CYBERBULLYING IN GREECE:
AN INTERDISCIPLINARY APPROACH

Editors
Haralambos Tsorbatzoudis
Lambros Lazuras
Vassilis Barkoukis

Thessaloniki 2012
COPYRIGHT IN GREECE:
AN INTERDISCIPLINARY APPROACH

Editors
Haralambos Tsorbatzoudis
Lambros Lazuras
Vassilis Barkoukis

© Copyright
Haralambos Tsorbatzoudis
Lambros Lazuras
Vassilis Barkoukis

Thessaloniki 2012


Published by:
7 K. Episkopou Str
Thessaloniki
T. 2310 203 566
www.copycity.gr

Copying or redistribution of this book and its content, in whole or in part, is strictly
forbidden (Act 2121/93, article 51). The prohibition also applies to public services,
libraries, etc (art. 18). Violators will be prosecuted according to the Law (art. 13, 64-
66).
Preface

Throughout our lives, we often find ourselves subjected to psychological dominance or to dependence by the very people who are closest to us.

It is well known that adolescence is the period in our lives when social conformism and acceptance plays a most predominant role, however, sadly, it is also during this age that individuals are most susceptible to psychological violence. Organized groups of teenagers very often exert abusive behavior targeting classmates and other weak or submissive minors. Victims are most frequently psychologically seriously abused, even if physical violence is absent, and develop behavioral patterns which effectively follow them throughout the rest of their lives. Many of us have, unfortunately, faced such incidences which may occasionally lead to tragic conclusions.

Psychological violence is imposed on us, adult internet users, most commonly through imperative messages mainly related to religious misinformation trafficking. The psychological impact of such messages, even to those who refuse to submit to similar practices is, at the very least, compelling. If we, adults, whose defenses are expected to hold much stronger, find ourselves affected by such practices, minors are far more vulnerable and susceptible to kinds of psychological violence specifically tailored to harm them.

Traditional forms of physical violence are more easily recognized by parents, particularly when it comes to face-to-face confrontations. Such cases are still not easy to deal with, however, at least combined efforts both by the school and the family can be undertaken to minimize any such attempts as well as the results of abusive behavior. The reason, though, that makes cyberbullying especially threatening is that, as is also the case with other forms of familial
privacy intrusion and violation by digital technologies, we find ourselves in a particularly alien and unexplored territory which is equally puzzling to parents and youngsters and, above all, is still very difficult to predict. Being approached by individuals highly proficient in using high-tech means, a fact that in itself reveals a form of technological superiority, exerts quite an effect on those least familiar with it, e.g. parents and minors. Occasionally such an approach may have a far more dramatic effect than brute physical force. Especially for parents, who are digitally centuries behind, cyberbullying may represent a new, far more upsetting domestic threat.

Facing the actual problem carries special value, and will most likely minimize the psychological impact of cyberbullying, since, at present, it is difficult to differentiate between the actual and the suspected threat of such a practice. Initiating a discussion on this problem is necessary to evaluate the actual frequency and severity of cyber bullying. Mostly, however, a comprehensive discussion on this problem will provide the uninformed parent with the knowledge s/he needs to face the unknown intruder of her/his domestic environment. Starting a discussion on such matters is particularly important to trigger our society’s contribution to bringing to light the still unknown facets of cyberbullying.

I would like to congratulate the editors for initiating the discussion on this important topic, and I do hope that the scientific and technological advances will provide tools to overcome yet one more of the negative aspects of digital and cyber technology, which is unfortunately present alongside its still unaccountable positive aspects.

Prof. Sofia Kouidou

Vice Chancellor of Research, Aristotle University Thessaloniki
Editors’ Preface

The rapid expansion of information and communication technologies (ICTs) has pervaded all aspects of human activity, from financial transactions and education, to social networking and entertainment. In fact, it can be argued that no other technological development had such a significant impact on human life in such a short period of time as the ICTs.

On the positive side, ICT use facilitates communication and enables fairly rapid and easy access to huge amounts of information. On the negative side, however, careless and malevolent use of ICTs can lead to a range of adverse effects, including cyber addiction, online fraud, child pornography, and online aggression or cyberbullying. These effects have only recently attracted the attention social scientists (e.g., sociologists, web scientists, psychologists, educators, and law scientists), who try to understand how and why some people use ICTs in maladaptive ways. Empirical research on cyberbullying has expanded over the last 5 years, and the available evidence points to several aspects of the problem that need to be resolved. Nevertheless, cyberbullying is a rather complex phenomenon that requires an interdisciplinary approach, so that the various aspects related to its nature and prevalence can be better understood. The present book is built on that argument and attempts to provide a holistic and interdisciplinary perspective on cyberbullying. Our aim is to present several approaches that can lead to more effective educational interventions against cyberbullying in the future. We present empirical evidence from school-based studies in Greece, as well as several contributions from education, law, psychology, and web science.

