University of Pardubice

Faculty of Economics and Administration

Cyberspace: (Advantages and its disadvantages)

Philip Bruce-Quaye.

Master Thesis

2016

DECLARATION

This thesis is presented as part of the requirements for MSc. System Engineering and Management awarded by University of Pardubice. I hereby declare that this Diploma Thesis is entirely the result of my work, research and enquires. Also, I confidently declare that this thesis is not copied from any other person. All sources of information have however been acknowledged with due respect.

In addition, I acknowledge that all the rights and duties resulting from Act. N. 121/2000 Sb., the Copyright Act, apply to my written work, especially that the University of Pardubice has the right to make a license agreement of use of this written work as a school work pursuant to § 60 section 1 of the Copyright Act. On the condition that the written work shall be used by me or a license shall be provided to another subject for the hereof, the University of Pardubice shall have the right to require from me a relevant contribution to reimburse the cost incurred for the making of such work including all relevant cost and total overall expenditure and expenses incurred and express my consent with making the work accessible in the University Library.

NAME	SIGNATURE	DATE
BRUCE-QUAYE PHILIP	**………………**	**……………**

Supervisor's Declaration

I hereby declare that the preparation and presentation of this Diploma Thesis were supervised in accordance with the guidelines on supervision of thesis laid down by the University of Pardubice**.**

Supervisor's Signature …………………… Date ……………………

Name: Prof. Ing. Jan Čapek, CSc.,

Acknowledgement

First, I am grateful to the Almighty God for His unlimited mercies, protection and guidance for endowing me with wisdom in all my academic endeavours.

In the process of writing this thesis many have contributed and helped me along the way, and I would like to acknowledge these efforts. I wish to express my sincere gratitude to my supervisor **Prof. Ing. Jan Čapek, CSc.**, for giving me valuable advice along the way. Also, I would like to say a big Thank You to my entire family and friends who have helped me with large and small things.

ABSTRACT

This study seeks to collect and describe advantages and disadvantages of the cyberspace and touching on the main threats in cyberspace as well as its threat in the global world. Also some areas such as cyber security, cyber bullying, cybercrime, information society and finally, cyber threats have also been talked about in this thesis

It came to light that cybercrime could be undertaken by the individual even at the comfort of his home without having physical contact with the respective victims. Cyber-crime and terrorism is an international problem which does not respect national borders. Cyber criminals operate from relatively safe territories beyond the easy reach of the law enforcement agencies of the countries in which their victims reside. Also, the research revealed that more females of school going age are cyber bullied more than their male counterparts. Measurement and recording is critical to understanding whether the scale of cybercrime is on the ascending or descending and how the nature of the problem is evolving over time. Without a better understanding of these things, it is harder to allocate the right resources to different issues and to recognise what is working and what is not. To ensure that good cyber security is being implemented, 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. In the late 1970s and the early 1980s, the term and the idea of the information society emerged. Since then, it has been witnessed the substantial changes in society as a whole, the changes that stemmed from the development of the new information and communication technologies. Information Society can be loosely defined as a society integrated by complex communication networks that rapidly developed and exchange information. Lastly, the research revealed that, internet usage in the Czech Republic for learning and various purposes far outweigh that of Ghana and this is due to the fact that, cost of devices and connectivity is one major factor preventing many people from accessing the internet in Ghana.

The simple random technique was used in the selection of students and the use of questionnaire was the instrument used to solicit the information from students or respondents. The data were entered using the Statistical Package for Social Science (S.P.S.S.) and total of 100 students and 50 teachers were used for the survey in Ghana.

Finally, some recommendations were made through the findings on how to strengthen cyber security, cybercrimes, and of course, how to minimize cyberbullying. Collaboration between governments, intelligence agencies and law enforcement officers is critical to prosecuting cybercrime, and new organizations should be created to combat cybercrime. Multi-stakeholder cooperation at the local, national and international level is an effective way to create awareness of the importance of child protection issues in some regions of the world and in conclusion, an important role in enabling people’s safety on the internet to help them understand the concepts of risk and safety online, which will allow children, youth or individuals make independent informed decisions.

.

.

.**Keywords: cyberspace, cyber-attacks, cyber threat, cyber conflict, Cybercrime, Cyber Security, Cyber Bullying and Information Society**

CONTENT

LIST OF TABLES

LIST OF ILLUSTRATIONS

Chapter One

INTRODUCTION AND LITERATURE REVIEW

1.1 Background to Study

Very few revolutions have had such an enormous impact on economic, social, political, cultural, and scientific activities and transformation of societies like Cyberspace. As every coin is adjudged to have two faces, Cyberspace also with its wide advantages has also created a platform for criminals to operate as well. This term has been defined by some authors as more than just the internet and was actually proposed by William Gibson in his sci-fi novel Necromancer [13].

Cyberspace could also imply communication between or among people via various means such as (video, voice, text) over the internet or any telecommunications network. Whereas, teaching and learning in cyberspace basically means communication between students and tutors over any telecommunications network. This term can further be classified as a domain that makes use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems since in cyberspace, what is common to all is access to technology and information. But, what is not common is how one uses that information for what purpose and goals.

The field of cyberspace on the other hand also serves as the new channel of communication, electronic communication, which is fast outmoding, or even replacing, more traditional methods of communication. We often send emails in place of paper letters, we leave electronic messages on bulletin boards rather than pinning slips of card to wooden notice boards, and more and more frequently we are able to read texts on-line in e-journals, for instance rather than on good old-fashioned wood pulp. The physical objects of traditional communication (letters, books and so on) are being antiquated by contemporary electronic objects. And, just as physical objects exist in physical space that is earth, so does these cyber objects exist in cyberspace [152]

Attacks in cyberspace have clearly been on the rise in recent years with a variety of participating actors and approaches. Countries like the United States has grown more reliant on information technology and networked critical infrastructure components and this has raised many questions about whether the nation is well prepared to defend its digital strategic assets in a situation of an assault on their cyberspace. [43].

As mentioned earlier, cyberspace has various advantages which comes in the form of informational resources, entertainment, and social networking. In spite the advantages of cyberspace, it has got some disadvantages as well. The drawbacks outweigh the advantages more because of the security and dangers that it entitles within. You never know who is accessing your personal information and what they will do with it. Also, this phenomenon or term could be seen as a socio technical system of systems, with a significant component being the human involved. Thus, a relationship that ensures or occurs between human beings, their environment and the various technologies they are predisposed to.

Situation awareness in Cyberspace refers to cyberspace data collection, situation understanding, projection and exhibit. In 1988 Ensley M. R proposed that situation awareness (SA) can be sectioned into the perception, comprehension and projection (See figure 1 below). Perception was explained as recognition of elements in the Cyber-environment. Comprehension, the integration of the collected data, and the analysis of the relevance among the data. Projection is futuristic view based on analysis of current information

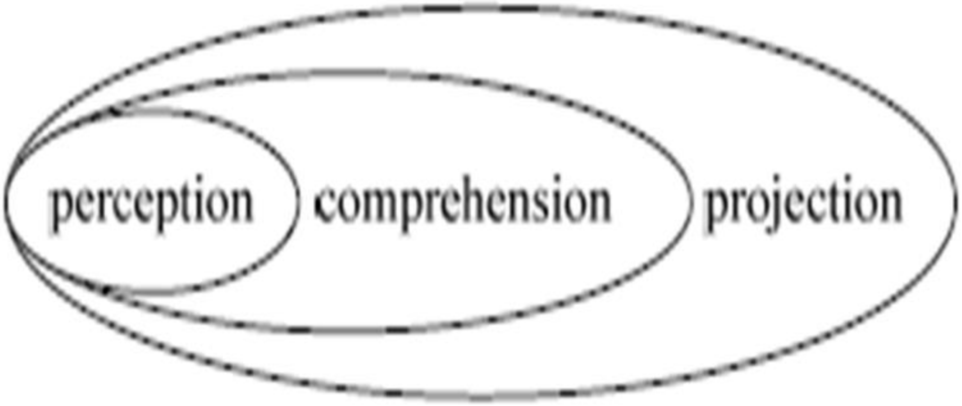


Figure1. Ensley Situation Awareness Model [140]

Cyberspace Situation Exhibition (CSE) also means giving the user a whole, correct view of what happened in the cyberspace. It is the last link of the CSA process

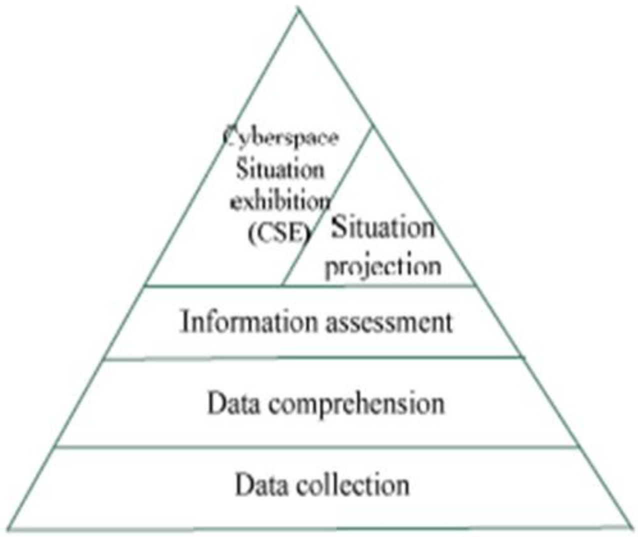


Figure2. CSE Model [140]

The final aim of CSA is to make the decision-makers comprehend the operational status of cyberspace. For we can only get specific data as decision-makers cannot be expected to know everything.

Cyberspace is not just a simple information highway or road; this space is more mental than anything, approximate border between the conscious and unconscious realities with ability to clarify the reality of life. This phenomenon is thus, shaping and changing the three dimensions of the information environment: how we create information content itself (a Web page, for example), how we share that content through new forms of connectivity (the internet links that make that Web page accessible to over a billion people), and how it affects human interaction and communication.

And finally, Cyberspace is a universal sphere within the information environment made up of mutually dependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers [149].

There is also therefore the need to factor in how information is created and distributed. An information society what actually makes it possible for the creations, distribution, use, integration and manipulation of information which is a significant economic, political, and cultural activity.

Digital information and communication technologies are its primary components and together, they have resulted in creating information sudden increase which have extremely changed all aspects of social organization, including the economy, education, health, warfare, government and democracy. The term dozen citizens have been used to describe people who have the means to partake in this form of society. This is one of many dozen labels that have been identified to suggest that humans are entering a new phase of society. In addition to information society, it may be contrasted with societies in which their economic underpinning is primarily Industrial or Agrarian. The main tools of the Information society are computers and telecommunications, rather than lathes or ploughs

The idea of a global Information Society can be viewed in relation to Marshall McLuhan's prediction that the communications media would transform the world into a "global village.". This term or concept is a must for the swiftly dynamic and developed world we find ourselves in today. There is virtually no place and no occupation which information cannot reach. Information is necessary for both the employer and the employee, for engineer who designs the machines and the customer who chooses the products of the company. The modern world is characterized with the transformation of industrial society into information society. Objectives of establishing information society include issues, such as the formation of legal basis for the Information Society, development of human resources, rights of the citizens for obtaining and using information, formation of electronic government and electronic trade, in particular, strengthening the intellectual capacity of the country, establishment of information and knowledge-based economy, development of modern information and communication infrastructure, formation of national electronic information space and provision of information security.

Also, because information society entails creation, distribution, diffusion, use, integration and manipulation of information the need to protect these data from being abused is very essential. Thus, the issue of cyber security comes in here to support the functioning of the state, society, the competiveness of the economy and innovation. It is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information and identity.

Cyber security is endured on the basis of the principle of proportionality while taking into account existing and potential risks and resources. Thus, ensured in a coordinated manner through cooperation between public, private and third sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services in cyber space.

Cyber security begins with the individual accountability for safe usage of ICT devices. One important main concern in ensuring cyber security is predicting as well as counteracting potential threats and taking action effectively to threats that will emerge at the same time being supported by intensive and internationally competitive research and development as well as via international cooperation with allies and partners. The main role of cyber security is thus, playing an important function in the evolving development of information technology, as well as internet services. Enhancing cyber security and protecting sensitive information infrastructures are the key to every nation's security and economic well-being. Safer internet (and protecting internet users) has become integral to the development of new services as well as government policy.

Prevalent usage of the internet has resulted in a range of traditional and new crimes that can now be carried out in cyberspace. Attribute of direct effects and unpredictable means, cybercrime has developed into ever more out of control around the world with an enormous impact. Hence, the fight against it calls for a high level of coordination, collaboration and alliance among all nations, particularly in the area of anti-terrorism.

Cybercrime is a main worry for the global community. The commencement, improvement, and usage of information and communication technologies have been associated by an increase in criminal activities. The internet is all the time frequently used tool and channel by world-wide organised crime. Its global crime status has affected the global revolution in ICTs. Also, cybercrimes are easy to learn and as such, easy to execute. They don't need more resources to cause any potential damage and can be committed in a territory without being physically present in it. Due to this, they are time and again not clearly seen as something unlawful. As a result of this, the new modes of cybercrime appear as new challenges to policymakers, law enforcement agencies, and international institutions. This requires the presence of an effective international as well as domestic mechanisms that keep in check the exploitation of ICTs for criminal activities in cyberspace.

Cybercrimes are into two groups first; those involving unapproved right of entry to data and systems for illegal intentions and second, those including scam, forgery, diversion of funds, obtaining illegitimate content, or offense via online services. This activity challenges the functioning of the economic space, decreases belief in digital services, and in a worst-case scenario, could lead to incidents causing loss of life. Professionals and modern technical instruments are needed in order to guarantee prevention, exposure and prosecuting of cybercrime.

To prevent cybercrime is an issue of national cyber security as well as critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. The fight against cybercrime needs a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is imperative that law-enforcement agencies are allowed to investigate and prosecute cybercrime effectively.

Cybercrimes are uniquely different from traditional crimes, and are often harder to detect and prosecute. It has a chance of putting at danger government systems and public infrastructure. Accordingly, the internet provides a new platform with respect to cyberspace for such crimes. In the virtual world, anyone might become the victim of cybercrimes, having no idea who the real offender is. Sometimes, when people begin to notice that, they would have already suffered from the damage already. However, traditional laws and rules are found to be incapable of dealing with the crimes committed in the cyber world, making the offenders more reckless.

Furthermore, this activity emerges in various modes, and are not limited to internet pornography and sexual harassment, fraud, trafficking and sale of prohibited goods, damage to people’s reputations and invasion of their privacy, and the manufacture and dissemination of computer viruses. Reasons why cybercrime is difficult to combat include defects in the internet itself, widespread software hacking, the internet’s cross-border and international nature, abuses in internet commerce, the internet’s indeterminate nature, and the failure of many countries to attack cybercrime aggressively.

It is also important to note that, cybercrimes are technologically based crimes and the computer or internet itself can be used as a weapon or means to do such crimes quite freely. They are organized in white collar crimes like cyber frauds, hacking, data theft, phishing, identity theft etc. and are committed with the help of technology since cyber criminals have deeper understanding of technology. In fact, cyber criminals are technocrats who understand the intricacies of information technology. In addition, it is very problematic to quantify the impact of cybercrime on society. The financial losses caused by cybercrime, as well as the number of offences, are very difficult to estimate. Nevertheless, surveys can help in understanding the impact of cybercrime.

It is understandable and reasonable for us to see cybercrimes as the crimes committed in the cyberspace or in the environment of networks unlike cyberbullying which is more of a psychological cybercrime in nature. The term cyberbullying involves the use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging, defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others. [108].

Cyberbullying on the other hand, has also turn out to be more rampant as students devote most of their time using technology that keeps them hooked-up to people at all hours of the day. There are numerous diverse ways in which cyberbullies get in touch with their victims or targets, including instant messaging over the internet, social networking web sites, text messaging and phone calls to cell phones. There are diverse forms of cyberbullying involving, but not restricted to, harassment, imposture, and cyberstalking. It has been revealed that, there are differences between not only the commonness of cyberbullying between males and females but also how males and females actually take on cyberbullying. Like bullying, cyberbullying is a serious problem which can cause the victim or target to feel incomplete and overly self-conscious, or even worse, suicide.

Schools, parents and students can help prevent cyberbullying and intervene when cyberbullying has occurred and there are many ways it can be done. Willard suggests steps that schools can take to mitigate such concerns such as increasing awareness of cyberbullying concerns; empowering educator’s students, parents, and community members with knowledge of how to prevent and respond to cyberbullying; and effective supervision and monitoring of online activities.

Cyberbullying is more likely than other forms of bullying to go unreported to parents and administrators. This is due to victims feeling they needed to learn to deal with it themselves and also being afraid that informing their parents may effectively reduce or eliminate substantial part or portion of their precious time spent on the internet. It has been found that 90% of respondents in the Juvonen and Gross study 2008 reported not telling adults about cyberbullying incidents due to these reasons. Victims of cyberbullying may experience stress, low self-esteem, and depression. Furthermore, it has come to a realization that cyberbullying can also have extreme repercussions such as suicide and violence [84]. Bullycide is bullying which eventually leads the victim to commit suicide.

Statement of the Problem

The challenges that cyberspace encounters are more because of the security and dangers that it comes with. You never know who is accessing your personal information and what they will do with it. Cybercrime limits the smooth operation of economic space and also scraps off trust in digital services, and, in a worst-case scenario, could lead to incidents of loss of life. Competent personnel and modern technical tools are needed in order to ensure prevention, detection and prosecuting of cybercrime. Operational information exchange between countries is also becoming increasingly important in the fight against cybercrime.

To prevent and deter future security threats, it is highly required that cyber security is constantly developed along with an equally serious investment in technology. Forward-looking procurement strategies too would be a desirable addition ensure production of reliable and competitive technical solutions which will support their export as well, whereas the knowledge and resources obtained in that process must be re-invested into innovative solutions.

Today, cyberspace become a source of great vulnerability, posing potential threats to national security and a disturbance of the pre-existing global order. Connected computers and the ecosystem that makes up cyberspace have pulled nations to the shores of complex security challenges. Cyberspace vulnerabilities do not arise from only technology, but also from inadequacies in governance, processes, management, culture, inter-dependencies and integration. It is however important for nations to understand every possible building block of cyberspace: its framework, associated processes, technology, people and ecosystem. In this new sphere of cyberspace, however, malicious activities are prevailing. Stealing personal, business, and organizational information and assets has been increasingly persistent in this technological age. There are also growing threats against national safety and security; governmental bodies and business operators, who are responsible for providing mission-critical infrastructure necessary for the people’s daily lives and economic activities, have been exposed to cyber-attacks that would risk their business operations and continuity. In light of such malicious activities, it is challenging to come up with the most concise means to counter these threats to ensure and maintain the free flow of information that is the “backbone” of democracy, the safe and secure living environment of the people, economic and social prosperity, and peace, while protecting intellectual properties and rights that are the fruits of the creativities and inspirations of individuals and businesses as well.

Uncertainties also exist as to the intent and full technical capabilities of several observed attacks. Enhanced cyber threat analysis is needed to address long-term trends related to threats and vulnerabilities. What is known is that the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving.

Significance of the Study

Cyberspace is a virtual space where people communicate with each other with information systems, while the objects of their communications may range from simple messages (ordinary day-to-day applications) to video. People will go shopping via the internet and pay through it. Using the internet as a research tool is by no means taboo. One could effectively educate oneself in virtually any discipline using only online libraries and online teaching materials. Esoteric information about one’s ratified academic fields of study like quantum physics, hydro- and aerodynamics, or brain chemistry, are now openly available to anyone who has an Internet connection.

Internet is a single platform where all the others can converge - information, speech and visual combined as digital information. Unlike the other technologies often referred as ‘push technologies’ where the process is one-way from those who produce to those who consume, internet is referred to as ‘push and pull technology’ offering interactive process. Cyberspace is a domain that makes use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems.

Teaching and learning in cyberspace (E- Learning) “draws on educational technology, instructional design and traditional pedagogic theory to design, deliver, and implement a learning environment to promote knowledge construction, critical analysis and reflective practice in our learners. It draws on student’s established social networking abilities and enables them to apply this to the realm of education [151]. Social networking also plays a major role in cyberspace. One cannot imagine an online life without Facebook or Twitter. Social networking has become so popular among the youth that it might one day replace physical networking. It has evolved as a great medium to connect with millions of people with similar interests. Apart from finding long-lost friends, you can also look for job, business opportunities on forums, communities etc. Besides, there are chat rooms where users can meet new and interesting people. Some of them may even end up finding their life partners.

Lastly, cyberspace is now considered as a powerful, collective mnemonic technology that promises to have an important, if not revolutionary, impact on the future compositions of human identities and cultures. And, it is also the conceptual space where word, human relationships, data, wealth, and power are manifested by people using computer-mediated communications.

LITERATURE REVIEW

This section provides background to the research through a review of some of the literature on the advantages and disadvantages of cyberspace, cyber security, cyber-crime and cyber bullying. The literature review is directed at those areas central to the scope of this research. Since the mid-1990s, a number of authors have offered useful insights that have helped shaped thought on this issue several consistent threads run through these insights, including the role of electronics, telecommunications infrastructures, and information systems.

The term *cyberspace* was popularized by William Gibson’s 1984 novel, Necromancer, in which he describes cyberspace as a network space of digital data stores with connectivity for access and interaction through a computer connection [13]

What we now recognise as cyberspace was envisioned and designed as an information environment and there is a long-drawn-out appreciation of cyberspace today. For example, Public Safety Canada in 2010 defines cyberspace as “the electronic world created by interconnected networks of information technology and the information on those networks [109]. It is a global and common platform where people are linked together to exchange ideas, services and friendship." Cyberspace is not static; it is a dynamic, evolving, multilevel ecosystem of physical infrastructure, software, regulations, ideas, innovations, and interactions influenced by a growing population of contributors who represent the range of human intentions [110]. This phenomenon is nowadays characterized as the fifth common domain (the others being land, sea, air and outer space) and is in great need for coordination, cooperation and legal measures among all nations as cybercrimes tend to increase day by day, leading to soaring revenues for the criminals and luck of trust in the internet for the users [1].

Also, Cyberspace has changed people's life style. Currently, cyberspace has been widely applied to education, finance, aviation, power, defence and other key sectors, more and more people are concerned about the development of cyberspace, the research of cyberspace has attracted wide interest by the scholars [2-5]. This term can further be defined as a multidimensional space, relevant to the computer and electronic space of which is constructed by the words cybernetics and space. There are many explanations about cyberspace as well as some main features about it [7].

FEATURES OF CYBERSPACE

1: Cyberspace is a virtual space, like some kind of mental states, is a place coexistence of real and virtual.

2: People can access cyberspace through physical devices with artificial processing functions. All these devices can be considered as the boundary of cyberspace, the window of the cyberspace.

3: Interaction and communication, which is independent of time and space. Because the cyberspace is not restricted by the time and the space .it is suffered a huge security threats.

Cyberspace has faced many security challenges like identity tracing, identity theft, cyberspace terrorism and cyberspace warfare.

