors to improve security, with adequate incentives and awareness and investment on innovation for security technologies. The Union along with the Commission proposed to have a European Cybercrime Centre (EC3) by 2013. The main aim of the centre would be to 'serve as a focal point for European cybercrime information, pool European cybercrime expertise to support Member States, provide support to Member States cybercrime investigations and become the collective voice of European cybercrime investigators across law enforcement and the judiciary' (ETW 2003).

On October 4, 2012 in a conference on cyber security at Budapest, the High Representative of EU, Catherine Ashton pointed out that 'cyber diplomacy' will have to be carried out continuously following the same path as the London Conference in 2011 (Nov 1-2 on cyberspace), where many inputs have come from the governments, business groups and civil societies to ensure a free and open cyberspace. Indeed, "internet began as a way of linking different computers over the phone networks, but it now connects billions of users worldwide forum wherever they happen to be via portable or fixed devices. People with no access to water, electricity or other services may have access to the internet from their mobile phone (OECD Internet Economic Outlook 2012). However, "the benefits of the Internet go far beyond its direct economic benefits. … (And) the worldwide connectivity has the potential to serve as a catalyst for many positive global developments, from the reduction of poverty to education and of course greater access to information. It is one of the most powerful agents for change, growth and jobs everywhere, but its impact is particularly forceful in the developing world. The Internet supports learning efforts in remote villages, provides information for innovators and empowers women and girls in developing societies" (Ashton 2012). Not only developing societies but also the developed societies of the Europe have to control the proliferation of cyber threats before becoming more vulnerable. Thus, "cyber-security is a priority for Europe's welfare and competitiveness" (European Commission 2012c).

A large amount of rhetoric has taken placed in 2012, and most of them were related to four things: protection of children; e-commerce and privacy in digital age; strengthening the cyber-security mechanisms- both EU and MS, formation and development of greater cooperation between all stakeholders and strengthening the securitising products (public, private, and research institutions) and global cooperation. On the other hand ENISA has performed its duty extensively in 2012 and produced a large amount of documents in response to cybersecurity. It became more active and more responding towards the cyber risks than before.

3.5(d) European Network and Information Security Agency

On 10 February, 2003, the Commission proposed to establish a European Network and Information Security Agency. The reason is the growing importance of the ICT in today's society... [and] a great deal of dependency on networks and information systems. [In fact] network security has become a key concern, especially in the aftermath of the 11th of September. The malfunctioning of networks and information systems concerns everyone alike- citizens, businesses and public administrations (Liikanen 2003). Therefore, on 10th march, 2004 the Commission through the Regulation No.460/2004 of the European parliament and of the council established the European Network and Information Security Agency. It became fully operational only on 1st September, 2005. Dr. Udo Helmbrecht is its present director. The main aim of ENISA is to develop a culture of network and information security (NIS).

> About ENISA:
>
> The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Since 2005, ENISA has been running a programme dedicated to the reinforcement of national and governmental CERTs. The goals of this programme are to support the member states of the EU in establishing and developing their national and governmental CERTs according to an agreed baseline set of capabilities, and to generally support and reinforce CERT co-operation by making available the good practices. ENISA seeks to reinforce this type of co-operation by analysing barriers to cross-border co-operation and proposing measures to tackle them (ENISA 2012: 21). But, it got a fresh momentum after the Estonian Crisis in 2007. In 2008 the ENISA released a document in favour of child protection which was entitled: '*Children on Virtual World and what Parents should know*'. Basically, it gave emphasis on parents (and guardians) responsibility towards the children's need and security in the digital realm. The ENISA concluded that:

> In today‘s world, virtual world sites for children are hugely popular and have become a compelling activity for many internet users. The spectrum of functionalities available, new technology, low fees and the social aspect related to these games are some of the reasons why their use has increased enormously. Children sometimes encounter dangerous situations in virtual worlds just as they do in the real world, leaving parents naturally concerned about how their children are using and acting in the virtual worlds. Although there is increasing awareness of the risks related to the insecure use of virtual worlds, there is still a significant amount of work to do. It is therefore crucial that parents are able to decide, with their child, what is appropriate and safe for their use, as well as how to behave responsibly in the virtual worlds. Working together, parents and children can reap the benefits available in these virtual worlds, whilst minimizing the possible dangers (ENISA 2008: 34).