The book is entitled ‘Cyberbullying in Greece: An Interdisciplinary Approach’ and is part of the deliverables of the
European-wide research project ‘Cyberbullying in adolescence: Investigation and intervention in six European Countries’, which was funded by the EUROPEAN COMMISSION, DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY, Daphne III Program. The leading investigator and project coordinator for Greece was Professor Haralambos Tsorbatzoudis.

This section summarizes the findings and perspectives presented in the Greek section of the book, by presenting a series of extended abstracts written in English. We hope that this effort will increase access to non-Greek speaking populations and accordingly reach a wider audience.

The following text includes a preface by Professor of Medicine Sophia Kouidou, Vice Chancellor for Research of the Aristotle University of Thessaloniki, as well as several theoretical and empirical contributions. Namely, Dr Antonis Travlos, Senior Lecturer at the Department of Sports Administration of the University of Peloponnese, and Ms Irene Douma, MSc discuss several theoretical approaches to bullying behavior. Dr Michalis Vafopoulos provides an interesting account about ‘web literacy’ by the perspective of Web science, whereas Dr George Nouskalis, Lecturer of Law at the Law School of the Aristotle University of Thessaloniki, discusses the legal framework and the available tools for the prevention and penalization of cyber crime behaviours.

What follows, is a series of empirical studies on Cyberbullying among Greek adolescents. Professor Haralambos Tsorbatzoudis and Dr George Angelakopoulos from the Department of Sports and Physical Education, Aristotle University of Thessaloniki, present prevalence data and characteristic of cyberbullying in a representative sample of Greek adolescents from several regions in mainland Greece and the islands. Ms Anastasia Kapatzia, MSc in
Psychology, and Professor Efthimia Syngollitou, Department of Psychology, Aristotle University of Thessaloniki, present findings from a school-based study in Northern Greece. Dr Lambros Lazuras, Research Psychologist at the South-East European Research Centre (SEERC) and Lecturer at the International Faculty of the University of Sheffield, together with Ms Despoina Ourda, MSc provide empirical evidence about an integrated theoretical model of psychosocial risk factors of cyberbullying. Finally, Dr Vassilis Barkoukis, Lecturer at the Department of Physical Education and Sports Science, Aristotle University of Thessaloniki, and Mr Christos Panagiotou, Physical Educator, based on their scientific expertise and practical experience, discuss evidence-based educational approaches for the prevention of cyberbullying in adolescence.

We would like to express our gratitude to all the students and educators who helped us complete this project by taking part in our studies. Also, this project would never be realized without the financial support of the European Commission (DAPHNE III Program). Finally, we would like to warmly thank Professor George Grouios, Department of Physical Education and Sports Science, Aristotle University of Thessaloniki, for his constructive comments and criticism that helped us improve the quality of this book.

We hope you enjoy reading

Haralambos Tsorbatzoudis
Lambros Lazuras
Vassilis Barkoukis
CONTENTS

PART 1

Bullying: An old problem in a new setting

Theoretical approaches in the study of bullying
Andonis Travlos & Irene Douma ................................................... 3

Changing (with) internet. But mind the gap
Michalis Vafopoulos ................................................................. 7

The provisions of the Greek penal code and the special criminal law statutes related with cyberbullying
George Nouskalis ....................................................................... 15

PART 2

Cyberbullying in Greece: Empirical data

Descriptive data on cyberbullying prevalence in schools across Greece
Haralambos Tsonbatzoudis & George Angelakopoulos ................. 29

Cyberbullying: Investigation of the nature and frequency of this phenomenon in adolescents
Anastasia Kapatzia & Efthimia Singollitou ................................. 33

Cyberbullying in adolescence: A social-cognitive study
Lambros Lazuras & Despoina Ourda ........................................... 41

PART 3

Educational perspective

Didactic approaches to tackle cyberbullying
Vassilis Barkoukis & Christos Panagiotou .................................. 47
PART 1

Bullying: An old problem in a new setting
CHAPTER 1
THEORETICAL APPROACHES TO THE STUDY OF BULLYING

Antonis K. Travlos & Irene Douma
Faculty of Human Movement and Quality of Life Sciences
Department of Sports Organization and Management, University of Peloponnese

It is commonly accepted and well recognized that school bullying has serious implications for students, educators, parents, and community members. Bullying is a widespread social problem that is linked to aggression, violence, psychological disorders, poor social adjustment, and physical unwellness as well as to later delinquency (Gini, 2006; Olweus, 1993; Swearer, Espelage, Vaillancourt, & Hymel, 2010). Although the scientific community is concerned with the study of bullying for almost forty years, no comprehensive theory has been developed to examine and explain bullying in all its dimensions. Instead, there are several theoretical approaches, models and assumptions, that have inspired the researchers to explain bullying based on the scientific fields of psychology, pedagogy, criminology, sociology and genetics. The aim of the present chapter is to (a) summarize the theoretical models that have been developed for the description and interpretation of bullying and victimization,
and (b) identify the variables and factors that can contribute to improving planning and quality of intervention programs, which aim at minimizing bullying in schools.