Cyberspace has been improving lifestyle since the 1980's. It has been widely used in various scenarios such as finance, hospitals, education and national defence [1-4].

From the standpoint of security, cyberspace faces all kinds of security threats [8]. There are 5 major secure goals for cyberspace namely, confidentiality, authentication, availability, non-reputation and integrity [4]

Attackers attack cyberspace to destruct confidentiality, authentication, availability, non-reputation and integrity of data. The classification of cyber-attacks can be shown as first, based on purpose. Secondly, legal classification, thirdly based on severity of involvement and finally, based on scope and network types [8]. The dependence on cyberspace by governments, corporate, industries, academia and many other sections of the society for their daily activities is growing at a rapid rate and at the same time, cyberspace is also expanding due to increased automation worldwide [9-12].

Gandhi, Sharma, Mahoney, Sousan, Qiuming and Laplante also described cyberspace as "a massive socio technical system of systems, with a significant component being the humans involved" [14]. And according to Wielki, this term is "a non-physical terrain existing around the internet (understood as a global computer network) in which, based on its technical infrastructure and the utilization of internet technology based tools, various entities such as firms, institutions or private persons operate to accomplish their own goals."[15]. And lastly on cyberspace, it can be viewed as three layers (physical, logical, and social) made up of five components (geographic, physical network, logical network, cyber persona and persona) [17]. The information environment in global fields which is composed of independent information technology infrastructure, including Internet, telecommunication network, computer system and embedded processor & controller [18].

Advantages and Disadvantages of Cyberspace

Cyberspace has gained so much importance, usefulness and dependent as a virtual world space, parallel to the physical world space in today's society within a short period of time. However, there are certain inherent disadvantages linked with the cyberspace as well. The foremost disadvantage and challenge is the fact that cyberspace has no borders or defined jurisdiction. This provides an ideal playing ground for malicious actors, who find it very easy to perform criminal activities online without being detected and punished. It emphasizes each nation to act responsibly for provision of secure, reliable and truthful networked environment.

INFORMATION SOCIETY AND CYBERSECURITY

Most information's which are created, discovered and their mode of channelling as a result of information society serves as a raw data acquired from our modern day digitalized society, ought to be protected by means of ensuring good cybersecurity systems.

Perception of the Information Society was conceived by Daniel Bell (born May 1919), arguably the most influential sociologist of the late twentieth century and also, information society is a master key for both social-scientific interpretations of contemporary society and socio-philosophical articulation of normative and public-policy issues [22]. Information Society can be loosely defined as a society integrated by complex communication networks that rapidly develop and exchange information. This concept is becoming an earthly phenomenon and the goal of every country is to ensure that their people achieve the status of information society.

As a development stage of the civilization, information society is characterized by the increase of the role of information and knowledge in the society, growth in the share of information communications, products and services in the flow of domestic goods, establishment of the global information space ensuring effective exchange of information and access into the global information resources of the people. Currently, the wide application of Information and Communication Technologies (ICT) in various spheres of the society, including economy, energy, ecology, etc. emerges the problem of information security. In general, the more dependence of all sectors of society and the people on ICT is stronger, the more obvious the importance of information security becomes.

As one of the major duties of the information society establishment, information security is becoming one of the main directions of providing security of the government, society and person. Many researchers face several cognitive and empirical challenges referring to information society (IS). The cognitive challenges refer to terminology describing information society, identification of phenomena, processes and success factors of this society and also the methodology of information society measurement. The empirical challenges are mainly connected with building information society and its measurement. Research of this scope is conducted in the academic environment [19], [20], as well as among practitioners [21].

To date there has not been in operation a commonly accepted definition of information society [22], [23], [24], [25], [26], [27], [28]. Lack of consensus with regard to the definition of information society is undoubtedly a derivative of complexity of processes taking place in a social system, characteristics of information as a resource, and the dynamics of ICT changes. This brings specific consequences for the undertaken attempts for measuring phenomena within the frame of a category, which might be and is understood in various ways. Nonetheless, despite the conceptual limitations there are attempts taken to describe the information society quantitatively.

Generally speaking, there are two approaches to the quantitative description of information society. The first one comprises the preparation of the list of indicators characterizing information society. The other is connected with compiling the so-called composite indexes which are aggregate measures. It should be stressed that the composite index is based on the previously chosen set of indicators. Some significant constraints can be pinpointed in both approaches. The arbitrariness of the choice of indicators, disorderliness of gathering source data, lack of standardization and time-space comparability, substantive errors in assigning indicators to specified information society dimensions and errors in constructing a given index – those are some of the significant drawbacks and constraints

Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Articulating a concise, inclusive, meaningful, and unifying definition will enable an enhanced and enriched focus on interdisciplinary cybersecurity dialectics and thereby will influence the approaches of academia, industry, and government and non-governmental organizations to cybersecurity challenges. The term "cybersecurity" has been the subject of academic and popular literature that has largely viewed the topic from a particular perspective. Based on the literature review described in this article, the term is used broadly and its definitions are highly variable, context-bound, often subjective, and, at times, uninformative. There is a lack of literature on what the term actually means and how it is situated within various contexts. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity potentially impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges. For example, there is a spectrum of technical solutions that support cybersecurity. However, these solutions alone do not solve the problem; there are numerous examples and considerable scholarly work that demonstrate the challenges related to organizational, economic, social, political, and other human dimensions that are inextricably tied to cybersecurity efforts [126]. Fredrick Chang, former Director of Research at the National Security Agency in the United States discusses the interdisciplinary nature of cybersecurity: “A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed.”

Cavelty noted there are multiple interlocking discourses around the field of cybersecurity. Deconstructing the term cybersecurity helps to situate the discussion within both domains of "cyber" and "security" and reveals some of the legacy issues [50]. “Cyber” is a prefix connoting cyberspace and refers to electronic communication networks and virtual reality [54]. It evolved from the term "cybernetics", which referred to the “field of control and communication theory, whether in machine or in the animal” [153]. The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure.” [49] The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.” [51]. DHS is the Department of Homeland Security.

Cybersecurity is a complex challenge requiring interdisciplinary reasoning; hence, any resulting definition must attract currently disparate cybersecurity stakeholders, while being unbiased, meaningful, and fundamentally useful. Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption." [53]. Furthermore, this concept involves reducing the risk of malicious attack to software, computers and networks. It also includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, and enable encrypted communications, [48].

Nagarajan, Allbeck, Sood and Janssen highlighted the importance of cyber security in terms of understanding for the computer users with various skill levels starting from novice to expert. They hold the view that, gaming can be a best approach to train the users on cyber security skills. They also investigate the current practices of training on cyber-security skills using gaming tools and suggest different ways to cyber-security training game design and development [55]. Hoffman, Burley and Toregas suggested an integrated method to build cyber-security talent involving all the stakeholders. Some of the stakeholders mentioned were educators, career professionals, employers, and policymakers, and believed that piece meal approaches do not work and seeks the support from all the stakeholders to build better approaches towards cyber-security [56].

The need for national level strategy which will also be to suitable beyond the borders to deal with cyber-security holistically in order to safeguard the interest of information economy is emphasized in [57]. Society's dependence on various communication and collaboration services is well known [57-58]. The societal challenges and other aspects that influence the creation of assurance in cyber-security by going to the core of it were investigated in [57]. Takahashi, Kadobayashi and Nakao [58] present a Cyber Security Operation activity model to overcome the communication problems due to lack of generally accepted operations terminology among organizations.

Puri and Rutkowski [59] discussed the need for more strong next generation networks with improved cyber-security capacities. It is believed that Cyber Security Information Exchange Framework (CYBEX) created by ITU-T study group 17, if implemented in future networks including Cloud computing and smart grids will improve the cyber security tremendously. Quantitative Evaluation of Risk for Investment Efficient Strategies (Queries) methodology to quantify security technology risks in complex systems that will be useful both in defence as well in industry to make better investment decisions based on quantified risks is detailed in [36]. The need to have proactive risk assessment of cyberspace when compared to the existing general reactive approaches followed is emphasized for technology implementations in operations [60]. Gavins and Hemenway [60] presents Joint Terminal Engineering Office (JTEO) approach that is based on combining qualitative and quantitative engineering analysis for proactive cyber-security risks assessments in both military systems development and its operations

There are also numerous cyber security threats, attacks and huge impacts, leading to growing importance for cyber security [61-62]. Unfortunately, most of the approaches to deal with cyber security are of fragmented nature. This is due to inadequate study and understanding of cyberspace leading to ineffective cyber security solutions that were implemented. Miller and Murphy [63] argued that the pervasive nature and rapid advancement in technologies, with multiple uses for many sections of the society also brought in less secure products that had short gestation times.

Kalay and Marx [64] critiques about the approaches that were used to utilize cyberspace with irrelevant resemblances without making use of rich data that helped the physical spaces and studied how best the past information about physical spaces and places will be useful for cyberspace. Kephart, Sorkin, and Swimmer [65] present an immune system for computers in cyberspace that is capable of identifying and eliminating the computer viruses that are previously not known and propagate very rapidly. Enterprises' cyberspace protection failures continue to happen, even when they spend lot of resources to prevent them from happening due to the current fragmented approaches to cyber security. These approaches tend to ignore having an understanding of the influences of the cyberspace on the enterprise cybernetically, before they identify the cyber threats and implement the cyber security solutions.

Cybernetics approach to study the influences of cyberspace on an enterprise. It is imperative that such a study will aid to understand the influences of cyberspace on the enterprise cybernetically, before effective cyber-security solutions for enterprises are provided. The awareness and understanding gained was used to identify the various cyber-security threats and their impacts to build credible cyber threat detection capabilities and develop effective cyber-security for the enterprise.

Cyber Security is not restricted to only to protection but rather, a broader network and information technology infrastructure. In addition, the aspect of cyber security cannot be overlooked in this modern era of development into computing. It is however important to make the internet more guarded and protect the user of internet from cyber-attacks in order to strengthen the services of people.

CYBERCRIME AND CYBERBULLYING

Cybercrime is more of a physical crime whereas cyberbullying involves more of a psychological approach. Definition of cybercrime, the microscopic theory of "crimes against computer networks is the use of computer technology on the integrity or normal operation of the computer network information systems to cause damage results constitute a criminal act.

The rationale of cybercrime is limited to the object of crime occurred to computer networks and criminal behaviour in cyberspace, crime and crime results in the network formation and end. Microscopic theory asserts that, network implementation, kidnapping, extortion, and so on should be attributed to the traditional crime, which does not belong to the scope of cybercrime. As a result, the microscopic theory of cybercrime is only for the criminal acts of the network itself hence can be summed up as an object theory. In order to understand the development of cybercrime it is required to study the language and culture of the internet as well as the pathways that connect users from around the world

Cybercrime involves traditional criminal activities like forgery, fraud, theft, mischief and defamation as well as web defacement, hacking, web jacking & cyber stalking which have evolved as a result of computer abuse. R Nagpal from Asian school of cyber law defines cybercrime as “unlawful acts wherein the computer is either a tool or a target or both” wherein used not only is meant for desktop computers but also includes Sophisticated watches, Mobile phones, Personal Digital Assistants (PDA) and a host of these gadgets. Most of the modern day crimes whether it is world famous attack on “World trade centre” in USA, Serial blasts, “The Taj” hotel in India, hacking of web portals were not possible without the help of computers. Unfortunately, since the major number of cybercrime is not reported so it is not possible to check with their exact impact on finance and society. As cyber-attacks can result in dreadful results disrupting the rail and air traffic controls, stock markets, banking systems; Intelligence agencies are preparing hard to check with these disasters. [30]

TYPES OF CYBERCRIME

A. Financial Crimes

B. Cyber Pornography

C. Sale of Illegal Articles

D. Online Gambling

E. Intellectual Property Crimes

F. Email Spoofing

G. Forgery

O. Virus/Worm Attacks

K. Email Bombing

J. Web Defacement

I. Cyber Stalking

N. Denial of Service Attacks

M. Salami Attacks

L. Data Diddling

H. Cyber Defamation

R. Web Jacking

Q. Internet Time Theft

P. Trojans & Key loggers

S. Email Frauds

T. Cyber Terrorism

U. Cyber Warfare

V. Use of Encryption by Terrorists

The internet is attractive to technologically-savvy criminals because it provides them the opportunity to locate and research their victim's behaviour, widens their field of activity and offers them the potential to change their identity. More importantly, they can operate from another country, thus making their prosecution a complex matter, due to the different legal frameworks and the international procedures that should be followed in order to arrest them. Contrary to traditional crimes, the perpetrator and the victim are seldom in the same physical location. Therefore, the law enforcement agencies face several difficulties in both investigating and closing such crime cases.

CYBER CRIME EXAMPLES

Several instances of the well-known "Nigerian letters" cybercrime occurred in December 2011. These involved sending emails to internet users for supposedly pending large amounts of money, mainly earned by participation in lotteries. The purpose was to collect personal information of the recipients of these letters. The messages were written in English and were also sent to mobile phone numbers. These messages were announcing to the recipient that they had won e.g. two million euros. In a second cybercrime case on September 2011, three people were accused for fraud and for exploiting a mobile phone company. By using advanced techniques, they succeeded in hacking into the company's computer systems and they managed to illegally sell internet connections to Cuba. The result was the company to be charged with the amount of 690,501 euros

Another cybercrime case for 2011 had to do with accessing pornographic websites, using computers running Microsoft Windows. While the website was still loading, a message appeared automatically, informing the users that they had visited sites with child pornography and for this reason the computer had been blocked by the Cyber Crime Police. The user would then have to pay to avoid being accused by the police. Eventually, it was discovered that the data was being stored on a Ukrainian server. Finally, in May 2012 a travel agency owner in Thessaloniki was accused for Internet fraud, because travel packages were advertised through different Facebook profiles. Tickets or hotel reservations were proved to be fake, while in other cases overcharging of credit cards was noticed.

Cybercrime is defined as any offence that is committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as internet (chat rooms, emails, notice boards and e-groups) and mobile phones (SMS/MMS). Such crimes could be a threat to a nation's security and financial health. Further, cracking, copyright infringement, child pornography, and child grooming, privacy problems owing to lawful or unlawful loss and interception of confidential information are some high profile issues related to cybercrime. [145]

MEASURING AGAINST CYBERCRIME

The best way to prevent theft of personal data is of course not to store personal data. In those many situations in which personal data is stored anyway, several other means are possible [34]: following strict rules when storing and processing personal data and storing and processing anonymized personal data only. Cybercrime is referred to as any illegal activity which make using a computer as the primary means of commission. This definition was expended by the U.S. Department of Justice, for any illegal activity to use a computer as a storage of evidence.

Based on [35], cybercrime could be categorized in two ways: content based and technology based crimes. The former is managed by any specific terrorist organization related to the article of threating, national security, child pornography, sexual harassment, etc. and the latter involves hacking, injecting malicious code, incidents of espionage, etc. The people who are involved in both types should have some technology knowledge. The cyber criminals tend to be residing in various types of world and enjoy getting the privilege of various citizens.

Several researchers acceded that cybercrime is any unlawful activity operated through the computer, notwithstanding, some vary on where it takes place. There are many types of cybercrime such as computer hacking, internet fraud, unsolicited bulk mail (spam), credit card fraud, identity theft, online gambling, fraudulent websites, malware spreading and so on [37]. A comprehensive approach is needed to stand against cybercrimes; providing technical solution only, are not enough to avert any crime. The law enforcement agencies should be allowed to effectively and efficiently probe and prosecute cybercrime [37, 38, 39].

This review is set within the context of ‘what is illegal offline is illegal online. Specific offences most commonly associated with cyber-dependent crimes, such as hacking and the creation or distribution of malware, are defined in the Computer Misuse Act 1990. Cybercrime is an umbrella term used to describe two distinct, but closely related criminal activities: Cyber-dependent and cyber-enabled crimes. the use of ‘cybercrime’ refers to both forms of criminal activity, and we distinguish between them as outlined below.

DIFFERENCE BETWEEN CYBER-DEPENDENT AND CYBER-ENABLED CRIMES

Cyber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other form of ICT. These acts include the spread of viruses and other malicious software, hacking, and distributed denial of service (DDoS) attacks, i.e. the flooding of internet servers to take down network infrastructure or websites. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud.

Cyber-enabled crimes are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT. Unlike cyber dependent crimes, they can still be committed without the use of ICT. For the purposes of this review the following types of cyber-enabled crimes are included:

1. fraud (including mass-marketing frauds, ‘phishing’ e-mails and other scams; online banking and e-commerce frauds);

2. theft (including theft of personal information and identification-related data); and

3. sexual offending against children (including grooming, and the possession, creation and/or distribution of sexual imagery).

There are a range of motivations behind cybercrimes. They focus largely around financial gain (for example, the use of malware or phishing emails to gain access to bank account details) or can be a form of protest and/or criminal damage (for example, hacking and website defacement). For child exploitation, the motive is clearly not always for profit. More unorthodox motivations for cybercrimes include intellectual curiosity/challenge; general maliciousness; revenge; gaining power/respect in online communities; or even simply boredom [44].

In-depth technical skills are not necessarily required for offenders to commit cyber-dependent and cyber-enabled crimes. The emergence of sophisticated and automated 'do-it-yourself' malware kits and hacking tools, available for purchase on online forums, means that opportunities for complex forms of offending have been opened up to a much wider range of lower-skilled individuals [31]. A small, but elite group of cyber offenders are thought to be responsible for creating these sophisticated tools, which can subsequently be used by a wide pool of semi- and unskilled offenders [33].

Cybercrimes are not, however, just about technical skills and rely heavily on the behaviour of the intended victim. Social engineering tactics are key to deceiving computer-users about the purpose of a file or an email they have been sent [33,45]. Phishing emails, for example, can be carefully designed to look like they are from a bank or other organisations in order to deceive individuals into parting with personal information or money. Computer-users may also unknowingly download viruses in attachments if they are led to believe the email is from someone else.

Most published evidence regarding cyber offenders is drawn from handfuls of case studies or interviews and tends to focus on offender motivations and methods. There is little comprehensive published evidence regarding other key information, such as offender characteristics, career pathways and the links between online and offline offending.

Organised cybercrime

Case-study evidence has identified that some traditional hierarchical organised crime groups have recognised the value of new technologies in facilitating the commission of crimes, for example, through extortion, money laundering, scams, credit card forgery and other online frauds [111]. Whilst these types of groups may not be working online themselves, evidence suggests that they may be prepared to pay for the information that cyber criminals have available, in order to carry out crimes in the physical, rather than the virtual world [47].

However, many ‘organised’ cyber criminals do not operate in this traditional way. They work as looser online networks of organised cyber criminals as part of global online marketplaces where they can buy and sell the technical tools or services used for, or products derived from, cybercrime attacks [32]. These groups are working within an organised structure, but unlike traditional organised crime groups the individuals in these online forums are not bound by the same hierarchy and governance, and tend to work together as loose affiliations for shorter, finite periods of time rather than on a continuing basis [46]. Researchers in the US [31] have explored the organisation of these types of cyber criminals through their interactions in online forums, with a view to informing disruption activities. At present, there are no reliable estimates of the precise scale or cost of organised cybercrime.

Improving the cybercrime evidence base

Cybercrime is a complex issue. Some of the main challenges to improving understanding of cybercrime include:

- lack of recording mechanisms that accurately distinguish between online and offline crime

- Under-reporting of cybercrime from the public and businesses and a lack of awareness that some cyber incidents are actually crimes (although not all are)

- Inconsistencies in the measurement and definition of cybercrime within the relevant research

- Information from industry sources often lacks transparency and comparability

- Few methodologically sound surveys of victims exist;

- Cybercrime can be undertaken on a large scale, potentially resulting in a relationship between victims and offenders that is very different to ‘offline’ crime; and

- Cybercrime is global in nature; it is not constrained by national boundaries.

Measuring cyber crime

Improving measurement and recording is critical to understanding whether the scale of cybercrime is increasing or decreasing and how the nature of the problem is evolving over time. Without a better understanding of these things, it is harder to allocate the right resources to different issues and to recognise what is working and what is not. The introduction of Action Fraud reporting is one key element to improving understanding of the scale and nature of cybercrime, but other improvements are also needed, including systematically improving the quality and range of individual measures of cybercrime. Following the establishment of Action Fraud cybercrimes are more.

Also, cybercrime fall into the category of digital crimes. In a narrow sense, cybercrimes is known as computer crime, which includes any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the date processed by them. In a broader sense, cybercrimes can be recognized as computer-related crime, which is an illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network [146]

With respect to cybercrimes, the internet is mainly the sole target. Also, illegal invasion on or destroying of information system. On the other hand, it could serve as mechanism for fraud, theft, corruption, embezzlement, espionage, breach of confidence, infringement of copyright and other common crimes.

The main factor in cyber-crime increase is the internet. By use of internet, cybercriminals often appeal to images, codes or electronic communication in order to run malicious activities. Among the most important types of internet crimes we can mention; identity theft, financial theft, espionage, pornography, or copyright infringement. The cyber-crimes can be divided into two categories. The crimes where a computer network attacks other computers networks for example a code or a virus used to disable a system. And the second category crimes where a computer network attacks a target population for identity theft, fraud, intrusions [147]. Issues revolving around cyber-crime have become more and more complex. Computer criminal activities have grown in importance and institutions are more interested than ever in putting an end to these attacks. Progressions have been made in the development of new malware software, which can easily detect criminal behaviour [148]. Moreover, high quality anti-virus systems are offered for free now in many countries at every purchase of a computer or an operating system.

The word cyberbullying did not even exist a decade ago, yet the problem has become a pervasive one today. Cyberbullies do not have to be strong or fast; they just need access to a cell phone or computer and a desire to terrorize. Anyone can be a cyberbully, and such persons usually have few worries about having face-to-face confrontation with their victims. In fact, the anonymity of cyberbullying may cause students who normally would not bully in the tradition-sense to become a cyberbully [66].

The double-edged nature of modern technology, continuously balancing between risks and opportunities, manifests itself clearly in an emerging societal problem known as cyberbullying [67]. More than 97% of youths in the United States are connected to the internet in some way and as such they engage theirselves in numerous activities over the internet of which some of them could possibly lead to cyber bullying. [68]

The collection of advantages, not-that -withstanding, has been recently eclipsed by numerous accounts of the internet's undesirable social implications, which appear in both scholarly literature and popular media. A fair amount of attention has been given to internet offenses, including cyberstalking Seto in 2002, sexual predation Dombrowski, Lemasney, Ahia, & Dickson, 2004, as cited in Tokunaga, 2010, and cyberbullying Bhat, 2008; David-Ferndom & Hertz, 2007 as cited in Tokunaga, 2010, which collectively place the safety of children and teens who use the Internet into question. [68]. Bullying and hostility among children is a long-standing and pervasive social issue [128]

Cyberbullying is the unfortunate by-product of the union of adolescent aggression and electronic communication and its growth is giving cause for concern [71]. While bullying among students is a recalcitrant problem in U.S. schools, research indicates that many students do not disclose bullying they experience or witness despite repeated efforts on the part of adults [115]

In a study conducted by Wong-Lo and Bullock in 2011 a total of 137 participants (62 adolescents; 75 parents) responded to a survey. Results indicated that 90% of the participants from the adolescent group have reported to have experienced cyberbullying either as victims or as a bystander. In addition, 70% of the victims have been cyberbullied one to two times within a month’s time and 50% of the victims did not know the perpetrator. Secondly, 89% of parent participants indicated to be knowledgeable about the issues relating to cyberbullying and 89% reported to have no knowledge if their child has or has not been a victim of cyberbullying [70].