ENISA has released a huge amount of policy documents and recommendations for the European Network and Information Security, such as the

Cyber Europe 2010[31], the European Cyber-security Month (it is a pilot project across Europe which started in 2012, and it contains the slogan i.e. be aware be secure) and the Cyber Europe 2012. On the other hand, it also guides and assists risk management, protection against online bullying and protection of critical infrastructures. 2010-2012 was the busiest period for ENISA because a lot of work was done to mitigate the destructive nature of cyber-threats.

Contribution, Achievements and Drawbacks of ENISA

Contribution

It has been stimulating and helping both the government and private sectors across the EU in building resilience to tackle the risks. The main contributions of ENISA in enhancing cyber security are in the following areas: identification and analysis of emerging trends and threats; awareness of network and information security risks and challenges; early warning and response; critical information infrastructure protection; adequate and consistent policy implementation; supporting other community actors in actions against cybercrime; international cooperation; information exchange; building communities (ENISA 2012: 9), and now also in enhancing the mechanisms to mitigate the cross-border problem.

Achievements

It has achieved many milestones since its inception as a prime agency of the Union to address the cybercrime and cyber-security. In 2012 it entered into a different phase altogether, because it achieved a bigger co-operation between the EU institutions and the MS cyber-security mechanisms. In fact, ENISA's recent achievements in co-operation include: managing Europe's biggest ever cyber security exercise, Cyber Europe 2012, involving all member states of the EU and countries from the European Free Trade Area (EFTA); taking a formal role in Europe's Cyber Incident Reporting framework, under Article 13a of the EU's Telecommunications Framework Regulation; responding quickly and efficiently to the member states' requests for assistance through ENISA's Athens-based Mobile Assistance Team

[31] It was the first ever pan European cyber-security exercise organised by EU Member States (MS), facilitated by the European Network and Information Security Agency (ENISA) and supported by the Joint Research Centre (JRC). The objective of the exercise was to trigger communication and collaboration between countries in Europe to try to respond to large-scale attacks.

(MAT); helping to establish new Computer Emergency Response Teams (CERTs) in Malta, Romania, Cyprus and Ireland, as well as on-going support to established teams (ENISA 2012: 5).

Despite its many contributions and achievements, there are certain shortcomings to ENISA.

Criticisms

There has been certain drawbacks in the ENISA which have been disabling it and posing a problem to its smooth and efficient functioning. First, its location on Crete, a distant island, 1,500 miles (2,500 kilometres) from Brussels, makes it hard to attract qualified IT personnel (Euro Wire 2011). Second, the strength of its staff members is a mere 65, which is an exceptionally small number of people in comparison to the breadth and span of its programs and responsibilities (Euro Wire 2011).

3.6. Conclusion

The *'Special Eurobarometer 371 on Internal Security'*, has outlined that the Europeans live in *relative safety,* but the challenges to peace and security are ever increasing. Many of these challenges, including the risk of *terrorism and cybercrime*, are 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 five key challenges of present society: terrorism, organised crime, natural and manmade disasters, *cybercrime* and security of EU borders are important, and many believe that they will grow in the next three years, the Union is slow to put together it cyber-security policies. Moreover, cybercrime is seen as a challenge most likely to increase in the next three years (Eurobarometer 2011: 8)

It is necessary for the EU to alleviate the pain of cybercrime. An analysis of the EU's *actorness* in the landscape of cybersecurity shows that it is neither far nor easy to confirm someone as an actor in the realm of digital age, because the virtual world is a melting pot with high risks of vulnerability. At the same time, most countries which have sophisticated IT are more prone to attacks. Although, developments in EU prowess to mitigate the risks have taken place by leaps and bounds, it still needs to more powerful in the global front. In fact, presently both the EU and the ENISA and other allied organisations have been putting in their maximum to tackle these problems. However, there is some uniqueness in EU's approach. First, it has been trying to build a harmonious environment through the P3 and EP3R approach. Second, the EU-US approach to fight against cybercrime. Last but not the least, EU's proactive approach to protect its Cyber domain. Eventually, the Union has adopted a detailed strategy to against cyber-threats in 2013 called 'Cybersecurity strategy of the European Union: an open, safe and secure cyberspace'.