Erdur-Baker’s 2010 study revealed that 32% of the students were victims of both cyberbullying and traditional bullying, while 26% of the students bullied others in both cyberspace and physical environments [73]. In Mishna’s et al 2012 study, over 30% of the students identified as involved in cyber bullying, either as victims or perpetrators; one in four of the students (25.7%) reported having been involved in cyberbullying as both a bully and a victim within a three-month period [74]. In Adams,2010 research, approximately 20% of students admitted to having been cyberbullied [112]. The absence of a universal cyberbullying definition is due to a lack of conceptual clarity [75]. Tokunaga emphasized a need for consistent not disparate conceptual and operational definitions [68]. Cyberbullying is a category of bullying that occurs in the digital realm/medium of electronic text [70]

Cyberbullying emerges most commonly from relationship problems (break-ups, envy, intolerance, and ganging up); victims experience powerfully negative effects (especially on their social well-being); and the reactive behaviour from schools and students is generally inappropriate, absent, or ineffective [76,82]. There is a significant correlation between becoming a cyber victim and loneliness among adolescents and studies show that electronic bullying peaks in middle school [77]. Two studies conducted by Smith, et.al found cyberbullying less frequent than traditional bullying, but appreciable, and reported more outside of school than inside [79]. Snakenborg, Van Acker, and Gable, state cyberbullying is especially insidious because it affords a measure of anonymity and the opportunity to reach a much larger number of victims without a significant threat of punishment [78]. Reece supported Snakenborg, et al in the anonymous nature of the internet making it easy to say and do things you would not say or do in person [80].

Students with exceptionalities are bullied at all grade levels, as well as in and away from school. Also, students with exceptionalities may be bullied directly or indirectly. Cyberbullying and relational bullying were not associated with perceived school safety. Males reported more physical victimization, verbal victimization, and verbal bullying, and less relational victimization [81].

The fact that females are cyberbullied more often than males adds much of what is known about gender differences in traditional bullying literature. When gender differences are uncovered in traditional bullying, boys are more involved as both bullies and victims than girls [83].

There are different forms of cyberbullying. These forms include flaming, harassment, denigration, impersonation, outing, trickery, exclusion, cyberstalking, and cyber threats. [138]. Willard (2006), also proposed nine main forms of cyberbullying: flaming, harassment, denigration, impersonation, outing, trickery, exclusion, cyberstalking and cyber treats. Flaming is online fights using electronic 7 messages with angry and vulgar language. Harassment is another form in which the cyberbully repeatedly sends insulting messages via the Internet. [138]

As previously mentioned cyberbullies often believe they are anonymous to the victim and therefore tend to say more hurtful things to the victims than they would if they were face to-face. However, 73% of the respondents to their study were "pretty sure" or "totally sure" of the identity of the cyberbully [84]. A particular victim of cyberbullying that lead to "bullycide" is Megan Meier. Megan was a I3-year-old female from Missouri who was cyberbullied to the point that she hung herself in her closet in October of 2006 [137]. Cyberbullying involves the use of information and communication technologies to cause harm to others [132]. According to the National Crime Prevention Council and Harris Interactive, Inc.'s study in 2006,43% of the students surveyed had been cyberbullied within the last year as cited in Moessner, 2007. That same year, the Pew internet and American life Project found that one out of three teens have experienced online harassment Lenhart, 2007. [135,136]

According to an article in the NASP Communique 2007, a poll conducted by the Fight Crime: Invest in Kids group found that more than 13 million children in the United States aged 6 to 17 were victims of cyberbullying. The poll also found that one-third of teens and one-sixth of primary school-aged children had reported being cyberbullied [133]

In Confronting cyber-bullying there are also additional concerns related to it. And these are anonymity, an infinite audience, prevalent sexual and homophobic harassment, and permanence of expression. Anonymity refers to the anonymous nature of cyberspace in which people are able to hide behind screen names that protect their identity [85].

There are six main ways by which cyber bullying could be channelled and they are basically e-mail, instant messaging, chat rooms bash boards, small text messaging, Web sites, and voting booths. E-mail is used to send harassing and threatening messages to the victims and although it is possible to trace where the e-mail was sent from, it is often difficult to prove exactly who sent the e-mail. Instant messaging (IM) allows for 'real time' communication. Although most IM programs allow users to create a list of screen names that they do not want to contact them, it is easy for bullies to create new screen names and therefore still be able to contact the victim. Chat rooms or bash boards are a lot like instant messaging, however, instead of one-on-one real time communication, there is a group of people who are all talking together at the same time [113]

According to a study conducted in 2008 by Hinduja & Patchin, females are as likely, if not more likely, to be involved in cyberbullying in their lifetime. Although, when students were asked about their recent experiences of being cyberbullies, males and females responded equally. When asked about lifetime participation, females reported higher rates of participating in cyberbullying, which leads one to believe females engage in these activities for a longer period of time [71]

Hinduja & Patchin 2008 researched the reasons why females participate in and experience cyberbullying more often than males. They found that due to females being more verbal and cyberbullying being text based, it is more likely for females to partake in cyberbullying. Females also tend to bully in more emotional and psychological ways, such as spreading rumours and gossiping, which is more in line with cyberbullying. Females tend to be less confrontational when in a face to face situation and therefore the anonymity of the online community may be more appealing to them. Hinduja & Patchin also state that females are generally culturally and socially constrained when it comes to using aggression or physical violence, however, are not under those constraints while they are online. Females are often more apt to require social support and in order to gain that, they often gang up against other females [71]. There are eight main steps that Willard suggested for addressing cyberbullying. They include engaging in participatory planning, conducting an assessment, ensuring an effective anti-bullying program is in place and reviewing policies and procedures related to internet and mobile communication devices. Additionally, it is important to conduct professional development of individuals in the district, include parents on prevention and identification of cyberbullying, educate students about cyberbullying and what to do about it, and finally, to assess the cyberbullying prevention and intervention plan periodically to determine its effectiveness [138]

It is also important for schools to provide anonymous drop boxes in which students can report bullying and other illicit activities [134]

There are many ways that schools, parents and students can help prevent cyberbullying and intervene when cyberbullying has occurred. Willard suggests steps that schools can take which contain elements of increasing awareness of cyberbullying concerns; empowering educators, students, parents, and community members with knowledge of how to prevent and respond to cyberbullying; [138]

Reasons for Cyberbullying

Externalizing behaviours were most predictive of cyber victim status. Increased awareness about the use of technology as a vehicle for bullying and identification of potential problems associated with cyber bullying and victimization will aid parents, educators, and psychologists in developing intervention and prevention strategies. (Williams, & Guerra) [127]. According to Calvete, et al 2010 cyberbullying was significantly associated with the use of proactive aggression, justification of violence, exposure to violence, and less perceived social support of friends. Other reasons for cyberbullying are: envy, prejudice and intolerance for disability, religion, gender, shame, pride, guilt, and anger [82, 114, 128] Anonymity Approval, Boredom Feel Better, Instigate Jealousy, No perceived consequences Projection of feelings, Protection Reinvention of self and revenge. According to the definition of the National Crime Prevention Council, cyberbullying is the use of the internet, cell phones or other technologies to send or post a text or images intended to hurt or embarrass another person [129].

Cyberbullying can be carried out through several technology platforms, such as chat rooms, emails, photo sharing websites, blogs, forums, social networking cites, cell phones, online games and voice mail. Bullying in the cyber environment is much crueller and more dangerous than the "traditional" forms of bullying, which take place in the real world [130]. Reasons for that are primarily aspects of the web: the persistence, the ability to search and copy, as well as invisible audiences [131].

Because of the web persistence, a victim cannot hide anywhere, since the audience is not confined to a room, school yard or street, but presents a large online community. According to Dempsey et al. [94], two basic characteristics of cyberspace are dominant for cyberbullying: anonymity in cyberspace and better control of social interaction in the cyber world. Abusers can choose when they want to harass the victim, how (through which medium), and whether they wish to bully him/her in front of an audience. Cyberbullying makes a major impact on society; consequently, it has become intensive field of research. Although many researchers analyse causes and consequences of cyberbullying, only few suggest possible solutions for the prevention that include software systems beyond the usual ones based on key words [87] - [93].

Threats in cyberspace

Needless to say the potential damage of cyber-attacks therefore is quite large. One of the greatest threats is attacks targeting various critical infrastructure assets, such as telecommunications, transportation, power, financial services and defence. While such attacks may not likely be the scope of what some contributors call a "Digital Pearl Harbor", nonetheless attacks can be very economically damaging and disruptive. In fact, cyber-attacks on critical infrastructures are now quite common. Perhaps one of the most famous ones is the Estonian case in 2007. After the decision to move a Soviet World War II memorial to a different location, which inflamed the Russian public as well as a significant Russian minority in Estonia, a wave of cyber-attacks hit various Estonian government sites and businesses. With 98% of Estonian banking done electronically the disruption of bank sites paralyzed banking activity in the country. Even basic government communications were significantly affected by these attacks [120]

In fact, some contributors on the topic of cyber threats have already boldly declared that the cyber arms race has begun. There might be good reason for such statements as well because many nations have stated in their strategic doctrines the importance to develop offensive cyber capabilities and amongst them some of the major global powers, such as the United States, Russia and China [121]. In addition, the US has already established its Cyber Command with the goal of protecting its military and defence networks form a continuous barrage of many thousands of attacks [122]

Yet despite the development of offensive cyber capabilities by states and the seriousness of cyber threats in general, they have not been fully addressed in international forums or on a truly global level [123]

It has been widely recognized that the lack of clear and widely excepted definitions on concepts relevant to cyber threats has been one of the main hurdles in developing global agreements on cyber security. In addition, clearer definitions on various types of cyber-attacks and international norm setting is important even when dealing with already existing international agreements. It is not clear now if cyber-attacks should be viewed as aggression that is covered under Article 51 of the UN Charter or possibly under the solidarity clause in the Lisbon Treaty or even by Article 5 of the NATO treaty [124] If cyber space can be seen as the fifth domain of defence (along with land, sea, air and space) then cyber-attacks could possibly be considered the same as kinetic attacks and therefore possibly even merit a physical response.

Most of the literature on cyber threats has been written by or aimed at policy makers and therefore has not gone over any major theoretical considerations. This is somewhat of a loss because of the potential explanatory power theoretical considerations might bring to the table [125]

Thus in conclusion, the literature on cyber threats is still largely dominated by policy makers and professionals in the field rather than political scientists, though the amount of academic work done on it is growing at a significant rate due to the importance of the issue. As a result of this most literature is very pragmatic in nature with little to no theoretical considerations. Yet there is a large consensus concerning the types of threats faced, even though the scale and severity of the threats might still be subject to debate. additionally, there seems to be a great and in fact a near universal agreement about the need for a global response in order to adequately combats these threats…

While cyberspace has brought significant benefits to our lives, malicious activities to harm these benefits are increasing. Cyberspace, which anyone can utilize without geographic and time constraints, gives advantages asymmetrically to malicious attackers, not defenders. At the same time, the increasing dependency of socioeconomic activities on cyberspace and the evolution of organized and highly sophisticated methods, or modus operandi, of cyber-attacks that might be state sponsored have caused grave damages and exerted negative impacts on the people's daily lives and socio-economic activities, and consequently, threats against national security have become more serious year after year.

Additionally, due to the arrival of the interconnected and converged information society, malicious activities in cyberspace will cause extensive impact on all kinds of connected physical objects and services, and the damage caused by cyber-attacks will spread more rapidly and widely in physical space; therefore, it is anticipated that the people's living will be exposed to more immense cyber threats in the future. To prevent further aggravation of such threats, the creation of "free and fair cyberspace" must be in parallel with the creation of "secure cyberspace.

The tremendous growth of information technology has abruptly changed the world into global village. It has caused the distances to shrink and information to flow across the globe as it occurs. At the same time, it has also given boost to vulnerabilities, threats, frauds and criminals in the cyberspace. The ease of access, user friendly hacking tools and sophistication in cyber-attacks has infringed the privacy of the individuals, organizations and states. The threat in cyberspace is defined as the potential that can originate an undesired event in cyberspace and capable of causing damage to individual or state assets, systems or an organization [29].

Chapter Three

METHODOLOGY

Overview

This chapter describes the research approach used in collection of data for the study. In this chapter, the development and design of the instrument used were the population, sample size and sampling technique. Aside those, administration of questionnaire as well as the limitation of the study are captured in this chapter.

Research design

The research design that would be adopted for the study is the descriptive survey method. Such a design is non-experimental. It studies the relationship between non-manipulated variables in a natural setting. According to Gay 1992, descriptive survey involves collecting data in order to test hypothesis or to answer questions on the impact of the use of internet and social media in learning. Selected places are Ghana and the Czech Republic.

Best and Khan in1996 recommends the descriptive survey for generalizing from a sample to a larger population for inferences to be made about characteristics, attitudes or behaviour of the population.

Population

The population was strictly on students. Also, the population was selected in relation to the objectives of the study The research focused on both endowed and less endowed schools in Ghana as well as some schools in Europe (Czech Republic). This is to provide a clear picture on the impact of the use of the internet and social media in learning in these respective countries

Sample and Sampling Procedure

The simple random technique was used in the selection of students. Schools are limited to the capital of Ghana where the total number of High Schools in the region is Forty-one (41), out of the total, five (12.2%) were chosen to be used for the research.

To give an equal chance of being selected, a simple random technique was used in the selection of students, out of each school ,100 students in all were presented with student's questionnaire solicit their response, views and suggestions on the items in the instrument.

Instrument

The research instrument designed for the students was the questionnaire. This instrument was chosen because they are the best possible media through which the right kind of information could be solicited from the students to really ascertain with factual findings the impact of the use of the internet and social media in learning in these respective countries.

Questionnaire consisted of both closed and open-end items. The open-ended questions were presented to allow students to freely express their opinion in the items provided. The questionnaire was to seek educational information from the respondents. The researcher was interested in finding out the impact of the use of the internet and social media in learning. The remaining questions were put into sections which are directly related to the research question.

Although we had in mind other applicable research instrument, we found it appropriate to use the questionnaire since it has relative advantage in terms of easy documentation, time saving correspondents view within a relative shorter time. The respondents were strictly high school students in Ghana.

Data Collection Procedure

After developing the questionnaire, it was attached with a cover letter and were presented to Heads of the respective schools that researches were undertaken.

The researcher was introduced to the high school students from various disciplines, things were briefly explained to them about the purpose of the study so as to feel at ease in answering the instrument.

Therefore, the relationship between the respondents and the researcher was very lengthy, cordial, and recommendable in that, healthy environment and happily welcomed suggestions were given by the respondents. In effect, this aided the effective and efficient collection of data.

Data Analysis

The data collected were edited, coded and analysed. The statistical tool used in analysing the data was the descriptive statistics. The data were entered using the Statistical Package for Social Science (S.P.S.S.) In order to get the direction of the responses from the respondents, percentages and frequencies were used. A higher percentage of responses showed a favourable response from the respondents. However, a lower percentage showed an unfavourable response to a particular item in the questionnaire.

Limitation of the study

A number of difficulties were encountered while undertaking the research. Some of the students were afraid they will be penalized for giving certain responses that tend to give their school a bad image. Also, as a result of limited time inadequate funding, the researchers could not administer the questionnaires to the entire students in the selected schools.

Despite the challenges, the researcher was able to do this by explaining to the various heads of institutions that the study is for educational purposes. Also, I had to explain to students that the information they were providing would be kept highly confidential.

Chapter Four

RESULTS AND DISCUSSION

Overview

This chapter discusses the presentation and analysis of the data that was collected from the respondents in order to find answers to research questions.

Discussion of Preliminary Data

This section discusses the background information of the respondents. It deals with the sex, age distribution, and the level or grade of students from whom primary data in Ghana.

Table 1

Distribution of Students and Teachers Access to the Internet

Access to Internet		Yes		No
	No.	%	No	%
Teachers	15	30	35	70.
Students	30	30.0	70	70.0

Source: Field work, 2016

Table 1, indicates that out of 50 teachers, 15 have access to the internet while 35 did not have access to the internet. This implied that the majority of teachers in senior high schools does not have access to the internet. Also, out of (100) students, thirty of the students had access to the internet as against 70 which do not have access. Thus a majority of students don’t have access to the internet.

Tables 2 and 3 display the distribution of responses to research question one: how do students in senior high schools use the internet in their learning?

Frequency of use of the internet by students and teachers

Table 2

Distribution of Frequency of Use of the Internet by Students and Teachers

	Very Frequently		Frequently		Occasionally		Rarely		Very Rarely	
Frequency of use	No.	%	No.	%	No.	%	No.	%	No.	%
Teachers	3	6.0	7	14.0	10	20.0	12	2 4.	18	36.0
Students	15	15	20	20.0	25	25.0	25	25.0	15	15.0

Source: Field work, 2016

A higher percentage of both teachers and students in senior high schools does not have access to the internet as indicated in Table 2. Majority of them hardly used the internet. Only a few frequently used it. This means that despite the fact that, both students and teachers have access to the internet, its resources were not being fully exploited for the benefits of both students and teachers to actually improve teaching and learning experiences. The various uses of the internet in senior high schools as well as how often students used it for each reported purpose is summarized in Table 3 below.

Students’ use of the internet

Table 3

Distribution of students‟ use of the internet

Purpose	Very Often		Often		Sometimes		Rarely		Not at all	
	No.	%	No.	%	No.	%	No.	%	No.	%
For practice	8	8.0	16	16.0	23	23.0	18	18.0	35	35.0
Visit on–line libraries	5	5.0	7	7.0	14	14.0	13	13.0	61	61.0
Accessing information	5	5.0	9	9.0	18	18.0	29	29.0	39	39.0
Exchanging information	8	8.0	9	9.0	17	17.0	17	17.0	49	49.0
Join discussion groups	6	6.0	7	7.0	14	14.0	11	11.0	62	62.0

Source: Field work, 2016

Table 3 shows that a higher percentage of students did not use the internet for re- enforcing what they learnt in class, visiting online libraries, exchanging information with other students, accessing information to do their assignments and joining discussion groups. Table 2 also shows that the few students who used the internet very often used it for exchanging information with their peers and joining discussion groups. This observation confirms the finding from the Turkson *et al* (2007) study that the internet was popular among the youth but in the case of Ghana and any other developing countries, it is really difficult to access good, fast and reliable internet since securing internet is also very expensive or cost involving. However, through our findings it was discovered that, the internet was mostly used for non – academic activities such as internet theft, pornography and hacking, a small number of respondents used it more constructively often using the internet to practice what they learnt in school or to enhance learning.

Table 4: Ranking of frequently visited sites by the students in Ghana

Websites	Very Often		Often		Sometimes		Rarely		Not at all	
	No.	%	No.	%	No.	%	No.	%	No.	%
Google	57	57.0	29	29.0	9	9.0	3	3.0	2	2.0
YouTube	28	28.0	36	36.0	16	16.0	14	14.0	6	6.0
Facebook	30	30.0	35	35.0	25	25.0	6	6.0	4	4.0
Yahoo	9	9.0	15	15.0	30	30.0	20	20.0	26	26.0

Source: Field work, 2016

Also, from the above data, to solicit the information from respondents on frequently visited sites, they were presented with choices to really ascertain how often they visit those sites and to the sites they rarely visit or do not visit at all. It could be clearly seen that, google is the most visited site by student and the main reason is for research or searching purposes. The second most frequently visited site is Facebook which is a social media platform where students can connect with their peers from all over the world. This is then followed by YouTube where students can watch online tuition or tutorials videos, watching movies, musical videos and for other entertainment purposes. Yahoo is the least visited site by students since most students are not used to sending and receiving e-mails.

Extent of social media use

This question was intended to find out which social media platforms were used mostly by the respondents in the quest to compare the situation in Ghana. From the data analysed, it was found that most of the respondents used by far Facebook. 96 out of the 100 respondents representing 96% said they used Facebook. They went on to say that it was their number one social media platform. This is suggestive that Facebook was the most popular social media platform in Ghana today. Comparing Facebook to other social media platforms revealed that the respondents ranked YouTube as their second used social media platform followed by Twitter, Google+, LinkedIn, Myspace, Instagram, Pinterest, Tumblr, and foursquare. This result reflects the results the survey by Frank N. Magid cited in Meeker & Wu, 2013 based on a study of 2K social media users aged 12-64, who asked respondents which social media they used

Frequency of visits to social networks

After finding out the extent of social media use in Ghana, there was the need to find out how often respondents visited social media sites. The data analysis revealed that 66 out of the 100 respondents representing 66 % said they visited social networks several times in a day. 15% said once a day, 10 % visited several times a week, while 5% said once a week and 4% do not visit any social media at all. Even though the number of hours spent by Ghanaians was not measured, the result was quit reflective of the global average as well the time spent by Americans; the average American spends over 3 hours per day on social networks, with usage trending higher among females, under-35s, business owners, and executives (Vivion, 2013).

Activity with social media networks

Furthermore, respondents were asked to state how often they actively used social media networks. 63% stated that they actively use and partake in such things as comment, posts, tweets, amongst others with social media networks several times a day, 11% used them once a day, 11% said several times a week, 4% did so once a week with 1% using them several times a month.1% went on to affirm that they actively used social media networks once every month with no respondent using it several times a year. However, 8% said they used them less often.

Ranking of activities with social media networks

Respondents were asked to list their activities on social media and rank them according to the most used to the least used such as: reading as in the reading of posts, comments and tweets; sharing as in the sharing of posts and contributions; commenting as in commenting on contributions; and contribution as in tweets/posts. Majority of the respondents (71%) ranked reading on social media as their number one and most used activity, 21% stated that sharing was their number one activity, 5% went for commenting with 3% choosing contribution. It can be concluded from these responses that the majority of Ghanaians on social media were more involved in such activities as reading posts, comments and tweets.

Table 5: Population Growth and Internet Usage in Ghana (1999-2011)

YEAR	Users	Population	% Pen.	Usage Source
2011	2,085,501	24,791,073	8.4 %	**ITU**
2010	1,297,000	24,339,838	5.3 %	**ITU**
2009	997,000	23,887,812	4.2 %	**ITU**
2008	880,000	23,382,848	3.8 %	**ITU**
2007	609 800	21 801 662	2.8 %	**ITU**
2006	401,300	21,501,842	1.8 %	**ITU**
2005	368,000	21,029,850	1.6 %	**ITU**
2001	40,500	19,101,878	0.3 %	**ITU**
2000	30,000	18,881,600	0.2 %	**ITU**
1999	**20,000**	**18,599,549**	**0.1 %**	**ITU**

Source: Ghana Statistical Service Department.

We could see from this data that, in spite the fact that, till now accessing good, fast and reliable internet in Ghana and other developing countries is a problem and also expensive nonetheless, the usage of internet as well as its users are increasing each year as the days go by which is an indication that the access to the internet will keep improving and will always get better in Ghana.

Table 6: Purpose of internet usage in Ghana by students

Purpose of internet usage	Percentage					
	Never	Rarely	Occasionally	Frequently	Always	Total
Entertainment	12.5	24.4	51	9	3.1	100
Education	0.625	5	25	45.625	23.75	100
Work-related Research	10.63	13.12	36.25	31.25	8.75	100
Personal finance (banking, stock trading)	26.25	23.75	34.375	13.125	2.5	100
Current events (news, sports and weather)	5.63	15	33.75	33.75	11.87	100
Travel-related (research, reservations)	38.18	28.75	19.37	8.7	5	100
Product information gathering	18.75	21.25	40.625	14.375	5	100
Making purchase from online merchants	52.4	17.5	18.75	6.35	5	100
Communicating with others (chat/email)	4.38	7.5	30	25	33.12	100

Source: Field work, 2016

ENTERTAINMENT

The internet provides a lot entertainment such musical entertainment, free videos, computer games, social networking, chatting etc. The internet is a means by which people can gain access to a bundle of services: The research revealed that, with entertainment 3.1% of respondents always use the internet for it. 9% frequently, 51% occasionally, 24.4% rarely use it and 12.5% never use it.

EDUCATION

Internet as a powerful tool for education provides learning platforms including online educational videos, Virtual Classrooms, Webcasting, Wikis etc. The research revealed that, more respondents use the internet for educational purposes especially for research and sending information to colleagues and lecturers. 23.7% use it always for educational purposes, 45.6% use it frequently, 25% occasionally, 5% rarely use it and only o,6% never use it for educational purposes.

RELATED WORK

A lot more Ghanaians and as well students now frequently use the internet for work-related research. The research showed 31.25% for frequent users, 36.25% for occasional users, 8.75% always, 13.12% rarely use it and 10.63% never use it for work-related research.

PERSONAL FINANCE (BANKING AND STOCK TRADING)

The internet provides the tool and power to keep track of financial trends, search for loans, account balance, and perform a variety of other essential financial tasks. Using the internet for banking and stock trading has shown a slight growth. 26.25% never use the internet for banking and stock trading. 23.75% rarely use it, 34.37 use it occasionally,13.13% frequently and 2.5% always use it for banking and stock trading

CURRENT AFFAIR (NEWS, SPORTS AND WEATHER)

The internet is now an important medium for people to search for the latest happenings around the world by a click of the mouse. Internet users get access to real time news and other information; the internet is the best choice for people to find all the latest happenings and thus stay informed. More Ghanaians now depend on the internet for sports, weather, economic and political news events [104]. The research revealed that, 33.75% frequently depend on it, another 33.75% also occasionally use it for news items, 11.87% always depend on it, 15% rarely use it and 5.63% never use it for news items

TRAVEL-RELATED (RESEARCH RESERVATION)

Internet is well suited for travel products and services with the synergy for electronic environment [105]. With travelling activities, very few Ghanaians depend on the internet for the search of information. 38.18% had never used the internet for it. 28.75% rarely use it, 19.37% occasionally and only 5% always depend on it for information concerning travelling.

PRODUCT INFORMATION

Using the internet to search for information on products and services has been one of the key usages [106]. The internet is one of the fastest growing technologies. The research revealed that, 40.6% of Ghanaians occasionally depend on the internet for product information gathering.14.4% frequently, 5% always, 21.25%rarely use it and 18.75% never use it.

MAKING PURCHASES ONLINE

Internet access and web applications, services and platforms improve productivity and make it easier for businesses to collaborate and access new markets via digital distribution and online retail; increases consumer choice and strengthens competition. The internet provides consumers the convenience of shopping anytime and anywhere, getting better access to information and a broader selection of products, comparing prices or obtaining opinions from other consumers.

Though internet provides global access to online goods and services as high as 52.4% of respondents never use internet to make purchases online, 17.5% rarely use it. 18.75% occasionally, 6.35% frequently and only 5% use it always to make purchases. Although in Ghana the internet is becoming more accessible, it is not mainly used by the respondents for online shopping. Online sellers must adopt strategies to maintain their appeal to consumers and it must extend sensitive orientations on ways of boosting online sales. The use of the internet for transaction purposes will vastly increases the value of the infrastructure, and thus create the incentives for organizations to build more ICT infrastructure. The ability of the banking industry in Ghana to capitalize on the internet will enhance economic growth; make financial services cost effective and competitive, and more accessible for customers.

COMMUNICATING ONLINE

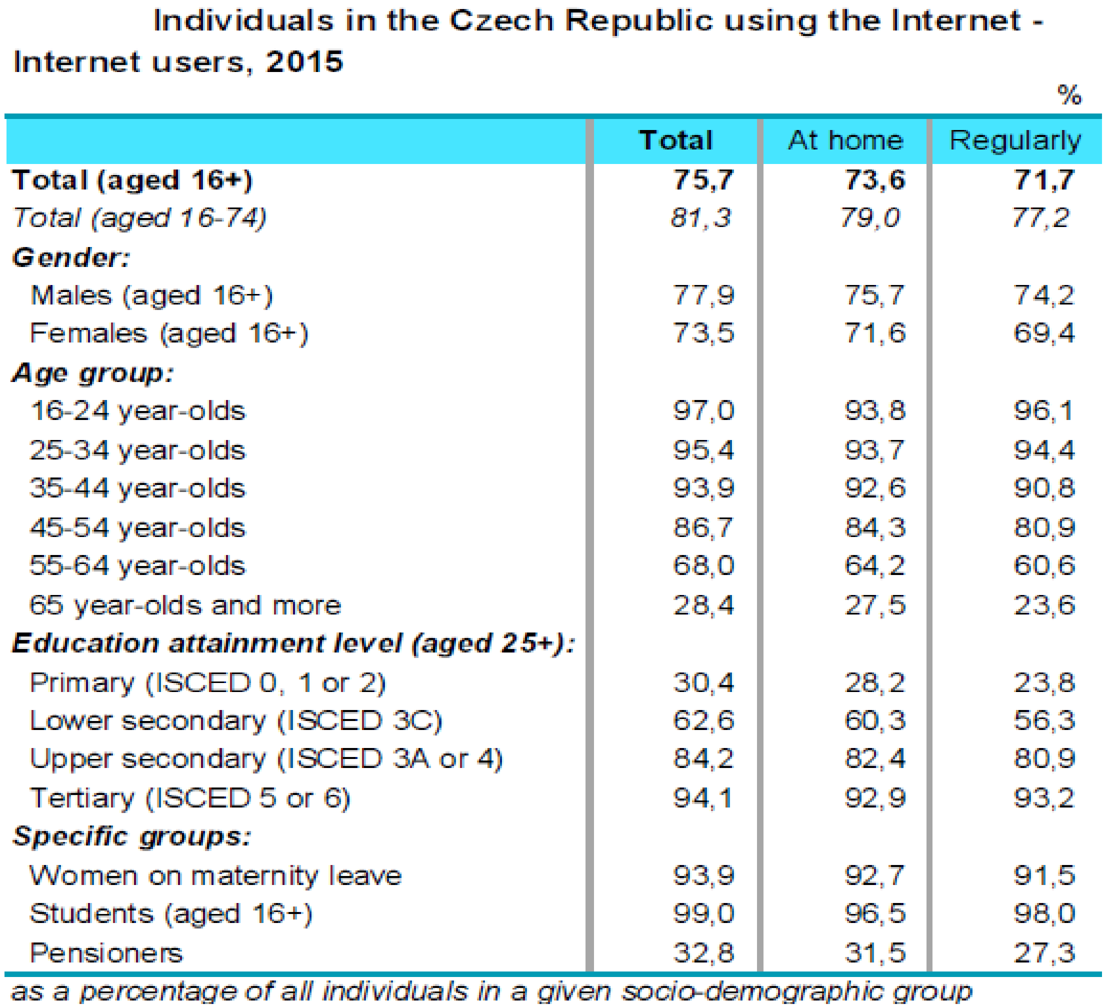
Access to the internet offers the possibility for people to communicate with each other and to access information of all types, without considerable spatial or temporal limits [107]. The internet provides a many-to-many communication medium, unlike the one-to-many model of the traditional mass media. The research showed that, 33% always use internet for online communication. 25% frequently, 30% occasionally,7.5% rarely use it and 4% never use it for online

The internet is the fastest growing technology. It's prominent in almost every country, and Ghana is no exception. The research revealed that 48% of Ghanaians have been using internet frequently, over the past five years. This is shown on table 2. Above 35.6% between two to five years and 15.6%, one year.

THE USE OF INTERNET IN EDUCATION. SOCIAL MEDIA AND OTHER ACTIVITIES IN THE CZECH REPUBLIC

The number of Czech internet users has been growing relatively fast in the last decade. Whereas in 2005 (the first World Internet Project Survey), the half of Czech population of the 15+ age group used the internet, in 2014 it was already four fifths of the population. The only age group with no increase was the 75+ people, where the differences are below the level of statistical error.

Table 7



Individuals in the Czech Republic using the Internet - Internet users, 2015

%

	Total	At home	Regularly
Total (aged 16+)	**75,7**	**73,6**	**71,7**
Total (aged 16-74)	*81,3*	*79,0*	*77,2*
Gender:			
Males (aged 16+)	77,9	75,7	74,2
Females (aged 16+)	73,5	71,6	69,4
Age group:			
16-24 year-olds	97,0	93,8	96,1
25-34 year-olds	95,4	93,7	94,4
35-44 year-olds	93,9	92,6	90,8
45-54 year-olds	86,7	84,3	80,9
55-64 year-olds	68,0	64,2	60,6
65 year-olds and more	28,4	27,5	23,6
Education attainment level (aged 25+):			
Primary (ISCED 0, 1 or 2)	30,4	28,2	23,8
Lower secondary (ISCED 3C)	62,6	60,3	56,3
Upper secondary (ISCED 3A or 4)	84,2	82,4	80,9
Tertiary (ISCED 5 or 6)	94,1	92,9	93,2
Specific groups:			
Women on maternity leave	93,9	92,7	91,5
Students (aged 16+)	99,0	96,5	98,0
Pensioners	32,8	31,5	27,3

as a percentage of all individuals in a given socio-demographic group

Source: Czech statistical Service Department

This table consist of people from 16+ or in other words 16 years and over. Out of a total of 79. 73.6 uses the internet at home whereas as a total of 77.2, 71.7 uses the internet regularly. Also, 75.7 representing males above 16 years uses the internet at home, 74.2 use the internet regularly. 71.6 of females above 16 years represents those who uses the internet at home and 69.4 of females uses the internet regularly.

16-24 years = 93.8 of them uses the internet at home and 96.1 uses the internet regularly.

25-34 years = 93.7 of them uses the internet at home and 94.4 uses the internet regularly.

35-44 years = 92.6 of them uses the internet at home and 90.8 uses the internet regularly.

45-54 years = 84.3 of them uses the internet at home and 80.9 uses the internet regularly.

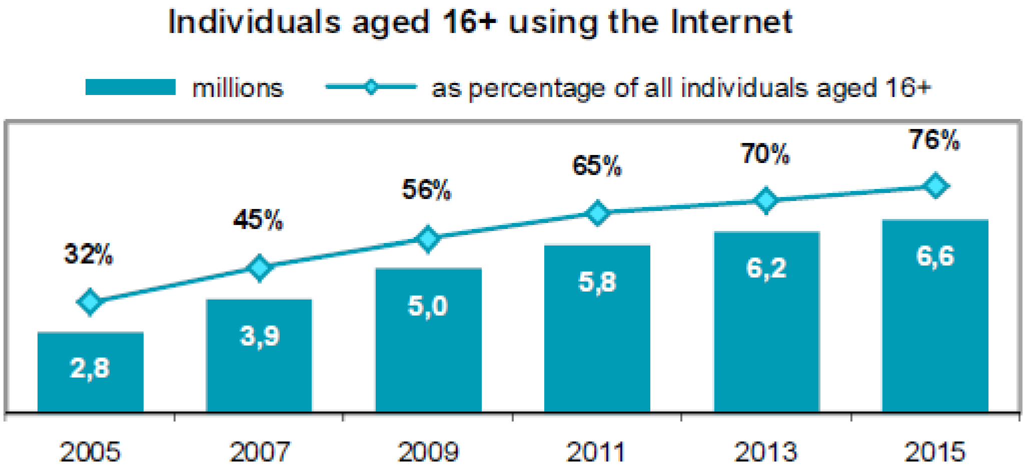
55-64 years = 64.2 of them uses the internet at home and 60.6 uses the internet regularly

65+ years = 27.5 of them uses the internet at home and 23.6 uses the internet regularly

Educational Attainment:

28.2 of people who have attained primary education uses the internet at home whereas 23.8 uses internet regularly.60.3 with lower secondary educational attainment uses the internet at home as 56.3 uses the internet regularly.82.4 of people with upper secondary also uses the internet at home and 80.9 uses the internet regularly. Last but not the least, 92.9 uses the internet at home as 93.2 uses the internet regularly.

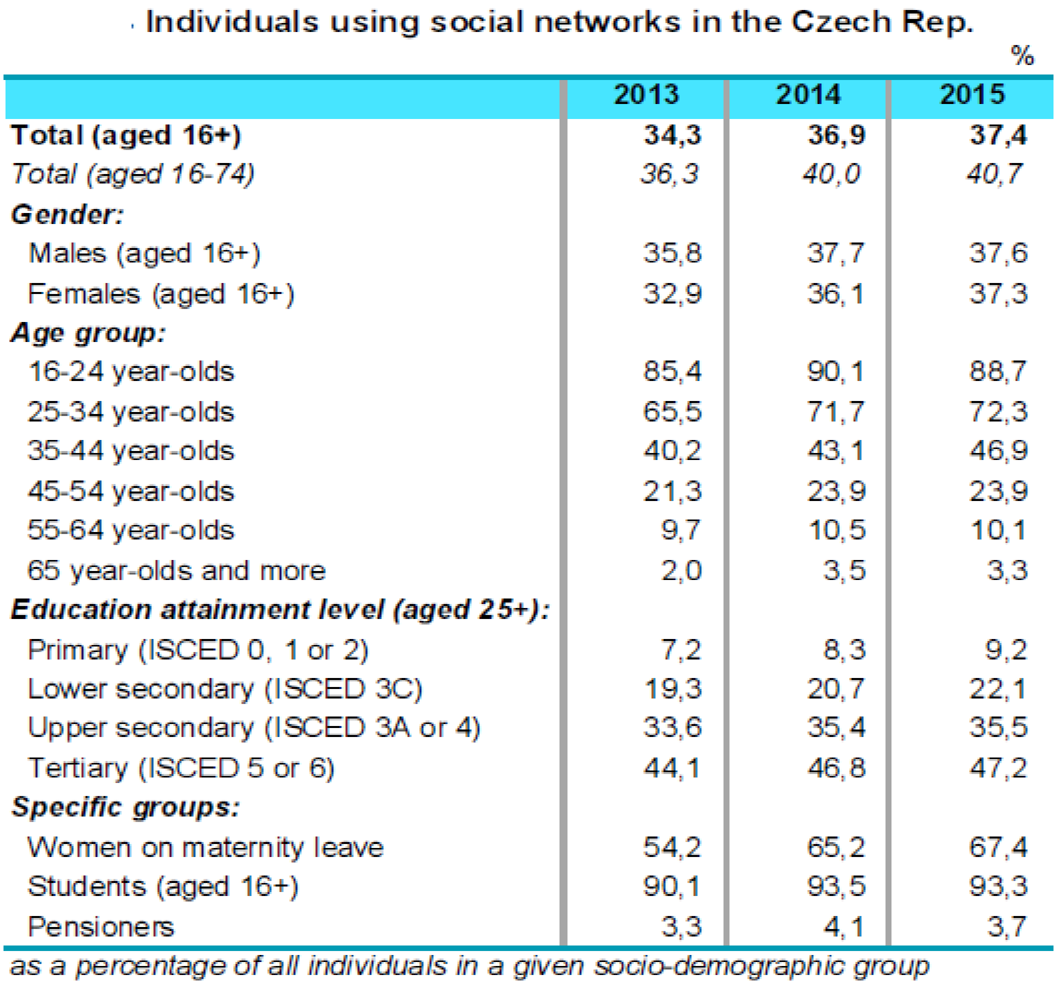
Finally, 96.5% of students above 16 years in general uses the internet at home while 98% of them uses the internet regularly.



Source: Czech Statistical Office, ICT use in households

The above graph shows the percentage growth of internet usage of people 16 years and over from 2005 to 2015 with the percentage increasing from 32% from 2005 to 76% in 2015.

Table 8



Individuals using social networks in the Czech Rep.

%

	2013	2014	2015
Total (aged 16+)	**34,3**	**36,9**	**37,4**
Total (aged 16-74)	*36,3*	*40,0*	*40,7*
Gender:			
Males (aged 16+)	35,8	37,7	37,6
Females (aged 16+)	32,9	36,1	37,3
Age group:			
16-24 year-olds	85,4	90,1	88,7
25-34 year-olds	65,5	71,7	72,3
35-44 year-olds	40,2	43,1	46,9
45-54 year-olds	21,3	23,9	23,9
55-64 year-olds	9,7	10,5	10,1
65 year-olds and more	2,0	3,5	3,3
Education attainment level (aged 25+):			
Primary (ISCED 0, 1 or 2)	7,2	8,3	9,2
Lower secondary (ISCED 3C)	19,3	20,7	22,1
Upper secondary (ISCED 3A or 4)	33,6	35,4	35,5
Tertiary (ISCED 5 or 6)	44,1	46,8	47,2
Specific groups:			
Women on maternity leave	54,2	65,2	67,4
Students (aged 16+)	90,1	93,5	93,3
Pensioners	3,3	4,1	3,7

as a percentage of all individuals in a given socio-demographic group

Source: Czech Statistical Office, ICT use in households

This table consist of people from 16+ or in other words 16 years and over using the internet for social networking purposes such as Facebook, twitter, viber etc,. 34.3, 36.9 and 37.4 percent uses the internet for social networking for 2013, 2014 and 2015 respectively. Also, 35.8, 37.7, 37.6 also depicting the percentage of males who uses the internet for social networking as of 2013,2014 and 2015 respectively. Their female counterparts above 16 years who also uses the internet for social networking are 32.9, 36.1, and 37.6 percent as 2013, 2014 and 2015 .

16-24 years = 85.4, 90.1 and 88.7 uses the internet for social networking as of 2013-2015.

25-34 years = 65.5, 71.7 and 72.3 uses the internet for social networking as of 2013-2015

35-44 years = 40.2, 43.1 and 46.9 uses the internet for social networking as of 2013-2015

45-54 years = 21.3, 23.9 and 23.9 uses the internet for social networking as of 2013-2015

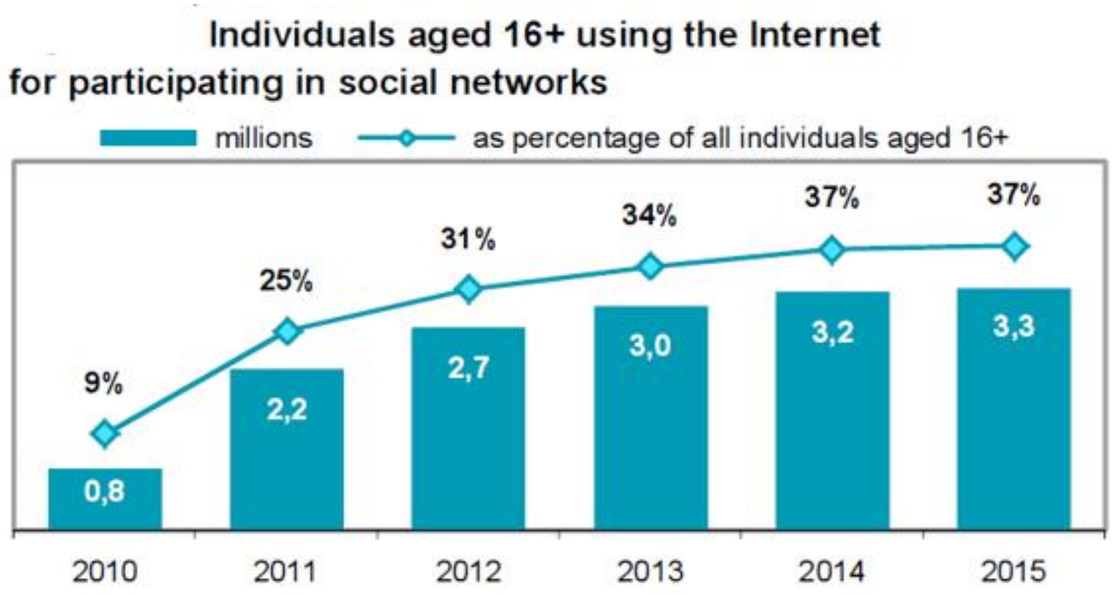
55-64 years = 9.7, 10.5 and 10.1 uses the internet for social networking as of 2013-2015

65+ years = 2.0, 3.5 and 3.3 uses the internet for social networking as of 2013-2015

Educational Attainment:

7.2, 8.3,9.2 percent of people who have attained primary education uses the internet as of 2013-2015 for social networking. Also, 19.3, 20.7, 22.1 percent of people with lower secondary educational attainment uses the internet for social networking as of 2013-2015. 33.6, 35.4 and 35.5 of people with upper secondary as well also uses the internet for social network as of 2013-2015. Last but not the least, 44.1, 46.8 and 47.2 percent of people with tertiary education uses the internet for social network as of 2013-2015.