CHAPTER 4

CONCLUSION

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffered a defeat. If you know neither the enemy nor yourself, you will succumbed in every battle [Sun Tzu, Art of War 1913]

Cyberattacks have tactical and operational implications, but do not have strategic ones (at least not yet). Someday, they might lead to widespread damage and destruction but, for now, they are most effective in distorting and manipulating the perceptions of decision makers. (Libicki 2007)

Cybersecurity is the new non-traditional threat which makes states and societies vulnerable and this has lead to the securitisation of the cyberspace. The governments have shown greater willingness to employ large number of security mechanisms in the cyber domain to protect their strategic assets. The issue of cyberspace and cyber threats has been transformed from a politicised into a securitised problem. Likewise, the cyberspace has also become a part of the non-traditional security paradigm and therefore, security of the cyberspace is an urgent priority. Not all the actors shares the same perspectives to justify the objectivity of the threats, rather have agreed on the urgency of the subject matter. In this new podium both government and private sectors have to come together to take a focal position to mitigate the menace of the cyber-threats. Thus, effective cybersecurity requires that national governments, private companies, IT experts, academia, and non-governmental organisations work together to understand threats in cyberspace and to share information and capabilities for mitigating those threats. This is becoming essential because cyber-ecosystem is an interconnected domain that provides tremendous benefits to the nations, organisations and individuals. The virtual attacks hits the functioning of government institutions, personal data and fundamentally the critical infrastructure, thus the actors needs to strengthen certain things such as: adequate policy formation, execution and implementation; tolerable mechanisms in response to risks and resilience; building and rebuilding of proper vigilant institutions to take proactive measures. Although, proactive action in response to cyber threats appears as a herculean task, due to lack of adequate information about the enemy and simultaneously the cyberattacks have tactical and operational implications and also are effective in destroying and manipulating the perceptions of the policymakers. Apart from cybersecurity, in contemporary geopolitical debates the cyber-war and cyber- warfare became buzz words after the 2007-08 cyber-incidents in Estonia (2007) and Georgia (2008). But most of the scholarly outcomė shows that defining cyber-war is a problem, literally it (war) takes two sides to be at conflict, which is yet to be the case in the cyber domain, even though it possesses all the potentiality like conventional warfare. The problem of cyber threats needs to be addressed through bottom-up approach and that should be put into action by its stakeholders. In this context, the issues of cybersecurity should not be limited to discussions at the top rather that should lead to a greater cooperation, which is yet to come at the global level. Although there are certain exceptions, some improved governmental and semi governmental as well private institutions have come forward to fight against cyber crime. UN agencies like UNODC (United Nation Office on Drugs and Crimes), semi governmental institute like IMPACT (International Multilateral Partnership Against Cyber Threats) and private players like the East West Institute (EWI) have been addressing the issues of cyberspace. The East-West Institute initiated worldwide a summit on cyber-security, which has covered three successive summits in Dallas 2010, London 2011 and in New Delhi 2012, but there needs to be large engagement for greater applicability and security.

National Security versus Freedom of Expression

50 years back there was no internet, 30 years back there was no such word called 'cyberspace', 10 years back present societies so called medium of freedom of expression (i.e. social networking sites like *facebook, tweeter* etcetera) was far from the horizon, but at present, *glocalisation* has diffused the technological and scientific revolution to the individual level, and that has lead to new debate viz. who should control the internet? Why it should be controlled?

In the present geopolitics context with the impact of ICTs, a large number of discussions and debate have been raising issues in the context of freedom of speech versus national security. Contemporary world order freedom of expression has both positive and negative effects and that might bring vulnerability to national security.

Cyberspace is playing a pivotal role for free flow of the information however, the domain itself is prone to threats. The paradox lies between the policy and outcomes. Which one should get the first priority national security or the freedom of speech, perhaps it is difficult to give equal treatment to justice and equality, when national security is threatened. This unpredictable situation challenges policymakers to develop effective policy with respects to cybersecurity.

What should the government do, surveillance or openness; protection of strategic assets or free flow of information.

The EU's position on Cyber security

The structural framework of Cyberspace has based on cooperation and coordination and no stakeholder alone is capable enough to tackle the threats and problems. Neither the US nor the EU or any other national government and international organisations is in a position to take a unilateral stand to shape the global cyber security policy.

The European Union's approach to the cybersecurity issues emerged in late 90s and in 2001 at Budapest, the Council of Europe Convention on Cybercrime. But the EU being a proactive actor in the cyber domain was far from easy during that time.

This research has examined the context (2003-2012) of the EU cyber security policy. It has structured and undertaken primarily within the time frame of 2003-2012, but it has also drawn some attention towards some significant documented policy which had come prior to 2003 i.e. '*Network and Information Security: Proposal for a European Policy Approach*' in 2001; '*eEurope 2002 Impact and Priorities*' in 2001; and '*eEurope 2005: An Information Society for All*' in 2002; along with some other documents which have contained the speeches and opinions of various Commissioners in the context of the cybercrime, cyber threats and cybersecurity. In 2001, the Union had outlined the importance of security for ICT and vice versa and on the other hand it also illustrates the correlation between the telecommunications, cyber-crime and data protection. In fact, it was the corner stone of the EU's cyber security policy. In the post 9/11 period, the EU has taken some substantial measures to address questions within security landscape. The High Representative of Common Foreign and Security Policy Javier Solana in 2003, had come with the agenda '*A*

Secure Europe in a better World' and that formally revealed the role of EU in Non-traditional security landscape. Subsequently in 2005 the Counter Terrorism Strategy had given more strenght to the EU but, till 2008, cybersecurity as a global threat failed to get any place in the major strategies of the EU.

The EU has become keen to develop its cybersecurity mechanisms (only after the Estonian cyber-attacks) and that largely falls under three sectors: greater cooperation between the multi-stakeholders; Public-Private-Partnership (P3) approach for risks management and resilient (i.e. EP3R); and encouraging cybersecurity and cybercrime issues onto the global level. The first two are fundamentally a bottom up approach to cyber threats, through this the Union is aiming to develop a security threshold for risk management and resilience. Whereas the ENISA has emerged as securitising actor in the European cyber domain, it has been facing serious *incremental changes* after the Estonian Cyber-attack. In addition, the ENISA has been putting into operation the European Public Private Partnership for Resilience among the Member States and also successfully completed two major pan- European cyber exercises i.e. Cyber Europe 2010 and Cyber Europe 2012, along with European cyber Security Month (ECSM). However, it is also a part of the EU-US cybersecurity and cybercrime cooperation, and consequently gaining focal position in the EU paradigm. The Union's approach in global level has remained a *prelocutionary act* and that has failed to move beyond the the transatlantic cooperation, indeed international cooperation yet to be furnished to bring coherence among the stakeholders.

There have been certain drawbacks in the EU to formulate a comprehensive approach to cyber-threats, i.e. internal dichotomy, definitional problem, institutional problem, fragmented policy, and lack of law enforcement mechanisms. In a globalised world the core concept of territorial boundary has been eroded and in the podium of the cybersecurity it became irrelevant. *Internal dichotomy*: after the Estonian cyber-crisis a large number of security checks have been developed by the Member States, and subsequently the big three of EU i.e. Germany (2009), France (2009) and UK (2010) along with Netherlands (2011) and Sweden (2009) mainly the IT hub of Europe Estonia (2008) has adopted unilateral cybersecurity strategy to mitigate the threats. This dichotomy has continued till the end of 2012 due to lack of the EU level strategy. *Definitional Problem*: cybersecurity is an umbrella term and along with its allied areas it became more difficult to define. Second, the Union is also facing this definitional deficit that is the reason policies overlapped to define cybersecurity. Third, national governments have certain kind of definition but it falls to draw any attention due to different opinion and orientation. Last but not the least, there is a lack of coherent policy and coordination between the national security, private security, individual security and cybersecurity both at the national and international level. *Institutional problem*: vulnerability is rising in the cyberspace that needs to be addressed with proper institutional channel. But, the EU is lagging behind because, '*Brusselisation* of the EU' underestimates other institutional areas; from above discussion it is clear that the national governments prefer to have their own mechanism to address the threats; and the prime securitising institutions of the EU (CFSP, ESDP etcetera) is far from cyber security issues, and others those meant for cyber security are moving from turbulent non-growth to incremental changes and trying to manage the situations. *Fragmented policy*: one composite policy is much better than thousands of policies. As far as cybersecurity is concerned it needs a composite policy that was missing in the EU policy structure till 2012. The EU is having some allied policies such as: protection of Network and Information System (NIS), CIIP, and risk management but that does not seems as good as a composite cyber-policy. *Lack of law enforcement mechanisms*: it is quite difficult to have a legally binding regime for cyberspace. The virtual space has emerged as the fifth domain but it far from easy to bring it under international jurisdiction. In this context, internet governance became a isue in many public debates. However, the European Union keeps it simple i.e. Open, Safe and Secure cyberspace. The EU has yet to have any strong legal standard for cyberspace, rather it focuses on its institutions like EUROPOL, EUCERT and so on against the cyber-criminals and hacktivists.