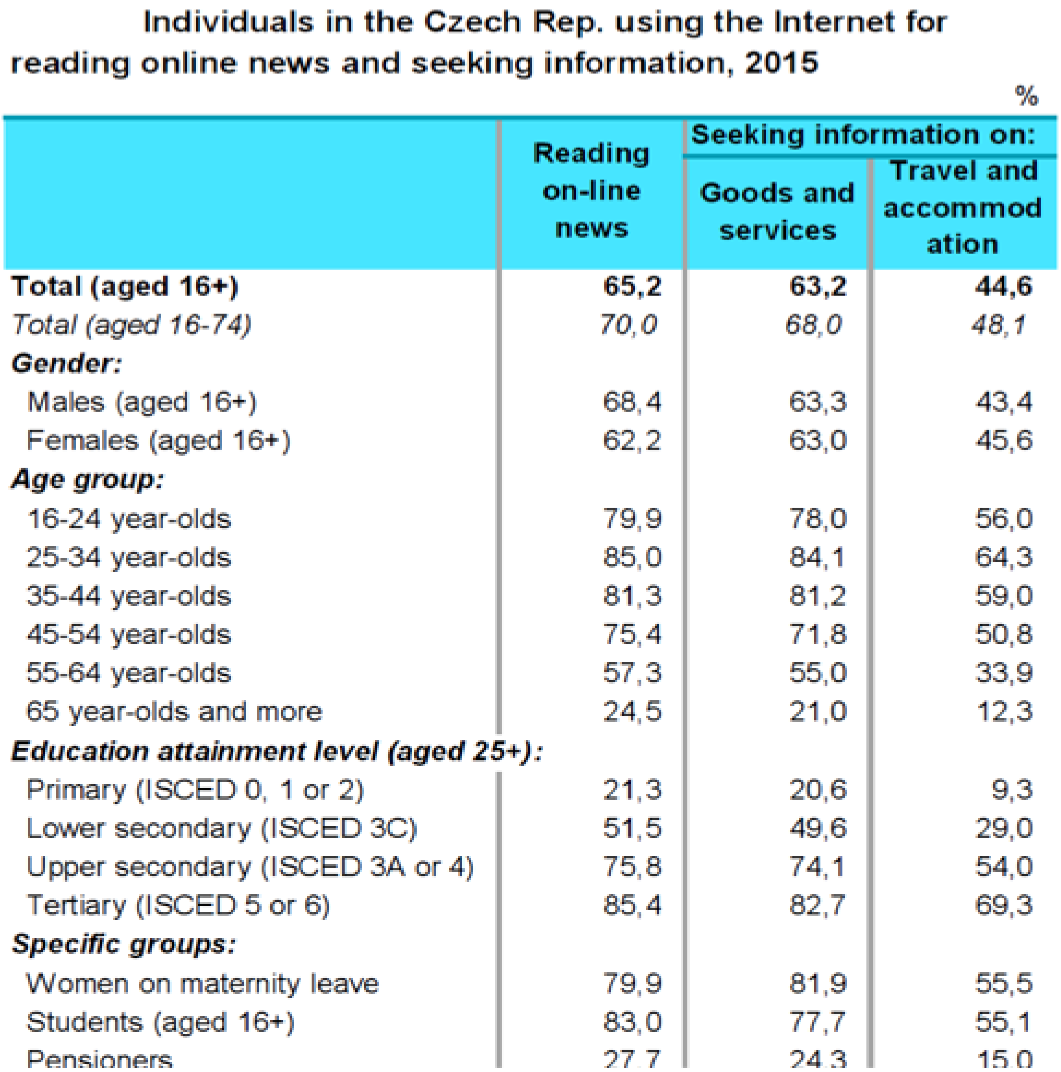
Finally, 90.1% of students above 16 years in general uses the internet for social network purpose in 2013 while 93.5% in 2014 and 93.3 in 2015.



Source: Czech Statistical Office, ICT use in households

The above graph shows the percentage growth of internet usage of people 16 years and over for participating in social networks from 2010 to 2015 with the percentage increasing from 9% in 2005 to 37% in 2015

Table 9



Individuals in the Czech Rep. using the Internet for reading online news and seeking information, 2015

%

	Reading on-line news	Seeking information on:	
		Goods and services	Travel and accommodation
Total (aged 16+)	**65,2**	**63,2**	**44,6**
Total (aged 16-74)	*70,0*	*68,0*	*48,1*
Gender:			
Males (aged 16+)	68,4	63,3	43,4
Females (aged 16+)	62,2	63,0	45,6
Age group:			
16-24 year-olds	79,9	78,0	56,0
25-34 year-olds	85,0	84,1	64,3
35-44 year-olds	81,3	81,2	59,0
45-54 year-olds	75,4	71,8	50,8
55-64 year-olds	57,3	55,0	33,9
65 year-olds and more	24,5	21,0	12,3
Education attainment level (aged 25+):			
Primary (ISCED 0, 1 or 2)	21,3	20,6	9,3
Lower secondary (ISCED 3C)	51,5	49,6	29,0
Upper secondary (ISCED 3A or 4)	75,8	74,1	54,0
Tertiary (ISCED 5 or 6)	85,4	82,7	69,3
Specific groups:			
Women on maternity leave	79,9	81,9	55,5
Students (aged 16+)	83,0	77,7	55,1
Pensioners	27,7	24,3	15,0

Source: Czech Statistical Office, ICT use survey in households

This table depicts people from 16+ or in other words 16 years and over. Out of a total of 70%, 65.2% uses the internet for reading on-line news. 63.2 % out of 68% also uses the internet to seek information on goods and services and in addition to this point, 44.6% out of 48.1% also uses the internet to seek information about travel and accommodation issues. Furthermore, 68.4 representing males above 16 years uses the internet for reading online news, 63.3. % use the internet also for seeking information on goods and services as 43.4% uses the internet for travelling and accommodation purposes. With respect to their female counterparts, 62.2 representing females above 16 years uses the internet for reading online news, 63% use the internet also for seeking information on goods and services as 45.6% uses the internet for travelling and accommodation purposes.

16-24 years = 79.9% of them uses the internet for reading news online, 78% uses the internet to seek information about goods and services as 56% of this age category also uses the internet for travelling and accommodation issues.

25-34 years = 85% of them uses the internet for reading news online, 84.1% uses the internet to seek information about goods and services as 64.3% of this age category also uses the internet for travelling and accommodation issues.

35-44 years = 81.3% of them uses the internet for reading news online, 81.2% uses the internet to seek information about goods and services as 59% of this age category also uses the internet for travelling and accommodation issues.

45-54 years = 75.4% of them uses the internet for reading news online, 71.8% uses the internet to seek information about goods and services as 50.8% of this age category also uses the internet for travelling and accommodation issues

55-64 years = 57.3% of them uses the internet for reading news online, 55% uses the internet to seek information about goods and services as 33.9% of this age category also uses the internet for travelling and accommodation issues

65+ years = 24.5% of them uses the internet for reading news online, 21% uses the internet to seek information about goods and services as 12.3% of this age category also uses the internet for travelling and accommodation issues or purposes

Educational Attainment:

Primary level

21.3 % of the people uses the internet for reading news online, 20.6 % of persons with primary level of education also uses the internet to seek information about goods and services as 9.3% uses the internet for travelling and accommodation purposes.

Lower secondary

51.5 % of the people with lower secondary education uses the internet for reading news online, 49.6 % of this same educational level also uses the internet to seek information about goods and services as 29% uses the internet for travelling and accommodation purposes

Upper secondary

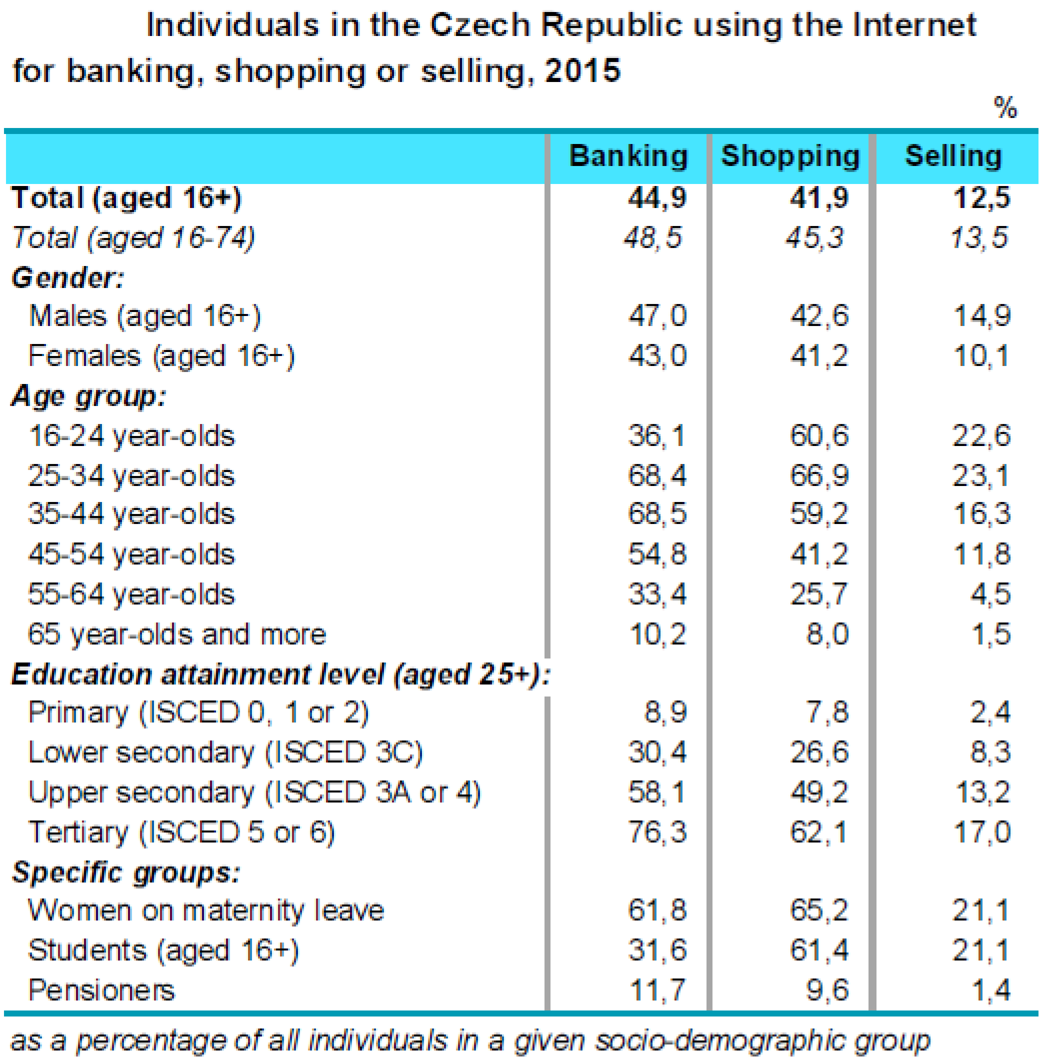
75.8 % of the people with upper secondary education uses the internet for reading news online, 74.1 % of this same educational level also uses the internet to seek information about goods and services as 54% uses the internet for travelling and accommodation purposes

Tertiary educational level

85.4 % of the people with tertiary education uses the internet for reading news online, 82.7 % of this same educational level also uses the internet to seek information about goods and services as 69.3% uses the internet for travelling and accommodation purposes

Finally, 83% of students above 16 years uses the internet for reading news online. 77.7% of students use the internet to seek information about goods and services as 55.1 % of students in general above 16 years also uses the internet for travelling and accommodation purposes

Table 10



Individuals in the Czech Republic using the Internet for banking, shopping or selling, 2015

%

	Banking	Shopping	Selling
Total (aged 16+)	**44,9**	**41,9**	**12,5**
Total (aged 16-74)	*48,5*	*45,3*	*13,5*
Gender:			
Males (aged 16+)	47,0	42,6	14,9
Females (aged 16+)	43,0	41,2	10,1
Age group:			
16-24 year-olds	36,1	60,6	22,6
25-34 year-olds	68,4	66,9	23,1
35-44 year-olds	68,5	59,2	16,3
45-54 year-olds	54,8	41,2	11,8
55-64 year-olds	33,4	25,7	4,5
65 year-olds and more	10,2	8,0	1,5
Education attainment level (aged 25+):			
Primary (ISCED 0, 1 or 2)	8,9	7,8	2,4
Lower secondary (ISCED 3C)	30,4	26,6	8,3
Upper secondary (ISCED 3A or 4)	58,1	49,2	13,2
Tertiary (ISCED 5 or 6)	76,3	62,1	17,0
Specific groups:			
Women on maternity leave	61,8	65,2	21,1
Students (aged 16+)	31,6	61,4	21,1
Pensioners	11,7	9,6	1,4

as a percentage of all individuals in a given socio-demographic group

Source: Czech Statistical Office, ICT use survey in households

This table depicts people from 16+ or in other words 16 years and over. Out of a total of 48.5%, 44.9% uses the internet for on-line banking services. 41.9 % out of 45.3% also uses the internet for online shopping activities or e-commerce purposes and in addition to this point, 12.5% out of 13.5% also uses the internet for selling purposes.

Furthermore, 47% representing males above 16 years uses the internet for on-line banking services, 42.6. % use the internet also for online shopping activities or e-commerce purposes as 14.9% uses the internet for selling purposes. With respect to their female counterparts, 43% representing females above 16 years uses the internet for online banking services, 41.2% use the internet also for online shopping activities or e-commerce purposes as 10.1. % uses the internet for selling purposes.

16-24 years = 36.1% of them uses the internet for online banking services, 60.6% uses the internet for online shopping or e-commerce purposes as 22.6% of this age category also uses the internet for selling purposes.

25-34 years = 68.4% of them uses the internet for online banking services, 66.9% uses the internet for online shopping or e-commerce purposes as 23.1% of this age category also uses the internet for selling purposes.

35-44 years = 68.5% of them uses the internet for online banking services, 59.2% uses the internet for online shopping or e-commerce purposes as 16.3% of this age category also uses the internet for selling purposes.

45-54 years = 54.8% of them uses the internet for online banking services, 41.2% uses the internet for online shopping or e-commerce purposes as 11.8% of this age category also uses the internet for selling purposes

55-64 years = 33.4% of them uses the internet for online banking services, 25.7% uses the internet for online shopping or e-commerce purposes as 4.5% of this age category also uses the internet for selling purposes

65+ years = 10.2% of them uses the internet for online banking services, 8% uses the internet for online shopping or e-commerce purposes as 1.5% of this age category also uses the internet for selling purposes

Educational Attainment:

Primary level

8.9 % of the people uses the internet for online banking services, 7.8 % of persons with primary level of education also uses the internet for online shopping or e-commerce purposes as 2.4% uses the internet for selling purposes.

Lower secondary

30.4 % of the people with lower secondary educational attainment uses the internet for online banking services, 26.6 % of persons with this same educational level also uses the internet for online shopping or e-commerce purposes as 8.3% uses the internet for selling purposes

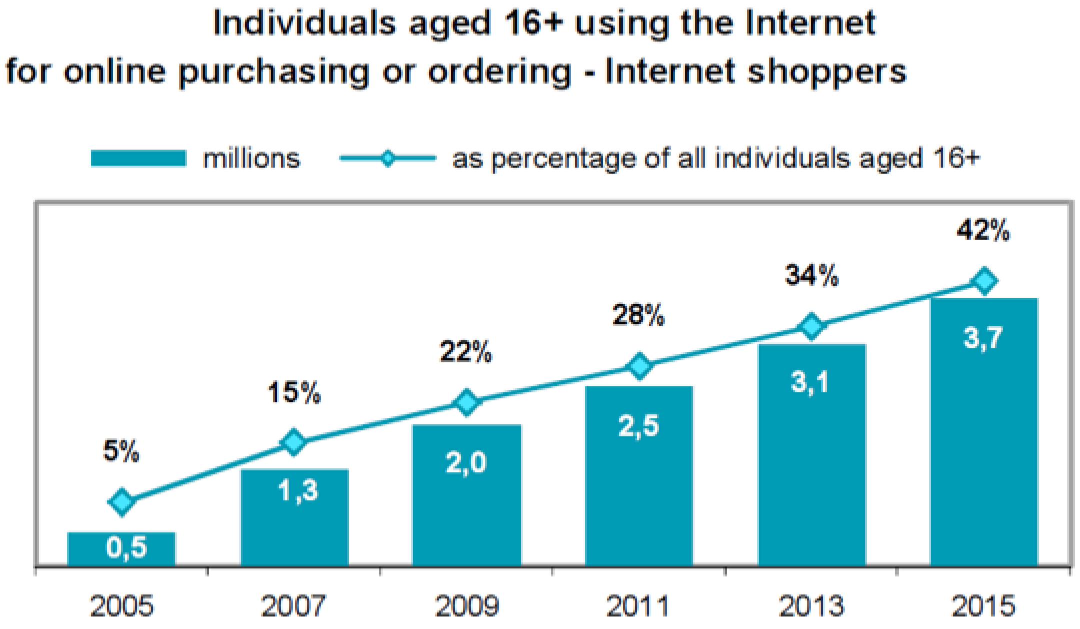
Upper secondary

58.1 % of the people with upper secondary educational attainment uses the internet for online banking services, 49.2 % of persons with this same educational level also uses the internet for online shopping or e-commerce purposes as 13.2% uses the internet for selling purposes

Tertiary educational level

76.3 % of the people with tertiary educational attainment uses the internet for online banking services, 62.1 % of persons with this same educational level also uses the internet for online shopping or e-commerce purposes as 17% uses the internet for selling purposes

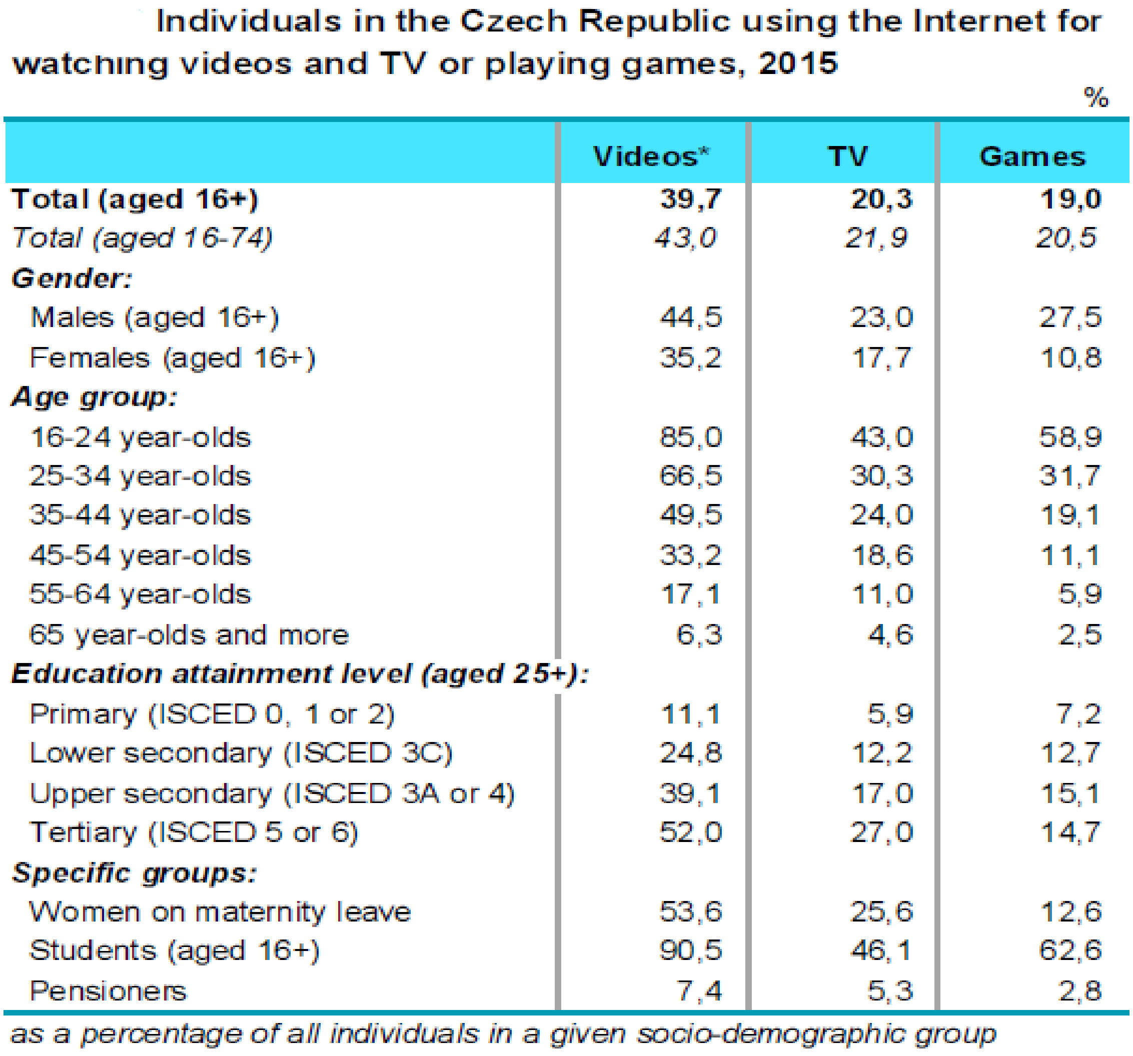
Finally, 31.6% of students above 16 years uses the internet for banking services online. 61.4% of students use the internet for online shopping or e- commerce purposes as 21.1 % of students in general above 16 years also uses the internet for selling purposes


Individuals aged 16+ using the Internet for online purchasing or ordering - Internet shoppers

Source: Czech statistical Service Department

The above graph shows the percentage growth of individuals over 16 years using the internet for online purchasing, ordering or internet shopping. The pattern increased from 5% in 2005 to 42% in 2015

Table 11



Individuals in the Czech Republic using the Internet for watchıng videos and TV or playing games, 2015

%

	Videos*	TV	Games
Total (aged 16+)	**39,7**	**20,3**	**19,0**
Total (aged 16-74)	*43,0*	*21,9*	*20,5*
Gender:			
Males (aged 16+)	44,5	23,0	27,5
Females (aged 16+)	35,2	17,7	10,8
Age group:			
16-24 year-olds	85,0	43,0	58,9
25-34 year-olds	66,5	30,3	31,7
35-44 year-olds	49,5	24,0	19,1
45-54 year-olds	33,2	18,6	11,1
55-64 year-olds	17,1	11,0	5,9
65 year-olds and more	6,3	4,6	2,5
Education attainment level (aged 25+):			
Primary (ISCED 0, 1 or 2)	11,1	5,9	7,2
Lower secondary (ISCED 3C)	24,8	12,2	12,7
Upper secondary (ISCED 3A or 4)	39,1	17,0	15,1
Tertiary (ISCED 5 or 6)	52,0	27,0	14,7
Specific groups:			
Women on maternity leave	53,6	25,6	12,6
Students (aged 16+)	90,5	46,1	62,6
Pensioners	7,4	5,3	2,8

as a percentage of all individuals in a given socio-demographic group

Source: Czech statistical Service Department

This table depicts people from 16 years and over. Out of a total of 43%, 37.9% uses the internet for watching videos. 21.9 % out of 20.3% also uses the internet for watching TV and in addition to this point, 20.5% out of 19% also uses the internet for online gaming.

Furthermore, 44.5% representing males above 16 years uses the internet for watching videos, 23 % use the internet also for watching TV online as 27.5% uses the internet for online gaming. With respect to their female counterparts, 35.2% representing females above 16 years uses the internet for watching videos online, 17.7% use the internet also for watching TV online as 10.8. % uses the internet for online gaming

16-24 years = 85% of them uses the internet for watching videos, 43% uses the internet for watching TV online as 58.9% of this age category also uses the internet for online gaming.

25-34 years = 66.5% of them uses the internet for watching videos, 30.3% uses the internet for watching TV online as 31.7% of this age category also uses the internet for online gaming.

35-44 years = 49.5% of them uses the internet for watching videos, 24% uses the internet for watching TV online as 19.1% of this age category also uses the internet for online gaming.