This research of the EU's policies on cyber security can be categorised in three phrases viz. '*Resilient EU, Vigilant EU and Proactive EU*' in the landscape of cybersecurity. *Resilient EU*: in post 9/11 scenario the Union had drawn attention mainly towards terrorism, organised crime and state failure, but after Estonia cyber-attack (2007) the Union took the issue much seriously that is the reason in the review of the Security Strategy (2008), it has placed cyber security as a emerging global threat to national security, and the EU became more realistic towards risks management and resilience. *Vigilant EU*: in 2009 there was a large number of *illocutionary act* has taken within EU, to address the nature of the threats; for greater cooperation between the Union and Member States; and strengthening security threshold for future action. *Proactive EU*: incremental changes have taken place during 2010-2012, ENISA got a new momentum viz. to empower the mechanisms, to promotion EP3R, and became a European cybersecurity actor. Transatlantic cooperation was agreed to establish cybersecurity and cybercrime centre after the EU-US summit 2010, Digital Agenda for Europe brought a comprehensive digital policy for the Member States that builds *cloud of trust* between the Commission and Member States. Moreover, on February 7, 2013 the Commission finally adopted the Cyber Security Strategy for Europe.

Way Forward

Now the Union is having a strategy for cyber security, however, the EU has to work on certain areas: International Engagement with non-Member States (i.e. India, Russia, G8, UN and other international actors) for global cyber defence mechanisms; Better Coordination of existing Commission initiatives (it is even underlined in the Cyber Security Strategy 2013); improving the standard of cyber security agenda so that it can have access to CFSP or adding Cyber agenda into the paradigm of CFSP; Trust building both inside (with Member States mechanisms) and outside (non-Member States), because a cyber attack can originate from Ghana, Russia or right next door, sometime it could be your best allies i.e. the US, as was revealed by Edward Snowden that the US has launched a large number of cyber-espionage against the EU and its Member States, in fact it is a earth-shaking news because both have agreed to establish a working group for cybersecurity and cyber crime after 2010 summit, second in 2011 both have conducted day-long table-top cyber exercises i.e. ‘Cyber Atlantic 2011’, prior to this the EU also attained the ‘Cyber Strom’ exercise which is carried out by the Department of Homeland Security (DHS), therefore, in this virtual world trust building is becoming a urgent priority for security; moreover ratification of the Council of European Convention on Cybercrime.

2013 would be the best year for the European cyber-security mechanism, due to the following reasons: first, the Commission has established the European Cybercrime Centre (E3) on January 11; second, the Commission adopted Cyber Security Strategy on February 7; and on July 4 the European Parliament (EP) has adopted a new EU legislation to fight cyber-crime, such as large-scale cyber-attacks, it helps to strengthen the cyber defence mechanism as well as the law enforcement mechanisms.

In this context Cecilia Malmström, EU Commissioner for Home Affairs opines:

> This is an important step to boost Europe's defences against cyber-attacks. Attacks against information systems pose a growing challenge to businesses, governments and citizens alike. Such attacks can cause serious damage and undermine users' confidence in the safety and reliability of the Internet. [I am therefore pleased that] formal approval has been reached on new rules concerning the definition of criminal offences and the sanctions in the area of cybercrime. The perpetrators of increasingly sophisticated attacks and the producers of related and malicious software can now be prosecuted, and will face heavier criminal sanctions. Member States will also have to quickly respond to urgent requests for help in the case of cyber-attacks, hence improving European justice and police cooperation. Together with the launch of the European Cybercrime Centre and the adoption of the EU Cyber-security Strategy, the new Directive will strengthen our overall response to cybercrime and contribute to improve cyber security for all our citizens.

However, this statement shows that the European Union is proactively enhancing its mechanisms to address the issues of cyber-threats, cyber-crime and cyber security.

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 2012, URL: http://europa.eu/rapid/press-release_SPEECH-12-685_en.pdf.

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 2012, URL: http://europa.eu/rapid/press-release_SPEECH-00-316_en.pdf.

Barak Obama (2010), *Cyber security,* The White House, [Online: Web], Accessed 05 January 2013, URL: http://www.whitehouse.gov/cybersecurity.

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

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 2012, 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 2012, 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 2012, 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 2012, 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 2012, 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 2013, URL: http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf.

European Commission (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 2012, URL: http://europa.eu/rapid/press-release_IP-97-313_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.

European Commission (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 2009, 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 2009, Brussels, [Online: Web], Accessed 20 October 2012, URL: http://europa.eu/rapid/press-release_MEMO-09-199_en.pdf.

_____________________ (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), *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 2013, URL: http://europa.eu/rapid/press-release_IP-11-1305_en.pdf.

_____________________ (2011c), *Internal Security: The EU needs better tools to fight Crime, Terrorism and Extremism*, IP/11/1453, November 25, Brussels,[Online: Web], Accessed 20 October 2012, URL: http://europa.eu/rapid/press-release_IP-11-1453_en.pdf.

_____________________ (2011d), *Internal Security, Special Eurobarometer 371*, DG COMM Research and Speechwriting Unit, November, [Online: Web] Accessed 05 June 2013, URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf.

_____________________ (2012a), *Europe this week*, 30 March, Brussels, [Online: Web], Accessed 20 January 2013, URL: http://europa.eu/rapid/press-release_ETW-12-3003_en.pdf.

European Commission (2012b), Europe's Information Society, *Internet Safer Day*, [Online: Web], Accessed 01 July 2013, URL: http://ec.europa.eu/information_society/activities/sip/events/day/index_en.htm.

_____________________ (2012c), *Cyber security Strenghtened at EU Institutions following successful pilot scheme*, IP/12/949, September 12, Brussels, [Online: Web], Accessed 20 January 2013, URL: http://europa.eu/rapid/press-release_IP-12-949_en.pdf.

European Council (2003) *European Security Strategy: a Secure Europe in a Better World*. 12 December. Brussels, [Online: Web], Accessed 05 May 2011, URL: http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.

_______________ (2007), *Lisbon Strategy*, Euro Found 19 March, [Online: Web], Accessed 25 June 2013, 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 2013, URL: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/er/117785.pdf.

_________________ (2013), *Digital Agenda for Europe*, [Online: Web], Accessed 09 June 2013, URL: https://ec.europa.eu/digital-agenda/en/our-goals/international.

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 2012, 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 2013, 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 2013, URL: http://www.enisa.europa.eu/events/enisa-events/enisa-high-level-event-2012/eu-cyber-cooperation-the-digital-frontline/at_download/fullReport.

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 2012, 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 2012, 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 2012, URL: http://europa.eu/rapid/press-release_SPEECH-07-515_en.pdf.

International Telecommunications Union (2010), *The World In 2009: ICT Facts and Figures*, ITU, [Online: Web], Accessed 20 December 2012, 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 2012, 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 2012, 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 2012, 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 2013, URL: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf.

____________________________ (2013), *Percentage of Individuals Using Internet*, ITU, [Online: Web], Accessed 20 June 2013, URL: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls.

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 2012, 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 2012, 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 2012, 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 2013, URL: http://europa.eu/rapid/press-release_SPEECH-12-409_en.pdf.

Ministry of Defence, Estonia (2008), *Cyber Security Strategy,* Tallinn, [Online: Web], Accessed 20 November 2012, URL: http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.

Organisation for Economic Cooperation and Development (2012), *Internet Economy Outlook* 2012 Highlights, OECD, [Online: Web], Accessed 20 January 2013, URL: http://www.oecd.org/sti/ieconomy/internet-economy-outlook-2012-highlights.pdf.

Patten C. (2004), Commissioner for External Relations, *The Western Balkans: The Road to Europe* SPEECH/04/209, 28 April, Berlin, [Online: Web], Accessed 05 May 2013, URL: http://europa.eu/rapid/press-release_SPEECH-04-209_en.pdf.

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 2013, URL: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Republic of France (2010), *Information System Defence and Security – France's Strategy,* France, [Online: Web], Accessed 20 November 2012, URL: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

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 2012, 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 2012, URL: http://europa.eu/rapid/press-release_SPEECH-09-231_en.pdf.

The Council of Europe (2001), *Convention on Cyber Crime,* ETS No. 185, 23 November, Budapest, [Online: Web], Accessed 5 September 2012, URL: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

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.

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.

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.

Annan, K. (2005), "In large Freedom: Decision Time at the UN", *Foreign Affairs*, May/June, [Online: Web], Accessed 05 May 2013, URL: http://www.unis.unvienna.org/pdf/freedom_annan.pdf.

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.

Bindi, F. (2010), *The Foreign Policy of the European Union: Assessing Europe's role in the World*, Washington DC, The Brookings Institutions.