45-54 years = 33.2% of them uses the internet for watching videos, 18.6% uses the internet for watching TV online as 11.1% of this age category also uses the internet for online gaming.

55-64 years = 17.1% of them uses the internet for watching videos, 11% uses the internet for watching TV online as 5.9% of this age category also uses the internet for online gaming.

65+ years = 6.3% of them uses the internet for watching videos, 4.6% uses the internet for watching TV online as 2.5% of this age category also uses the internet for online gaming.

Educational Attainment:

Primary level

11.1 % of the people uses the internet for watching online videos, 5.9 % of persons with primary level of education also uses the internet for watching TV online as 7.2% uses the internet for online gaming

Lower secondary

24.8 % of the people with lower secondary educational attainment uses the internet for watching online videos, 12.2 % of persons with this same educational level also uses the internet for watching TV online as 12.7% uses the internet for online gaming purposes.

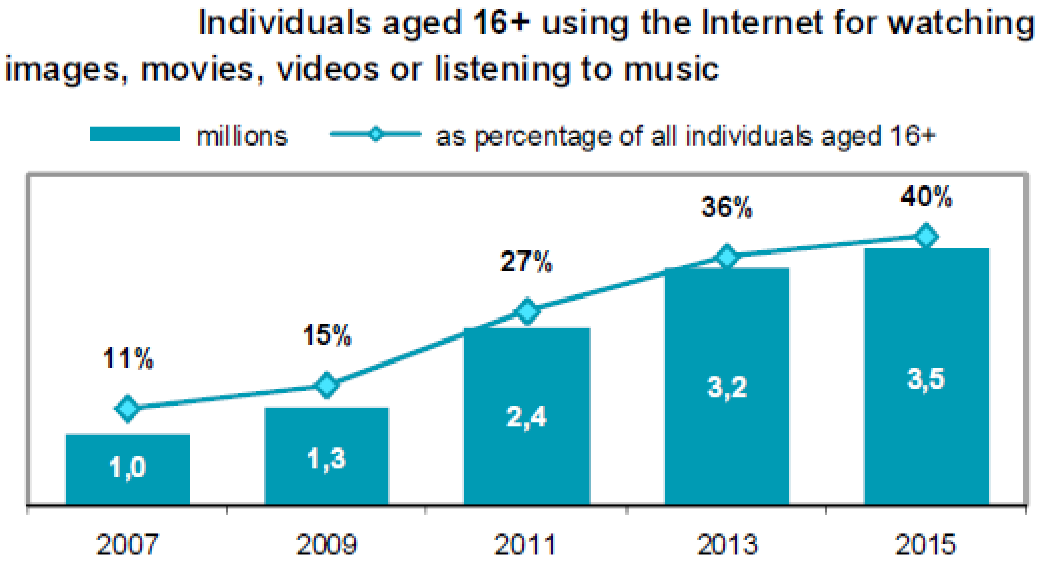
Upper secondary

39.1 % of the people with lower secondary educational attainment uses the internet for watching online videos, 17 % of persons with this same educational level also uses the internet for watching TV online as 15.1% uses the internet for online gaming purposes

Tertiary educational level

52 % of the people with lower secondary educational attainment uses the internet for watching online videos, 27 % of persons with this same educational level also uses the internet for watching TV online as 14.7% uses the internet for online gaming purposes.

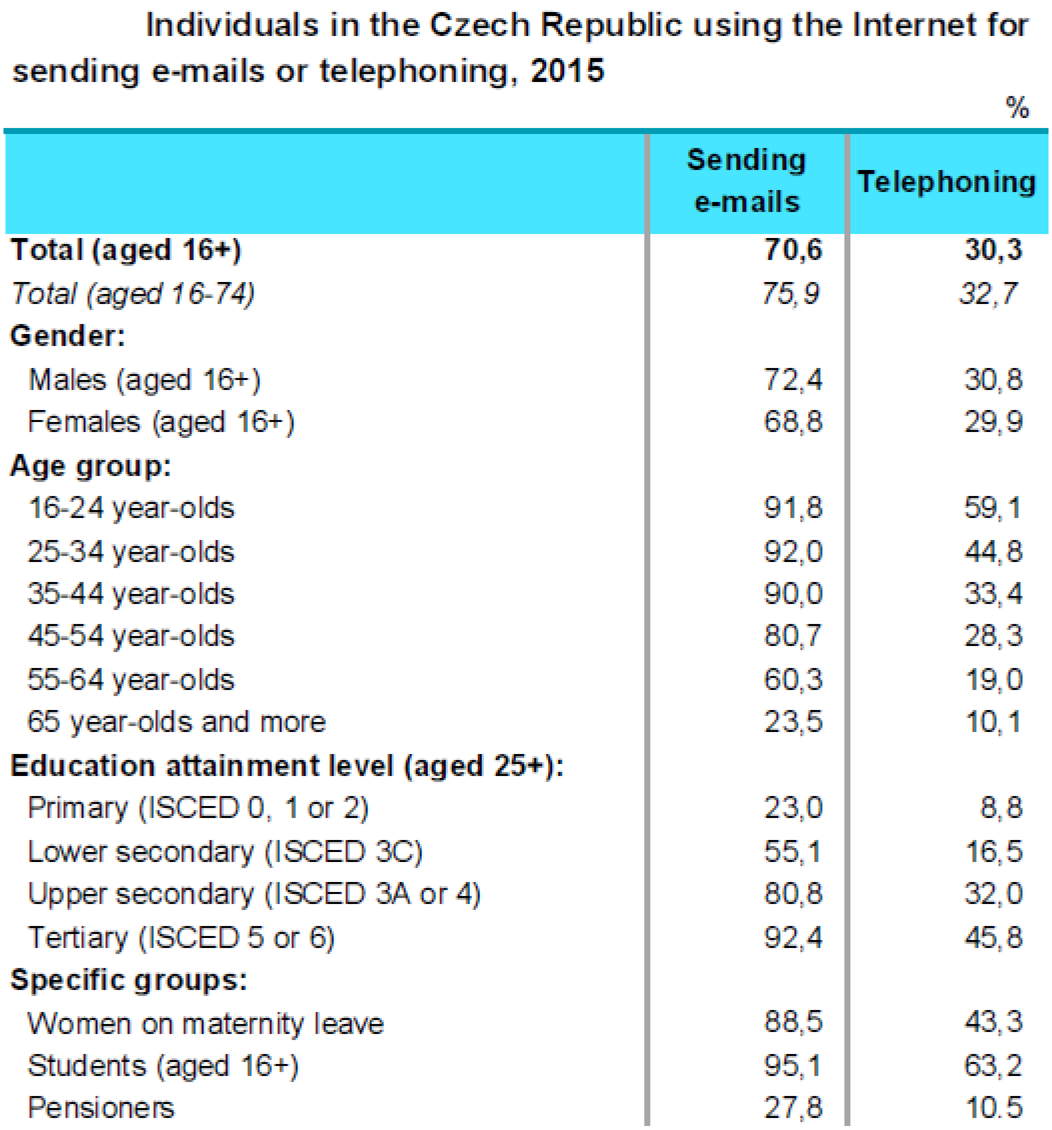
Finally, 90.5 % of students above 16 years uses the internet for watching online videos. 46.1% of students use the internet for watching TV online as 62.6 % of students in general above 16 years also uses the internet for online gaming purposes.



Source: Czech statistical Service Department

The above graph shows the percentage growth of individuals over 16 years using the internet for watching online images, movies, videos or listening to music. The pattern increased from 11% in 2007 through to 40% in 2015.

Table 12



Individuals in the Czech Republic using the Internet for sending e-mails or telephoning, 2015

%

	Sending e-mails	Telephoning
Total (aged 16+)	**70,6**	**30,3**
Total (aged 16-74)	*75,9*	*32,7*
Gender:		
Males (aged 16+)	72,4	30,8
Females (aged 16+)	68,8	29,9
Age group:		
16-24 year-olds	91,8	59,1
25-34 year-olds	92,0	44,8
35-44 year-olds	90,0	33,4
45-54 year-olds	80,7	28,3
55-64 year-olds	60,3	19,0
65 year-olds and more	23,5	10,1
Education attainment level (aged 25+):		
Primary (ISCED 0, 1 or 2)	23,0	8,8
Lower secondary (ISCED 3C)	55,1	16,5
Upper secondary (ISCED 3A or 4)	80,8	32,0
Tertiary (ISCED 5 or 6)	92,4	45,8
Specific groups:		
Women on maternity leave	88,5	43,3
Students (aged 16+)	95,1	63,2
Pensioners	27,8	10.5

Source: Czech statistical Service Department

This table depicts people from 16+ or in other words 16 years and over. Out of a total of 75.9%, 70.6% uses the internet for sending e-mails. 30.3 % out of 32.7% also uses the internet for telephoning.

Furthermore, 72.4 % representing males above 16 years uses the internet for sending e-mails. 30.8 % use the internet also for telephoning whereas with their female counterparts, 68.8% representing females above 16 years also uses the internet for sending e-mails and 29.9 % uses the internet for telephoning.

16-24 years = 91.8% of them uses the internet for sending e-mails and 59.1 % uses the internet for telephoning.

25-34 years = 92 % of them uses the internet for sending e-mails and 44.8 % uses the internet for telephoning.

35-44 years = 90% of them uses the internet for sending e-mails and 33.4 % uses the internet for telephoning.

45-54 years = 80.7% of them uses the internet for sending e-mails and 28.3 % uses the internet for telephoning.

55-64 years = 60.3% of them uses the internet for sending e-mails and 19 % uses the internet for telephoning.

65+ years = 23.5 % of them uses the internet for sending e-mails and 10.1 % uses the internet for telephoning.

Educational Attainment:

Primary level

23 % of the people with primary educational attainment uses the internet for sending e-mails and 8.8 % uses the internet for telephoning.

Lower secondary

55.1 % of the people with lower educational level also sends e-mails via the internet as 16.5% uses the internet for telephoning.

Upper secondary

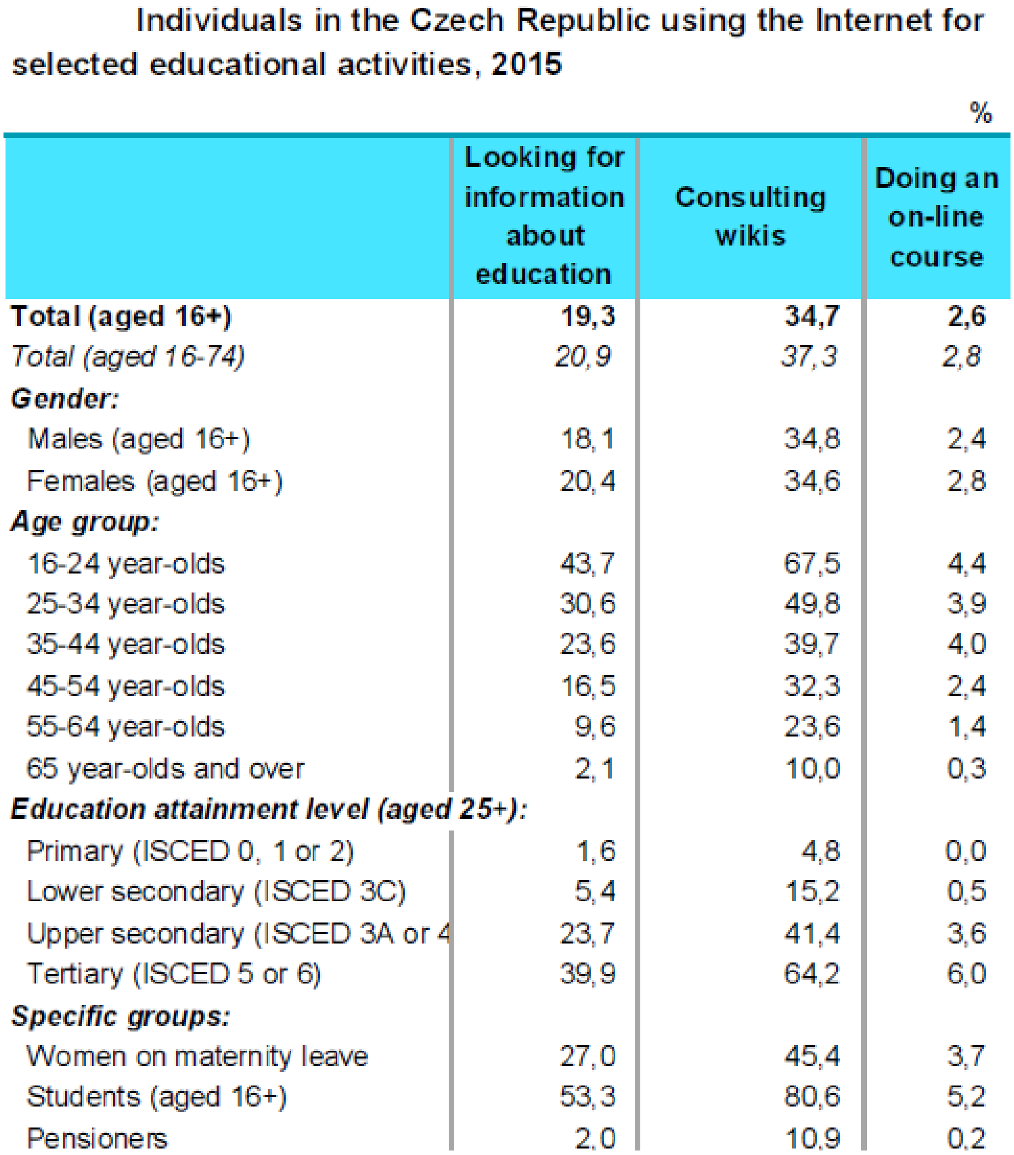
80.8 % of the people with primary educational attainment uses the internet for sending e-mails and 32 % uses the internet for telephoning.

Tertiary educational level

92.4 % of the people with primary educational attainment uses the internet for sending e-mails and 45.8 % uses the internet for telephoning.

Finally, 95.1 % of students in general above 16 years uses the internet for sending information via e-mails and 63.2 % uses the internet for telephoning.

Table 13



Individuals in the Czech Republic using the Internet for selected educational activities, 2015

%

	Looking for information about education	Consulting wikis	Doing an on-line course
Total (aged 16+)	**19,3**	**34,7**	**2,6**
Total (aged 16-74)	*20,9*	*37,3*	*2,8*
Gender:			
Males (aged 16+)	18,1	34,8	2,4
Females (aged 16+)	20,4	34,6	2,8
Age group:			
16-24 year-olds	43,7	67,5	4,4
25-34 year-olds	30,6	49,8	3,9
35-44 year-olds	23,6	39,7	4,0
45-54 year-olds	16,5	32,3	2,4
55-64 year-olds	9,6	23,6	1,4
65 year-olds and over	2,1	10,0	0,3
Education attainment level (aged 25+):			
Primary (ISCED 0, 1 or 2)	1,6	4,8	0,0
Lower secondary (ISCED 3C)	5,4	15,2	0,5
Upper secondary (ISCED 3A or 4	23,7	41,4	3,6
Tertiary (ISCED 5 or 6)	39,9	64,2	6,0
Specific groups:			
Women on maternity leave	27,0	45,4	3,7
Students (aged 16+)	53,3	80,6	5,2
Pensioners	2,0	10,9	0,2

Source: Czech statistical Service Department

This table shows people from 16 years and over. Out of a total of 20.9%, 19.3% uses the internet for searching information about educational stuffs. 34.7 % out of 37.3% also uses the internet for consulting wikis and in addition to this point, 2.6 % out of 2.8 % also uses the internet for undertaking online courses.

Furthermore, 81.1% representing males above 16 years uses the internet for searching information about educational stuffs, 34.8 % use the internet also for consulting wikis as 2.4% uses the internet for undertaking online courses. In comparison to their female counterparts, 20.4% representing females above 16 years uses the internet for searching for information about educational, 34.6%

use the internet also for consulting wikis as 2.8. % also uses the internet for undertaking online courses.

16-24 years = 43.7% of them uses the internet for searching information about educational stuffs, 67.5% uses the internet for consulting wikis as 4.4% of this age category also uses the internet for undertaking online courses.

25-34 years = 30.6% of them uses the internet for searching information about educational stuffs, 49.8% uses the internet for consulting wikis as 3.9 % of this age category also uses the internet for undertaking online courses

35-44 years = 23.6 % of them uses the internet for searching information about educational stuffs, 39.7 % uses the internet for consulting wikis as 4 % of this age category also uses the internet for undertaking online courses

45-54 years = 16.5 % of them uses the internet for searching information about educational stuffs, 32.3 % uses the internet for consulting wikis as 2.4 % of this age category also uses the internet for undertaking online courses

55-64 years = 9.6 % of them uses the internet for searching information about educational stuffs, 23.6% uses the internet for consulting wikis as 1.4% of this age category also uses the internet for undertaking online courses

65+ years = 2.1 % of them uses the internet for searching information about educational stuffs, 10 % uses the internet for consulting wikis as 0.3% of this age category also uses the internet for undertaking online courses

Educational Attainment:

Primary level

1.6 % of the people with primary educational attainment uses the internet for searching information about educational stuffs, 4.8 % of persons with this same level of education also uses the internet for consulting Wikis as 0% uses the internet for undertaking online courses.

Lower secondary

5.4 % of the people with lower secondary educational attainment uses the internet for searching information about educational stuffs, 15.2 % of persons with this same level of education also uses the internet for consulting Wikis as 0.5 % uses the internet for undertaking online courses

Upper secondary

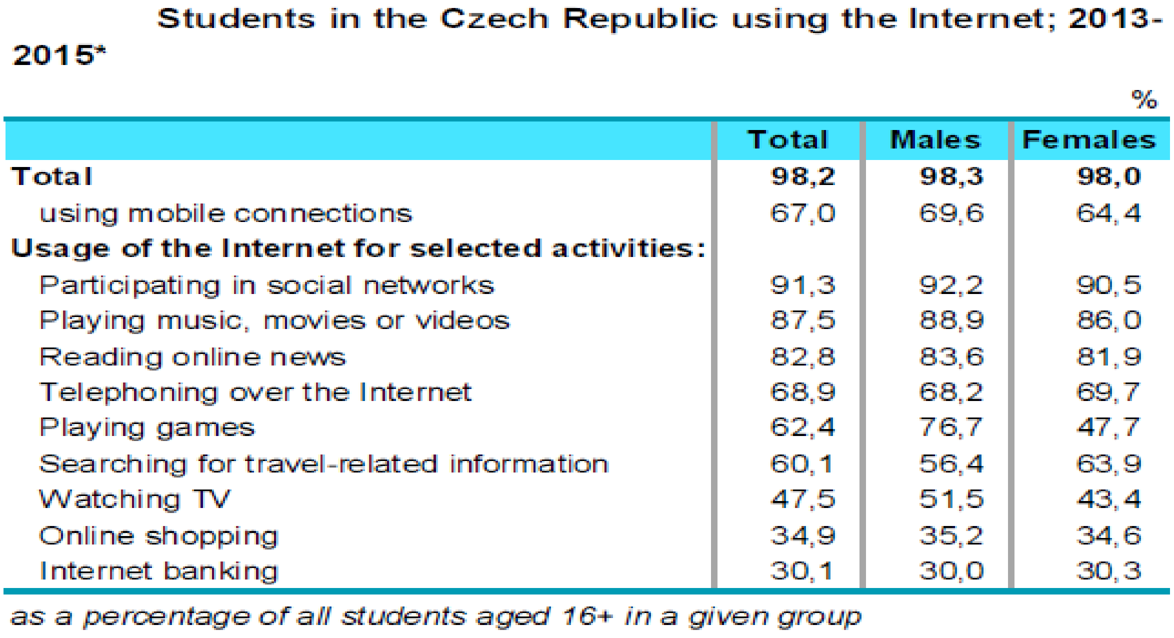
23.7 % of the people with upper secondary educational attainment uses the internet for searching information about educational stuffs, 41.4 % of persons with this same level of education also uses the internet for consulting Wikis as 3.6 % uses the internet for undertaking online courses

Tertiary educational level

39.9 % of the people with primary educational attainment uses the internet for searching information about educational stuffs, 64.2 % of persons with this same level of education also uses the internet for consulting Wikis as 6% uses the internet for undertaking online courses

Finally, 53.3 % of students above 16 years uses the internet for searching information about educational stuffs. 80.6% of students use the internet for consulting Wikis as 5.2 % of students in general above 16 years also uses the internet for undertaking online courses.

Table 14



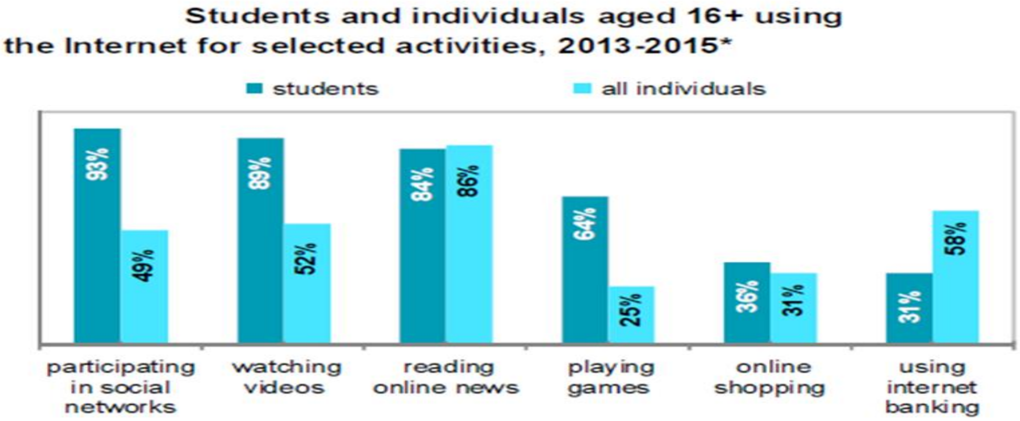
Students in the Czech Republic using the Internet; 2013-2015*

%

	Total	Males	Females
Total	**98,2**	**98,3**	**98,0**
using mobile connections	67,0	69,6	64,4
Usage of the Internet for selected activities:			
Participating in social networks	91,3	92,2	90,5
Playing music, movies or videos	87,5	88,9	86,0
Reading online news	82,8	83,6	81,9
Telephoning over the Internet	68,9	68,2	69,7
Playing games	62,4	76,7	47,7
Searching for travel-related information	60,1	56,4	63,9
Watching TV	47,5	51,5	43,4
Online shopping	34,9	35,2	34,6
Internet banking	30,1	30,0	30,3

as a percentage of all students aged 16+ in a given group

Source: Czech statistical Service Department



Source: Czech statistical Service Department

From the table above, 92.2 % of male students uses the internet for participation in various networks whereas 90.5 % representing that of the females. 88.9% of males as compared to 86% of female's students also uses the internet for playing music, movies. Other activities which includes reading online news, telephoning over the internet, playing online games etc. are indicated in the table with their respective number of percentage distribution

A. <u>INTERNET USAGE BY STUDENTS IN GHANA IN COMPARISON WITH THAT OF THE CZECH REPUBLIC</u>

28.2 % of people who have attained primary education in the Czech Republic uses the internet at home whereas 23.8 % uses internet regularly. 60.3 % with lower secondary educational attainment uses the internet at home as 56.3 % uses the internet regularly. 82.4% of people with upper secondary also uses the internet at home and 80.9 % uses the internet regularly. Last but not the least, 92.9 % of people with tertiary level of educational attainment uses the internet at home as 93.2 % uses the internet regularly. Finally, 96.5% of students above 16 years in general in the Czech Republic uses the internet at home while 98% of them uses the internet regularly.