___________ (2010a), "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, [Online: Web], Accessed 05 May 2013, URL: http://www.iar-gwu.org/sites/default/files/articlepdfs/Niloy%20Biswas%20-%20Is%20the%20Environment%20a%20Security%20Threat.pdf.

Biscop, S. and J. J. Andersson (eds.) (2007), *The EU and the European Security Strategy: Forging a Global Europe*, London: Routledge.

Booth, K. (2007), *Theory of World Security*, New York: Cambridge University Press.

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 Inc.

Buzan, B. and L. Hansen (2009), *Evolution of International Security Studies*, New York: Cambridge University Press.

Bretherton, C. and J. Vogler (2006), The European Union as a Global Actor, London, Routledge.

Charney, S. (2012), “Emerging Cyber-Norms Debate: Advancing International Cyber-Security through Strategy and Partnership”, *Europe's World*, Spring 20: 39.

Cavelty, M. D. and V. Mauer (eds.) (2010), *The Routledge Handbook of Security Studies*, London: Routledge.

Cavelty, M. D. (2002), *Information Age Conflicts: A study of the Information Revolution and a Changing Operating Environment*, Zurich, Switzerland: Center for Security Studies.

____________ (2010), “Cyber-threats”, in Myrian D. Cavelty and Victor Mauer (eds.), *The Routledge Handbook of Security Studies*, London: Routledge.

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.

Cooper, R. (2000), *Post-Modern State and the World order*, UK: DEMOS.

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.

Eriksson, J. et al. (2007), *International Relations and Security in the Digital Age,* Abingdon: Routledge.

____________ (2006), “The Information Revolution, Security, and International Relations: (IR) relevant Theory?”, *International Political Science Review,* 27 (3): 221-244.

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.

Filtenborg, 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.

Genachowski, J. (2012), Chairman of the Federal Communications Commission, Commercial Perspectives on Cyber-security, *Georgetown Journal of International Affairs*, Washington D.C., [Online: Web] Accessed 05 June 2013, URL: http://journal.georgetown.edu/wp-content/uploads/209-242-Conference-Panel-31.pdf.

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.

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.

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.

Hansen, L. and H. Nissenbaum (2009), "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly,* 53 (4): 1155-1175.

Hass, B. E. (1991), '*When Knowledge is Power: three model of change in International Organisation*' US, University of California Press. [Online: Web] Accessed 05 June 2013, URL:http://books.google.co.uk/books?hl=en&lr=&id=9iio_YItRNEC&oi=fnd&pg=PR11&dq=when+knowledge+is+power+change+and+challenges+of+international+organizations&ots=M2ZxjuRTL0&sig=82zsyATE6s5wse3T-sKvobnAZy4#v=onepage&q=when%20knowledge%20is%20power%20change%20and%20challenges%20of%20international%20organizations&f=false.

Hathaway, M. (2012), "Leadership and Responsibility for Cybersecurity", *Georgetown Journal of International Affairs*, Special Issue, 71-80. [Online: Web] Accessed 05 June 2013, URL: http://belfercenter.ksg.harvard.edu/files/71-80-hathaway.pdf.

Herzog, S. (2011), "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Respons", *Journal of Strategic Security*, 4(2): 49-60.

Huysmans, J. (1997), "Revisiting Copenhagen, or, About the Creative Development of a Security Studies Agenda in Europe", *European Journal of International Relations*, 4(4):488–506.

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.insaonline.org/CMDownload.aspx?ContentKey=e1f31be3-e110-41b2-aa0c-966020051f5c&ContentItemKey=161e015c-670f-449a-8753-689cbc3de85e.

Islam, S. (2003) Big Bang Expansion of the European Union, 28, Jan, Yale Global Online, [Online: Web] Accessed 05 June 2013, URL: http://yaleglobal.yale.edu/content/big-bang-expansion-european-union.

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, UK: Stanford University Press.

Keohane, R. O. and J. Nye (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.

Kshetri, N. (2010), *The Global Cybercrime Industry*, Springer-Verlag, Berlin Heidelberg.

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.

Libicki M. (2007), *Conquest in Cyberspace: National Security and Information Warfare* London: Cambridge University Press.

March, J.G. and J.P. Olsen (1995), *Democratic Governance*, New York: The Free Press.

Mearsheimer, John 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: W.W. Norton & Company.

Mutimer, D. (2010), "Critical Security Studies", in Myrian D. Cavelty and Victor Mauer (eds.), *The Routledge Handbook of Security Studies*, London: Routledge.

Novosti, Ria (2007), "Estonia has no evidence of Kremlin involvement in cyber attacks," September 6 2007, [Online: Web] Accessed 05 June 2013, URL: http://en.rian.ru/world/20070906/76959190.html.

Nye, J. (2011), "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly*, 5 (4): 18-38.

_________ (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.

Pollitt, M. M. (1998), Cyberterrorism – fact or fancy?, FBI Laboratory 935, Pennsylvania Ave. NW, Washington, D. C. 20535, [Online: Web] Accessed 05 May 2013, URL: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html.

Richardson, J. (2011), 'Stuxnet as Cyber-warfare Distinction and Proportionality on the Cyber Battlefield' [Online: Web] Accessed 05 December 2012, URL: http://globalinvestmentwatch.com/wp-content/uploads/2011/07/Stuxnet-as-Cyberwarfare-Distinction-and-Proportionality-on-the-Cyber-Battlefield.pdf.

Rieker, P. (2007), *The EU as a Security Actor: the Development of Political and Administrative Capabilities*, Working Paper: 725, Oslo: Norwegian Institute of Internationl 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 2013, URL: http://dx.doi.org/10.1080/07036330903274599.

Rousseau, D. L. and T. C. Walker (2010), "Liberalism", in Myrian D. Cavelty 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 2013, URL: http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html.

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 2013, URL: http://www.nato.int/docu/review/2000/0001-04.htm.

Sjostedt, G. (1977), *The External Role of the European Community*, Farnborough: Saxon House.

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.

Szakonyi, D. (2007), "The Rise of Nationalism under Globalization and the Case of Post-Communist Russia," *Vestnik: The Journal of Russian and Asian Studies*, 6 (Summer), [Online: Web] Accessed 05 June 2013, URL: http://www.sras.org/economic_nationalism_under_globalization.

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?", Brief No: 54, June, Washington DC, SETA, [Online: Web], Accessed 10 May 2013, URL: http://www.setadc.org/pdfs/SETA_Policy_Brief_No_54_Western_Balkans_Fatma_Turhan.pdf.

Waltz, K. (1959), *Man, the State, And War*, New York: Columbia University Press.

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. Cavelty 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.

NEWS PAPER ARTICLS

Singh Shalini (2013), "Cyber security Plan to Cover military, Govt. and Business Assets", *The Hindu*, New Delhi, 2 July 2013.

INTERNET SOURCES

Bumiller E. & T. Shanker (2012), Panetta Warns of Dire Threat of Cyberattack on U.S., *The New York Times*, [Online: Web], Accessed 10 January 2013, URL: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.

Buzan, B. (2011), TEDxCentralSaintMartins- No more Superpowers, YouTube, [Online: Web] Accessed 05 December 2012, URL: http://www.youtube.com/watch?v=TuzUPoZNKrc.

Fourkas Vassilys, (N.D.), "What is 'Cyberspace'?", [Online: Web] Accessed 05 May 2013, URL: http://www.waccglobal.org/en/20043-communication-rights-an-unfinished-agenda/495-What-is-cyberspace.html.

HackDomian.com (2012), 2012 Cyber Attacks Statistics, [Online: Web], Accessed 10 June 2013, URL: http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/.

Heraclitus [Ephesus 500 BC], The Flux and Fire Philosophy, [Online: Web], Accessed 18 March 2013, URL: http://www.thebigview.com/greeks/heraclitus.html.

Library of Congress (2009), "European Union Signing of Agreement on Social Networking", 18 February, GLM, [Online: Web], Accessed 20 October 2012, URL: http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205401014_text.

McDowell, M. (2013), *Security Tip (ST 04-015) Understanding Denial -of -Service attacks*, [Online: Web] Accessed 05 June 2013, URL: http://www.us-cert.gov/ncas/tips/ST04-015.

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 2013, URL: http://www.novinite.com/view_news.php?id=67035.

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 2013, URL: http://www.timeshighereducation.co.uk/180751.article.

Tzu, Sun (1913), "*The Art of War*", Translated by Lionel Giles, [Online: Web], Accessed 04 July 2013, URL: http://www.chinapage.com/sunzi-e.html.

YouTube (2011), 'Stuxnet *Virus*', [Online: Web], Accessed 06 October 2012, URL: http://www.youtube.com/watch?v=SAy46DhWW8Y.