With respect to internet usage by secondary school students in Ghana, 15% uses the internet very frequently, 20% uses the internet frequently as 25% uses the internet on occasional basis. Also, 25% uses the internet rarely and 15% uses the internet very rarely.

In the light of the above analysis, we could clearly see the percentage of internet usage by students in the Czech Republic outweigh that of that Ghana right from the primary level through to the secondary and tertiary level.

B. STUDENTS USE OF INTERNET FOR EDUCATION PURPOSES

From our study, most students in Ghana uses the internet for educational purposes such as practising online workbook, visiting on-line libraries, accessing information on the internet, exchanging information and Join-discussion groups online whereas students in the Czech Republic also uses internet for educational activities such looking for information about education, consulting Wikis and doing on-line course.

C. OTHER PURPOSE OF INTERNET USAGES

12.5% of students in Ghana never use the internet for entertainment purpose, 24.4 % uses the internet rarely for entertainment, 51.5% also occasionally uses the internet for entertainment, 9% frequently use internet for such a purpose, and finally, 3.1 % of students in Ghana always uses the internet for entertainment. With the Czech students between 2013-2015, (92.2%) of males uses the internet participating in social networks as 90.5 % goes to that of the females. 88.9 % of males and 86% of females also uses the internet for playing music, movies or videos. Finally, 76.7% of males use the internet in playing online games and 47.7 % of females also do likewise.

We can then conclude from the above analysis that, Czech students uses the internet for numerous entrainment purposes than that Ghanaian students

INTERNET BANKING

26.25% of students in Ghana never use the internet for online banking, 23.75 % uses the internet rarely for internet banking, 34.345% also occasionally uses the internet for internet banking, 13.125% frequently use internet for such a purpose, and finally, 2.5 % of students in Ghana always uses the internet for online banking. In the case of Czech students, 61.4% of students uses the internet for online banking which outweigh that of Ghana student usage of internet for online or internet banking.

TRAVEL RELATED RESEARCH OR RESERVATIONS

38.18% of students in Ghana never use the internet for travel-related (research, reservation purposes), 28.75 % uses the internet rarely for (research, reservation purposes), 19.37 % also occasionally uses the internet for (research, reservation purposes), 8.7 % frequently use internet for such a purpose, and finally, 5 % of students in Ghana always uses the internet for (research, reservation purposes). With the Czech students between 2013-2015, (56.4%) of males uses the internet for searching travel-related information as 63.9 % goes to that of the females.

We can then conclude from the above analysis that; Czech students uses the internet much more for travel -related issues than Ghanaian students

COMMUNICATION WITH OTHERS (CHATS/ E-MAILS)

4.38% of students in Ghana never use the internet for communicating with others (chats / e-mails), 7.5 % uses the internet rarely for (chats / e-mails), 30 % also occasionally uses the internet for (chats / e-mails), 25 % frequently use internet for such a purpose, and finally, 33.12% of students in Ghana always uses the internet for communicating with others (chats / e-mails). This with respect to Czech students, 95.1% of overall students 16 years and over uses the internet for sending e-mails and 63.2 % even have the opportunity of using the internet for online telephoning.

Chapter Five

Conclusion and Recommendations

The purpose of this study is to understand the nature of cyberspace, what really entails cyberspace as well the advantages and disadvantages of cyberspace. Also, in this research includes some terminologies such as cybercrime, cyber security, cyber bullying and information society. These terminologies have been well explained to enable us to really understand their impact to people and the environment or society we find ourselves in as well as some possible preventions.

In addition to the study objective of this research is to compare the usage of internet in the Czech Republic and that of Ghana by students for learning purposes, usage of social media and their influence of learning on the part of students.

From the study, it can conclude that, the usage of internet in the Czech Republic far outweigh the usage of internet in Ghana and that of the usage of social media by students as well.

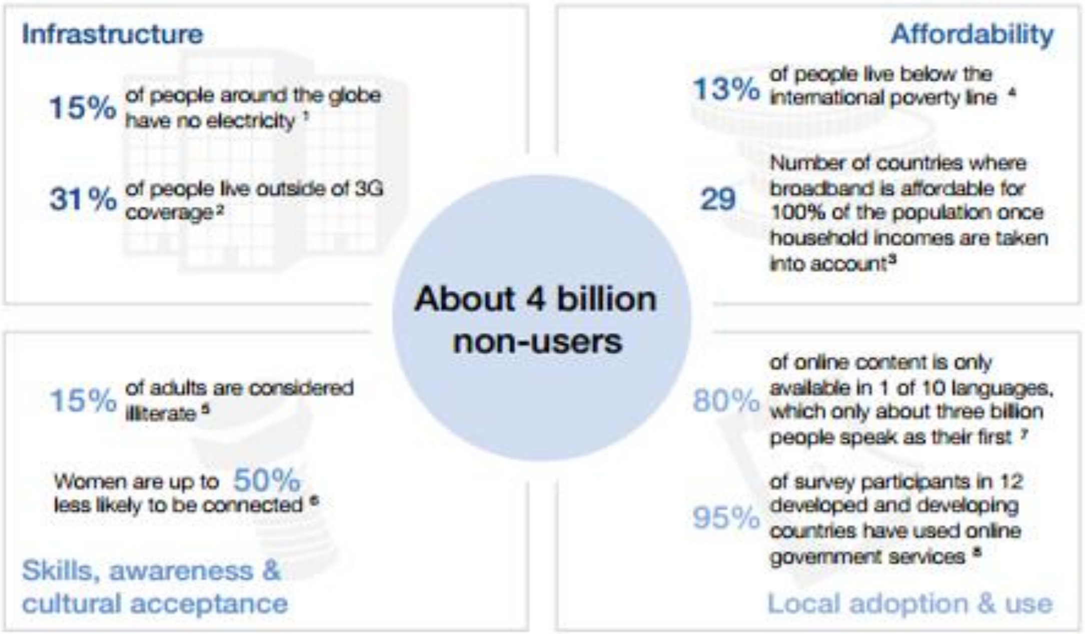
Internet access is the process that enables individuals and organisations to connect to the internet using computer terminals, computers, mobile devices, sometimes via computer networks. Once connected to the internet, users can access internet services, such as email and the World Wide Web. Internet service providers (ISPs) offer internet access through various technologies that offer a wide range of data signaling rates (speeds).

More than 4 billion people, mostly in developing countries, still don’t have access to the internet. This means that over half of the world’s population is missing out on the life-changing benefits of connectivity, from financial services to health and education, being brought about by the increasing pace of innovation known as the Fourth Industrial Revolution,

Universal, affordable internet access is part of the UN’s Sustainable Development Goals (SDGs), and governments, companies, local and international organizations, and members of civil society are working to get more people online. However, as a new report from the World Economic Forum explains, the problem is “big, complex and multidimensional

REASONS WHY DEVELOPING COUNTRIES AND LOTS OF PEOPLE ARE STILL OFFLINE

There are four main reasons that so many people are still offline more especially in Afica and developing countries according to Forum’s Internet for All report.


Infrastructure
15% of people around the globe have no electricity [1]
31 % of people live outside of 3G coverage [2]
Affordability
13% of people live below the international poverty line [4]
29 Number of countries where broadband is affordable for 100% of the population once household incomes are taken into account [3]
About 4 billion non-users
15% of adults are considered illiterate [5]
Women are up to 50% less likely to be connected [6]
Skills, awareness & cultural acceptance
80% of online content is only available in 1 of 10 languages, which only about three billion people speak as their first [7]
95% of survey participants in 12 developed and developing countries have used online government services [8]
Local adoption & use

Most recently available figures used: 1. World Bank, 2012; 2. ITU, 2015 estimate; 3. Broadband Commission for Digital Development, ITU, UNESCO, *The State of Broadband 2015*, 2015; 4. World Bank, 2015 (2012 data); 5. UNESCO, *Adult and Youth Literacy*, 2015; 6. Controlling for education level and household income, World Wide Web Foundation, 2015; 7. World Bank, 2014; 8. BCG, 2014a

Source: Broadband Commission for Digital Development,ITU

Infrastructure: One reason many people aren't logging on is simply that a good, fast connection is not available – 31% of the global population do not have 3G coverage, while 15% have no electricity. In sub-Saharan Africa some 600 million people (almost two thirds of the region's population) do not have regular electricity, and this applies to nearly a quarter of people living in South Asia.

Affordability: The cost of devices and connectivity is another factor preventing many people from accessing the internet, especially the 13% of the world population living below the poverty line. Broadband is only affordable for 100% of the population in just 29 countries.

Skills, awareness and cultural acceptance: A key barrier for some is education – 15% of adults globally are considered illiterate. There are also cultural issues, with women up to 50% less likely to be using the internet than men.

Local adoption and use: The vast majority (80%) of online content is only available in 10 languages, which only about 3 billion people speak as their first language.

Children or the youth get involved in a wide variety of activities on the internet, and many overlap each other, as Web 2.0 platforms increasingly are becoming a part of today’s youth culture. A 25 country survey conducted by European Union Kids Online and funded by the European Commission’s Safer Internet Programme suggests that top activities for children and youth using the internet are: schoolwork (92%), playing games (83%), watching video clips (75%) and social networking (71%). 59% of European children who use the internet have their own social network profile. Only 28% of 9-10 year olds, but 59% of 11-12 year olds, have a social network profile, suggesting that it is the start of secondary school rather than the minimum age set by popular providers, that is a major trigger for social networking. [95] To this end, identifying and establishing norms that can inform online interactions should become an integral part of a child's education and must begin in the primary grades through to the secondary levels.

Another transition that Africa is not implementing fast enough is that to the new internet addressing protocol, IPv6. IPv6 is necessary for long term internet expansion, especially as the Internet of Things (IoT) becomes a reality. To date, South Africa and Egypt registered 97% of the African IPv6 addresses, which means adoption in all the other countries is lagging.

Most national ICT policies and strategies mention capacity building as a priority; however, most countries fall short on implementation. This translates into significant capacity gaps – especially at the level of specialists able to build and maintain infrastructure and services – making Africa overly reliant on external expertise. Africa needs a coherent strategy for capacity development at all levels, and this strategy needs to look first at ICTs as a discipline and secondly as a cross-cutting enabler of other disciplines.

International internet connectivity is one of the most critical requirements for the development of the internet in any country, particularly for developing countries that access significant amounts of content from more developed regions. Users in countries with more international bandwidth and national coverage are better able to access and enjoy a wide range of online services, while those in countries that lack adequate international bandwidth are significantly restrained in their internet access and usage.

But not only does insufficient bandwidth choke internet access, it also keeps prices high and the quality of services low. Even where access is available, relatively high prices for international connectivity can be very discouraging, often leading to a lack of user interest in internet services. Where this is the case, Internet traffic volumes and related revenues dwindle, reducing the attractiveness of investment in international bandwidth. As such, problems of access, affordability, and quality of service in the country may persist. Bandwidth, which is critical to the access and use of the internet, is scarce and thus expensive in developing countries in general and in Africa in particular. Users in Africa have to pay many times more for internet access than their peers in developed countries.

IMPORTANCE ON THE USE OF INTERNET

There are many benefits associated with internet use, such as access to needed information, worldwide access to news and events, and interpersonal communication through email. The internet is a massive, computer-linked network system used globally to access and convey information, either by personal or business computer users; it is also used for communication, research, entertainment, education and business transactions Kraut, et al., 1998; Schneider, et al.,

2006. Today, the internet can link all online computers so that people can use it to communicate throughout the world Schneider, et al., 2006. The word internet emanates from the words "Internet Connection Network" Greenfield, 1999, connecting computers around the world by the use of a standard protocol. In addition, Chou 2001 indicated that the most appreciated internet features included interactivity, simplicity, availability, and abundant and updated information. In fact, the internet's attractiveness has increased as a result of its availability, accessibility, and affordability. The development of friendlier interfaces provides users with easier and more comfortable access

The internet is an increasing part of today's culture, especially for children and youth, for whom schoolwork, online gaming, and social networking are among the most popular activities

SOME PROBLEMS ENCOUNTERED USING THE INTERNET

From our study, in spite of the many advantages of the internet yet, it has got some disadvantages of which some of them could be recognized as;

- Exposure to inappropriate images or content, whether inadvertently or deliberately.
- Solicitation by sexual predators in chat rooms, other forms of social media, and by email.
- Online bullying or harassment.
- Inappropriate disclosure of personal information and data theft (through over-sharing or other means).
- Spyware, viruses and malicious software.
- Scams
- Excessive commercialism: advertising and product-related websites.
- The consequences of the temptation to engage in piracy of software, music or video.

HOW TO PROMOTE AND STRENGTHEN CYBERSECURITY

Youth is the fastest growing age group using the internet; yet where they lack awareness and have limited ability to assess risk and make decisions, they are vulnerable. Multi-stakeholder cooperation at the local, national and international level is an effective way to create awareness of the importance of child protection issues in some regions of the world, Furthermore, policing offences requires multi-agency co-operation at the local and national level, while on an international level, cooperation and information-sharing is vital in dealing with child protection.

HOW TO CONTROL, PREVENT OR MINIMIZE CYBERBULLUYING

An important role in enabling children's safety on the internet is to help them to understand the concepts of risk and safety online, which will allow children make independent informed decisions. Internet safety education is critical in protecting young people against online threats; both external threats, such as 'inappropriate' content and activities (e.g. gambling) or contact with the 'wrong' people (e.g. bullying, stalking, scams), and internal threats, such as disclosure of too much personal information. By working together with children, and listening to their needs and learning from their experience, we can shape an environment for children, enabling them to make the most of the opportunities that the Internet offers, while behaving in a safe and responsible way. At the same time, such an environment can help those children who take advantage of the internet to commit 'bad acts' to understand the true impact of their actions on more vulnerable subjects.

However, it is important to bear in mind that the internet is not an 'evil' tool, exposing children to unprecedented dangers. This idea is in line with the resilience-based school of thought, which illustrates how "preserving adaptive capacity – the ability to adapt to changed circumstances while fulfilling once core purpose is an essential skill in an age of unforeseeable disruption and volatility". [96] Based on this theory, when it comes to child safety online, legislating and regulating might, at the end, be counterproductive. It is impossible (and potentially futile) to seek to ban every single activity that potentially exposes children to dangers in the internet; a much healthier, resilient-based approach sees education and empowerment as the tools that will enable parents, educators or the state to address such issues relating to the safety of children in the Internet. We should strive towards engaging children with the internet at a gradual pace and use resiliency strategies to teach them how to cope with the online environment and its dangers. To this end, teaching children about the importance of 'netiquettes' and instilling to them the notion of "think before you click" should be our primary goal.

RECOMMENDATIONS

First and foremost, it is recommended countries around the world should have to develop national approaches to internet regulation, with varying degrees of success and sometimes with unintended consequences. This could be achieved if the rapidly rising number of countries that have chosen the approach of simply limiting access to internet content in recent years. Also, countries should endeavour or try to impose internet filtering, a technical approach to controlling access to content. Generally, three techniques are commonly used to block access to websites: IP blocking, DNS filtering, and URL blocking using a proxy. Keyword blocking, which blocks access to websites based on the words found in requested URLs, or blocks searches based on a list of blacklisted terms, is a more advanced technique that a growing number of countries are employing. These methods can be implemented at different locations; for example, at the ISP, by an institution or at the specific internet-connected device.

Parents, guardians, educators, or other authorities should also make an effort to have access to programs and tools which are able to monitor, track and block access to specific online activities on devices used by children; for example:

- Proxies and software that can allow or block specific sites and protocols (including anti-virus protection, email spam filters, pop-up blockers, anti-spyware, cookie deletion software, etc.)

- Content filtering software that finds and blocks specific content or websites

- Configuration options to set site privacy and monitoring features (e.g., Google Safe Search filter, Privolock)

In 2011, the OECD released a report titled *The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them*, and in 2012, the OECD adopted a Council Recommendation on the Protection of Children Online establishing three key principles: empowerment, proportionality and fundamental values as well flexibility.

Further, the Recommendation [97] calls on governments to demonstrate leadership and commitment through their policies. Additionally, to support a co-ordinated response by all stakeholders; foster consistency and coherence of domestic child online protection initiatives across public and private stakeholders. The recommendation further entreated member states to foster awareness-raising and education as essential tools for empowering parents and children. To support evidence-based policies for the protection of children online, encourage the development and adoption of technologies for the protection of children online that respect the rights of children and the freedom of other internet users. Lastly, the recommendation aimed at strengthening international networks of national organisations dedicated to the protection of children online as well share information about national policy approaches to protect children online and in particular develop the empirical foundations for quantitative and qualitative international comparative policy analysis. Finally, parents, guardians, educators and trusted influencers should take an active role in teaching children and young people about the risks they may face from sexually explicit materials online and from Internet predators and scammers and how to avoid them. Equally important, children should also be educated about how to communicate privately with known friends, and to be careful about sharing personal information on the Internet. Of course, to teach effectively it is important for parents, guardians, educators and peers to be computer literate.

REFERENCES

[1] S. Schjolberg and S. Ghernaouti-Helie, A Global Treaty on Cybersecurity and Cybercrime, 2nd ed. AiTOslo, 2011

[2] Gao Z, Ansari N. Tracing cyber-attacks from the practical perspective[J]. Communications Magazine, IEEE,2005, 43(5): 123-131

[3] Nirkhi SM, Dharaskar R V, Thakre V M. Analysis of online messages for identity tracing in cybercrime investigation[C] // Cyber Security, Cyber Warfare and Digital Forensic (CyberSec),2012 International Conference on. IEEE,2012: 300-305

[4] Zheng R, Qin Y, Huang Z, et al. Authorship analysis in cybercrime investigation [M] // Intelligence and Security Informatics. Springer Berlin Heidelberg, 2003: 59-73.

[5] Banday M T, Mir F A. A study of Indian approach towards cyber security[C] // Emerging Technology Trends in Electronics, Communication and Networking (ET2ECN), 2012 1 st International Conference on. IEEE, 2012:1-6.

[6] Li Hao , Philosophical thinking about the network space China Communication Industry Association, 2011-01-26.

[7] Scott Thil. March 17, 1948: William Gibson, Father of Cyberspace "http:// www. Wired.com /science/discoveries /news/2009/03/dayintech_0317

[8] M. Uma and G. Padmavathi, A Survey on Various Cyber Attacks and their Classification. International Journal of Network Security, Vol.15, No.6, PP.391-397,Nov.2013.

[9] Ghernaouti-Helie, S.; "Going Digital -- Rethinking Cybersecurity and Confidence in a Connected World: A Challenge for Society," Emerging Security Technologies (EST), 2012 Third International Conference on, vol., no., pp.8-11, 5-7 Sept. 2012

[10] Nurse, J.R.C.; Creese, S.; Goldsmith, M.; Lamberts, K.; "Guidelines for usable cybersecurity: Past and present," Cyberspace Safety and Security (CSS), 2011 Third International Workshop on, vol., no., pp.21-26, 8-8 Sept. 2011

[11] Kriz, D., "Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity," Cybersecurity Summit (WCS), 2011 Second Worldwide, vol., no., pp.1-3, 1-2 June 2011

[12] Sami Saydjari, O., "Defending cyberspace," Computer, vol.35, no.12, pp. 125- 127, Dec 2002

[13] Gibson, W., "Necromancer", New York: Ace, 1984

[14] Gandhi, R.; Sharma, A.; Mahoney, W.; Sousan, W.; Qiuming Zhu; Laplante, P., "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," Technology and Society Magazine, IEEE, vol.30, no.1, pp.28-38, Spring 2011.

[15] Wielki, J., "A Framework of the Impact of Cyberspace on Contemporary Organizations," Database and Expert Systems Applications, 2006. DEXA '06. 17th International Workshop on, vol., no., pp.314-318.

[16] W. House, “Cyberspace policy review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” Comprehensive National Cybersecurity Initiative, 2009.

[17] Force U S A, “Cyberspace Operations,” Air Force Doctrine Document, pp. 3-12, 2010.

[18] RICHARD A CLARKE, ROBERT KNAKE. Cyber war: The next threat to national security and what to do about it[M]. New York: Harper Collins publisher,2010.

[19] M. Goliński, Społeczeństwo informacyjne. Geneza koncepcji iproblematyka pomiaru. Warszawa: Oficyna Wydawnicza Szkoły Głównej Handlowej, 2011.

[20] R. Żelazny, “Wybrane mierniki rozwoju społeczeństwa informacyjnego i gospodarki opartej na wiedzy. Problemy pomiaru na poziomie regionalnym,” in Kierunki rozwoju społeczeństwa informacyjnego i gospodarki opartej na wiedzy w świetle śląskich uwarunkowań regionalnych, C. M. Olszak, and E. Ziemba, Eds. Katowice: Wydawnictwo Uniwersytetu Ekonomicznego, pp. 48-57, 2010.

[21] Raport monitoringowy Strategii Rozwoju Społeczeństwa Informacyjnego Województwa Śląskiego do roku 2015. Katowice: Śląskie Centrum Społeczeństwa Informacyjnego, 2013, retreive from: http://www.e-slask.pl/files/zalaczniki/2013/04/09/127 6770448/1365509299.pdf, 2013.

[22] D. Bell, The coming of post-industrial society: A venture in social forecasting. New York: Basic Books, 1973.

[23] A. Toffler, The third wave. New York: Bantam Books, 1980

[24] L. Z. Karvalics, Information society – what is it exactly? Budapest: Network for Teaching Information Society, 2007.

[25] R. Mansel, The information society. Critical concepts in sociology. London: Routledge, 2009.

[26] C. M. Olszak, and E. Ziemba, Eds. Kierunki rozwoju społeczeństwa informacyjnego i gospodarki opartej na wiedzy w świetle śląskich uwarunkowań regionalnych. Katowice: Akademia Ekonomiczna, 2010.

[27] D. R. Raban, A. Gordon, and D. Geifman, “The information society. The development of a scientific specialty,” Information, Communication & Society, vol. 14, issue 3, pp. 375–399, 2011

[28] E. Ziemba, “The holistic and systems approach to the sustainable information society,” Journal of Computer Information Systems, to be published

[29] Zahri yunos “The reality of cyber threats today” STAR In-Tech, Malysia September 2008.

[30] Neufeld, D J. (2010). Understanding cybercrime. Proceedings of the 43rd Hawaii International Conference on System Sciences. IEEE Computer Society Press. OECD (2005) Guide to measuring the information society / Working Party on indicators for the Information Society (DSTI/ICCP/IIS(2005)6/FINAL). Paris: Organization for Economic Co- operation and Development

[30] Neufeld, D.J.; "Understanding Cybercrime," System Sciences (HICSS), 2010 43rd Hawaii International Conference on, vol., no., pp.1-10, 5-8 Jan.2010

[31] Holt, T. J. (2013a) ’Exploring the social organization and structure of stolen data markets’, Global Crime, 14, pp 155-174.

[32] Holt, T. J. (2013b) 'Examining the forces shaping cybercrime markets online', Social Science Computer Review, 31, pp 165-177.

[33] Holt, T. J. and Kilger, M. (2012) 'Examining Willingness to Attack Critical Infrastructure Online and Offline', Crime & Delinquency, 58 (5), pp 798–822.

[34] M. Wamier, F. Dechesne, and F. Brazier,” Design for Privacy” ed: Delft University of Technology, to appear.

[35] M. Thangiah, S. Basri, S. Sulaiman, "A framework to detect cybercrime in the virtual environment". Computer & Information Science (ICClS), 2012 International Conference on, 2012.

[36] Carin, L.; Cybenko, G.; Hughes, J., "Cybersecurity Strategies: The Queries Methodology," Computer, vol.41, no.8, pp.20-26, Aug. 2008

[37] W. Chung, H. Chen, W. Chang, and S. Chou, "Fighting cybercrime: a review and the Taiwan experience," Decision Support Systems, vol. 41, pp. 669-682, 2006

[38] R. Broadhurst and L. Y. Chang, "Cybercrime in Asia: Trends and Challenges," in Handbook of Asian Criminology, ed: Springer, 2013, pp. 49-63.

[39] R. G. Smith, N. Wolanin, and G. Worthington, E-crime solutions and crime displacement: Australian Institute of Criminology; 2003

[40] Aamir, Muhammad, and Mustafa Ali Zaidi. "DDoS Attack and Defense: Review of Some Traditional and Current Techniques." In: CoRRabs/1401.6317 (2014).

[41] Alomari, Esraa, Selvakumar Manickam, B. B. Gupta, Shankar Karuppayah, and Rafeef Alfaris. "Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. "International Journal of Computer Applications, vol. 49, no.7, July 2012.

[42] Meena, Darshan Lal, and R. S. Jadon. "Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches." International Journal, vol. 2, no. 4, Apr. 2014.

[43] DDoS Quick Guide, White Paper, January 2014.https://www.uscert. gov/security-publications/DDoS-Quick-Guide

[44] Kirwan, G. and Power, A. (2012) The Psychology of Cyber Crime. Hershey: IGI Global

[45] Furnell, S. (2010) 'Hackers, Viruses and Malicious Software'. In Handbook of Internet Crime, Jewkes, Y. and Yar, M., pp 173–193. Culhompton: Willan Publishing.

[46] Lusthaus, J. (2013) 'How organised is organised cybercrime?' Global Crime, 14 (1) pp52-60.

[47] McCusker, R. (2006) 'Transnational organised cyber-crime: distinguishing threat from reality', Crime, Law and Social Change, 46 (4-5), pp 257–273.

[48] Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press.

[49] Canongia, C., & Mandarino, R. 2014. Cybersecurity: The New Challenge of the Information Society. In Crisis Management: Concepts, Methodologies, Tools and Applications: 60-80. Hershey, PA: IGI Global.

[50] Cavelty, M. D. 2010. Cyber-Security. In J. P. Burgess (Ed.), The Routledge Handbook of New Security Studies: 154-162. London: Routledge.

[51] DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014:

http://niccs.us-cert.gov/glossary#letter_c

[52] ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU).

http://www.itu.int/rec/T-REC-X.1205-200804-I/en

[53] Lewis, J. A. 2006. Cybersecurity and Critical Infrastructure Protection. Washington, DC: Center for Strategic and International Studies.

http://csis.org/publication/cybersecurity-and-critical-infrastructure-pr.

[54] Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014:

http://www.oxforddictionaries.com/definition/english/Cybersecurity

[55] Nagarajan, Ajay; Allbeck, Jan M.; Sood, Arun; Janssen, Terry L., "Exploring game design for cybersecurity training," Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on, vol., no., pp.256-262, 27-31 May 2012

[56] Hoffman, L.; Burley, D.; Toregas, C., "Holistically Building the Cybersecurity Workforce," Security & Privacy, IEEE, vol.10, no.2, pp.33-39, March-April 2012

[57] Ghernouti-Helie, S., "A National Strategy for an Effective Cybersecurity Approach and Culture," Availability, Reliability, and Security, 2010. ARES '10 International Conference on, vol., no., pp.370-373, 15-18 Feb. 2010

[58] Takahashi, T.; Kadobayashi, Y.; Nakao, K., "Toward global cybersecurity collaboration: Cybersecurity operation activity model," Kaleidoscope 2011: The Fully Networked Human? - Innovations for Future Networks and Services (K-2011), Proceedings of ITU, vol., no., pp.1-8, 12-14 Dec. 2011

[59] Puri, R.; Rutkowski, A.M., "Enhancing cybersecurity for Future Networks," Kaleidoscope: Beyond the Internet? - Innovations for Future Networks and Services, 2010 ITU-T, vol., no., pp.1-8, 13-15 Dec. 2010

[60] Gavins, W.; Hemenway, J., "Cybersecurity: A joint terminal engineering office perspective," MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010, vol., no., pp.918-923, Oct. 31 2010-Nov. 3 2010

[61] Gandhi, R.; Sharma, A.; Mahoney, W.; Sousan, W.; Qiuming Zhu; Laplante, P., "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," Technology and Society Magazine, IEEE, vol.30, no.1, pp.28-38, Spring 2011.

[62] Landwehr, Carl E., "History of US Government Investments in Cybersecurity Research: A Personal Perspective," Security and Privacy (SP), 2010 IEEE Symposium on, vol., no., pp.14-20, 16-19 May 2010

[63] Miller, H. Gilbert; Murphy, Richard H., "Secure Cyberspace: Answering the Call for Intelligent Action," IT Professional, vol.11, no.3, pp.60-63, May-June 2009

[64] Kalay, Y.E.; Marx, J., "The role of place in cyberspace," Virtual Systems and Multimedia, 2001. Proceedings. Seventh International Conference on, vol., no., pp.770-779, 2001

[65] Kephart, J.O.; Sorkin, G.B.; Swimmer, M., "An immune system for cyberspace," Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on, vol.1, no., pp.879-884 vol.1, 12-15 Oct 1997

[66] Poland, S. (2010). Cyberbullying continues to challenge educators. District Administration, 46(5), 55.

[67] Walrave, M., & Heirman, W. (2011). Cyberbullying: Predicting victimization and perpetration. Children & Society, 25(1), 59-72.

[68] Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. Computers in Human Behavior 26, 277–287.

[69] Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. Computers in Human Behavior, 26(3), 277-287. DOI: 10.1016/j.chb.2009.11.014.

[70] Wong-Lo, M., Bullock, L. M. (2011). Digital aggression: Cyber world meets school bullies. Part of a special issue: Cyberbullying By: Preventing School Failure, 55(2), 64-70. DOI: 10.1080/1045988X.2011.539429

[71] Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. Deviant Behavior, 29(2), 129-156

[72] Hinduja, S., & Patchin, J. W. (2010). Cyberbullying: A review of the legal Issues facing educators. Part of a special issue: Cyberbullying: Preventing School Failure, 55(2), 71-78.

[73] Erdur-Baker, Ö. (2010). Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools. New Media & Society, 12(1), 109-125. DOI: 10.1177/1461444809341260.

[74] Mishna, F., Khoury-Kassabri, M., Gadalla, T., & Daciuk, J. (2012). Risk factors for involvement in cyber bullying: Victims, bullies and bully–victims. Children & Youth Services Review, 34(1), 63-70. DOI: 10.1016/j.childyouth.2011.08.032. add authors to citation in paper

[75] Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. Cyber Psychology & Behavior, 11(4), 499-503. DOI: 10.1089/cpb.2007.0042.

[76] Mesch, G. S. (2009). Parental mediation, online activities, and cyberbullying. Cyber Psychology & Behavior, 12(4), 387-393

[77] Şahin, M. (2012). The relationship between the cyberbullying/cyber victimization and loneliness among adolescents. Children & Youth Services Review, 34(4), 834-837.

[78] Snakenborg, J., Van Acker, R., & Gable, R. A. Cyberbullying: Prevention and intervention to protect our children and youth. Preventing School Failure, 55(2), 88-95. DOI: 10.1080/1045988X.2011.539454.

[79] Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child Psychology & Psychiatry, 49(4), 376-385

[80] Reece, T. (2012). Cyberbullying 411. Current Health Teens, 38(5), 7-9.

[81] Humphrey, N., & Symes, W. (2010). Responses to bullying and use of social support among pupils with autism spectrum disorders (ASDs) in mainstream schools: A qualitative study. Journal of Research in Special Educational Needs, 10(2), 82-90.

[82] Hoff, D. L., & Mitchell, S. N. (2009). Cyberbullying: Causes, effects, and remedies. Journal of Educational Administration, 47(5), 652-665.

[83] Boulton, M., Lloyd, J., Down, J., & Marx, H. (2012). Predicting undergraduates' self-reported engagement in traditional and cyberbullying from attitudes. Cyber psychology, Behavior, and Social Networking, 15(3), 141-147.

[84] Juvonen, J, & Gross, E. F. (2008). Extending the school grounds? --Bullying experiences in cyberspace. Journal of School Health, 78(9), 496-505.

[85] Shariff, S. (2009a). Confronting cyber-bullying: What schools need to know, to control misconduct and avoid legal consequences. New York: Cambridge University Press.

[86] "What is Cyberbullying". http://www.stopbullying.gov/.

[87] D. Yin, Z. Xue, L. Hong, B. Davison, A. Kontostathis, L. Edwards. Detection of Harassment on Web 2.0. In CAW 2.0 '09: Proceedings of the 1st Content Analysis in Web 2.0 Workshop, Madrid, Spain 2009.

[88] K. Dinakar, R Reichart, H. Lieberman. Modeling the detection of textual cyberbullying, International Conference on Weblog and Social Media - Social Mobile Web Workshop, Barcelona, Spain 2011

[89] J. Bayzick, A. Kontostathis, L. Edwards. Detecting the Presence of Cyberbullying Using Computer Software, WebSci '11, June 14-17, 2011, Koblenz, Germany 2011.

[90] Sanchez, S. Kumar, Twitter Bullying Detection, 2011.http://users.soe.ucsc.edu

2011.http://users.soe.ucsc.edu/~shreyask/ism245-rpt.pdf 2014.07.17.

[91] M. Ptaszynski, P. Dybala, T. Matsuba, F. Masui, R. Rzepka, K. Araki, K. Machine Learning and Affect Analysis Against Cyberbullying, Proceedings of the Linguistic and Cognitive Approaches To Dialog Agents Symposium, Rafal Rzepka (Ed.), at the AISB 2010 convention, 29 March – 1 April 2010, De Montfort University, Leicester, UK.

[92] M. Dadvar, D. Trieschnigg, R. Ordelman, & F. de Jong, Improving cyberbullying detection with user context. In Advances in Information Retrieval (pp. 693-696). Springer Berlin Heidelberg, 2013.

[93] V. Nahar, S. Al-Maskari, X. Li, and C. Pang. "Semi-supervised Learning for Cyberbullying Detection in Social Networks." In Databases Theory and Applications, pp. 160-171. Springer International Publishing, 2014.

[94] A. Dempsey, M. Sulkowski, J. Dempsey, E. Storch, Has Cyber Technology Produced a New Group of Peer Aggressor, Cyber psychology, behavior, and social networking, 2011, 14(5), 297-302.

[95]http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20 reports.aspx

[96] Andrew Zolli & Ann Marie Healy (2012). "Resilience: Why Thins Bounce Back", Free Press,

[97]http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272 &Instrument PID=277&Lang=en&Book=False

[98] Meeker, M., & Wu, L. (2013). 2013 Internet Trends. KPCB. Retrieved November 21, 2013, from http://www.kpcb.com/insights/2013-internet-trends

[99] TechCrunch. (2013). Snapchat usage now bigger than Facebook and Instagram combined. battenhall. Retrieved December 31, 2013, from http://battenhall.net/blog/snapchat-usage-now-bigger-facebook-instagram-combined/

[100] Vivion, N. (2013). Social media demographics in 2012. Tnooz. Retrieved December 31, 2013,

from http://www.tnooz.com/article/social-media-demographics-in-2012-research/

[101] ITU. (2013a). Measuring the Information Society. Geneva. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2013.aspx

[102] ITU. (2013b). ICT Facts and Figures 2013. Retrieved November 21, 2013, from http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[103] ITU. (2013c). Press Release. Retrieved December 30,2013, from http://www.itu.int/net/pressoffice/press_releases/2013/37.aspx#.UsIMPPsk_Dk

[104] Quarshie, O.H., the Impact of Computer Technology on the Development of Children in Ghana. Journal of Emerging Trends in Computing and Information Sciences, May, 2012. 3(5): p. 717 - 722.

[105] Garín-Muñoz, T. and T. Pérez-Amaral, Internet Usage for Travel and Tourism. The Case of Spain, in 21st European Regional ITS Conference 2010. 2010: Copenhagen

[106] Seybert, H., Internet use in households and by individuals in 2011. Statistics in focus 2011

[107] Polat, R.K., the Internet and Political Participation: Exploring the Explanatory Links. European Journal of Communication, 2005. vol. 20 no. 4 435-459.

[108] Belsey, Bill. (2004). Cyberbullying.ca. Retrieved July 31, 2004, from Website: www.cyberbullying.ca

[109] Singer, P. W., & Friedman, A. 2013. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press.

[110] Deibert, R., & Rohozinski, R. 2010. Liberation vs. Control: The Future of Cyberspace. *Journal of Democracy*, 21(4): 43-57.http://dx.doi.org/10.1353/jod.2010.0010

[111] Choo, K.-K. R. and Smith, R. G. (2008) 'Criminal Exploitation of Online Systems by Organised Crime Groups', *Asian Criminology*, 11, pp 37–59.

[112] **Livingstone, S., Haddon, L., Gorzig, A. and Olafsson, K.** (2011) *Risks and safety on the internet: The perspective of European Children. Full Findings.* London: LSE, EU Kids Online

[112] Adams, C. (2010). Cyberbullying: How to make it stop. Instructor. 120(2), 44-49

[113] Beale, A. V., & Hall, K. R. (2007). Cyberbullying: What school administrators (and parents) can do. Clearing House, 81(1), 8-12. DOI: 10.3200/TCHS.81.1.8-12

[114] Calvete, E.,Orue, I., Estévez, A., Villardón, L., & Padilla, P.(2010). Cyberbullying in adolescents: Modalities and aggressors' profile. Computers in Human Behavior, 26(5), 1128-1135. 8p. DOI: 10.1016/j.chb.2010.03.017.

[115] deLara, E. W. (2012). Why adolescents don't disclose incidents of bullying and harassment. Journal of School Violence, 11(4), 288-305

[116] Pew Research Center. (2013). *Teens and technology*. Retrieved from http://www.pewinternet.org/~/media/Files/Reports/2013/ PIP_TeensandTechnology2013.pdf

[117]Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49, 376-385. doi:10.1111/j.1469-7610.2007.01846.x*

[118] Meeker, M., & Wu, L. (2013). 2013 Internet Trends. *KPCB*. Retrieved November 21, 2013,

from http://www.kpcb.com/insights/2013-internet-trends

[119] 17. Vivion, N. (2013). Social media demographics in 2012. *Tnooz*. Retrieved December 31, 2013,

from http://www.tnooz.com/article/social-media-demographics-in-2012-research

[120] Geers K. (January 2009) "The Cyber Threat to National Critical Infrastructures: Beyond Theory" Information Security Journal: A Global Perspective; 18 (1):1-7

[121] Goel, S. (August 2011) "Cyber warfare: Connecting the Dots in Cyber Intelligence" Communications of the ACM; Vol. 54, No. 8, 132 – 140

[122] Glenny, M. "The Cyber Arms Race Has Begun". Nation, October 31, 2011; 293 (18): 17 - 20

[123] Maurer, T. (September 2011) "Cyber Norm Emergence at the United Nations – An Analysis of Activities at the UN Regarding Cyber-Security" Explorations in Cyber International Relations Discussion Paper Series, Belfer Center for Science and International Affairs, Harvard Kennedy School

[124] Zanders, J. P. (2009) "Cyber Security: What Role for the CFSP?" Institute Report - seminar organized jointly by General Secretariat of the Council of the EU & the EU Institute for Security Studies in cooperation with Estonia held in Brussels on 4 February 2009, European Union Institute for Security Studies

[125] Eriksson, J. and Giacomello, G. (July 2006) "The Information Revolution, Security, and International Relations: (IR) Relevant Theory" International Political Science Review, Vol. 27, No. 3, 221 – 224

[126] Goodall, J. R., Lutters, W. G., & Komlodi, A. 2009. Developing Expertise for Network Intrusion Detection. Information Technology & People, 22(2): 92-108. http://dx.doi.org/10.1108/09593840910962186

[127] Williams, K. R., & Guerra, N. G. (2007). Prevalence and predictors of Internet bullying. Journal of Adolescent Health, 41(6,Suppl), S14-S21.

[128] Jones, S. E., Manstead, A. S. R., & Livingstone, A. G. (2011). Ganging up or sticking together? Group processes and children's responses to text-message bullying. British Journal of Psychology, 102(1), 71-96

[129] NCPC (2006) Cyberbullying, available at http://www.ncpc.org/cyberbullying

[130] D. Boyd, Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life, MIT Press., 2007

[131] A. Kovacevic, D. Nikolic, "Automatic detection of cyberbullying to make Internet a safer environment". Handbook of Research on Digital Crime", in Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance (pp. 1-675). editores Cruz-Cunha, M. M., & Portela, I. M., Hershey, PA: IGI Global, 2015

[132] Belsey, B. (2004). What is cyberbullying? Retrieved April 4, 2009, from: www.bullying.org/external/documents/ACF6F8.pdf

[133] Cook, C.R., Williams, KR., Guerra, N.G., & Tuthill, L. (2007, September). Cyberbullying: What it is and what we can do about it. NASP Communique, 36(1), n.p.

[134] Fryer, W.A. (2006, November 20). Addressing cyberbullying in schools. The TechEdge: The Journal of the Texas Computer Education Association. Retrieved March 15, 2009, from: www.wtvi.comlteks/06 _ 07 _articles/cyberbullying.html

[135] Moessner, C. (2007, April). Cyberbullying. Youth and Education Research: Trends & Tudes by Harris Interactive, 6(4), 1-5.

[136] Lenhart, A. (2007). Cyberbullying and online teens. Pew Internet & American Life Project. Retrieved April 2, 2009, from: www.pewinternet.org

[137] Pokin, S. (2007, November 13). Megan Meier story. The St. Charles Journal, n.p. Quiroz, H.C., Arnette, J.L., & Stephens, R.D. (2006). What is school bullying? National School Safety Center. Retrieved March 24,2009, from: www.schoolsafety.us

[138] Willard, N .E. (2006). Educators guide to cyberbullying: Addressing the harm caused by online social cruelty. Retrieved April 4, 2009, from: www.asdkI2.orglMiddleLinklAVBlbully_topics/ EducatorsGuide _ Cyberbullying.pdf

[139] Willard, N.B. (2007, March). Cyberbullying legislation and school policies: Where are the boundaries ofthe "schoolhouse gate" in the new virtual world? Center for Safe and Responsible use of the Internet. Retrieved March 15, 2009, from: http://csiru.org

[140] Endsley, M. R(1988) . Situation Awareness global assessment technique (SAGAT). Paper presented at the National Aerospace and Electronic Conference (NAECON), Dayton, OH

[145] Halder, D., & Jaishankar, K. (2011) Cybercrime and victimization of women: Laws, Rights , and Regulations. Hershey,PA, USA: IGI Global. ISBN 978-1-60960-830-9

[146] Shinder, Debra Littlejohn & Cross, Michael. 2008. Scene of the Cybercrime. Rockland: Syngress Media

[147] Svensson, P. (2011). Nasdaq hackers target service for corporate boards. Retrieved from http://news.yahoo.com/s/ap/20110205/ap_on_hi_te/us_nasdaq_hackers

[148] Balkin, J. M. et al. (2007). Cybercrime: digital cops in a networked environment. New York: New York University Press (NYU).

[149] US Department of Defence, 'Department of Defence Dictionary of Military and Associated Terms', Joint Publication 1-02(8 November 2010, as amended through 15 March 2014), 64:11:9

[150] Mcconnell International, Cybercrime...and Punishment? Archaic Laws Threaten Global Information [Dec., 2000].

[151] Jennings D. (2011) UCD Teaching and Learning. Retrieved on 3/01/2012 from http://www.ucd.ie/teaching/resources/e-learning/

[152] Cyberspace: The New World Game. 1994. In B. Cotton and R. Oliver. The Cyberspace Lexicon. London: Phaidon

[153] Wiener, Norbert, Cybernetics, or control and communication in the animal and the machine. Cambridge, Massachusetts: The Technology Press; New York: John Wiley & Sons, Inc., 1948.

APPENDIX A

QUESTIONNAIRES

A

1. How often do you use the Internet for each of the following purposes? (TICK)	Never	Rarely	Occasionally	Frequently	Always
Entertainment					
Educational					
Work-related research					
Personal finance (banking, stock trading)					
Current events (news, sports,					
Travel-related (research,					
Product information gathering					
Making purchases from online merchants.					
Communicating with others					

B

2. How many times per week, on average, do you connect to the Internet?	Once	Twice	3 times	4 times	5 or more times
From Home					
From office					
Internet café					

C

3. How many hours per week are you actively using the Internet?	0 -1 hour	2 – 3 hours	4 – 7 hours	8 – 10 hours	More than 10 hours
From Home					
From office					
Internet café					

D

3. FREQUENTLY USE OF THE INTERNET (TICK)	VERY FREQUENTLY	FREQUENTLY	OCCASSIONALLY	RARELY	VERY RARELY
STUDENTS					
TEACHERS					

E

4. STUDENT'S USE OF THE INTERNET(TICK)	**VERY OFTEN**	**OFTEN**	**SOMETIMES**	**RARELY**	**NOT AT ALL**
For Practice					
Visit on-line Libraries					
Accessing Information					
Exchanging Information					
Join Discussions					

F

5. FREQUENTLY VISITED SITES	**VERY OFTEN**	**OFTEN**	**SOMETIMES**	**RARELY**	**NOT AT ALL**
Google					
You Tube					
Facebook					
Yahoo					

G

6. PURPOSE OF INTERNET USAGE(TICK)	**NEVER**	**RARELY**	**OCCASSIONALLY**	**FREQUENTLY**	**ALWAYS**
ENTERTAINMENT					
Work-related Reseach					
Personal Finance (Banking, stock, trading)					
Current events (news, sports, and weather)					
Travel-related (research, reservations)					
Product information gathering					
Marketing purchase from online merchants					
Communicating with others(chat /emails)					