Considering the scientific literature, the theoretical models that are mostly used for describing, explaining and predicting bullying are attachment theory, attraction theory, homophily hypothesis, social dominance theory, social information processing theory, theory of mind, social learning theory, social cognitive theory and moral disengagement, sociocultural theory, reintegrative shaming theory, and social-ecological theory.

Attachment theory argues that the quality of the relationship of children with parents or caregivers helps developing an internal processing model of relationships, which then affects how a person will interact with others (Main, Kaplan, & Cassidy, 1985). Attraction theory hypothesizes that adolescents, due to their need to establish independence from their parents, are affiliated more to peers who exhibit independence (e.g., disobedience, aggression) and non-compliant behaviors, than to younger peers that possess characteristics that reflect obedience and docility (Bukowski, Sippola, & Newcomb, 2000). Homophily hypothesis suggests that individuals have the tendency to associate with similar others that exhibit similar attitudes and behaviors as a result of “selective association” or/and “reciprocal socialization” (Espelage, Holt, & Henkel, 2003; Kandel, 1978). Social dominance theory accepts that people have the tendency to create hierarchies of social dominance. Groups with a clear hierarchy are better organized and therefore able to attack others to obtain additional resources or to defend themselves, thus increasing the likelihood of survival (Sidanius & Pratto, 1999). Social information processing (SIP) theory involves six stages of processing social information. Supporters of the model
agree that bullying is a result of incomplete or incorrect processing of social information in one or more of these stages (Crick & Dodge, 1994). Sutton, Smith, and Swettenham (1999) pointed out that the skills acquired by the bullies assume the appearance of a theory of mind – TOM, which is defined as the ability of children to justify their mental states (including beliefs, desires and intentions) for themselves and others, and use the knowledge to predict and understand behavior. From a social learning perspective, children learn through observation of adult and peer models (Bandura, 1971), “to use aggressive means to achieve their goals” (Espelage, Bosworth, & Simon, 2000, p. 326). According to social cognitive theory (Bandura, 1986, 1999), moral disengagement is the socio-cognitive process which allows the individual to commit negative and inhuman acts against others. This cognitive process includes eight mechanisms through which individuals may deploy to justify bullying behaviors. Sociocultural theory suggests that bullying can be addressed effectively by understanding the culture of the organization (e.g., school, home, society), rather than individual differences factors. Sociocultural theories emphasize the importance of modifying situational factors in behavior, rather than the individuals within the organization (Monks, Smith, Naylor, Barter, Ireland, & Coyne, 2009). Reintegrative shaming theory specifies that an important contributing factor to deal with bullying is the management of shame. The theory supports that the process of reintegration must take place in the presence and participation of social support mechanisms which respect and care about bullies and victims (Ahmed, Harris, Braithwaite, & Braithwaite, 2001). According to socio-ecological theory, bullying behaviors emerge from a complex interaction between personality and mood of children, which is modified as they experience various behaviors during childhood and adolescence (Swearer, Espelage, & Napolitano, 2009).
Although a number of interventions are available for bullying, the intervention programs do not have the expected success for three reasons; (a) no explicit theories are used for the selection and development of intervention programs, (b) basic structures of the theories are not used for the evaluation of programs, and (c) the selected programs are not compatible with the theoretical background of the problem (Orpinas & Horne, 2006). It is critical to emphasize that before choosing a specific intervention program, bullying specialists need to explore whether or not the intervention (a) is based on theory, as well as valid and reliable research findings, and (b) promotes positive social behavior (Swearer, Espelage, Vaillancourt, & Hymel, 2010).

*List of references at pages 23-32.
CHAPTER 2

THE WEB AS A TECHNO-SOCIAL SYSTEM

Michalis Vafopoulos
National Technical University of Athens, vaf@aegean.gr

The test of a free society is the liberty for the collective transformation of the world through abstractions freely chosen and freely actualized (Wark, 2004).

The Web emerged as an antidote to the rapidly increasing quantity of accumulated knowledge in the 20th century, which has been caused mainly by scientific progress and digitization technology. Human memory and processing power are extended through the storage and interconnection of online content. Web has been evolved from a piece of software code to a dynamical ecosystem of Users and multi-purpose functionalities. Despite its profound importance, it still remains an unexplored research field. Existing research efforts consider the web either as a pure technological construct or as an epiphenomenon of social discourse. Web science argues that the Web is a transformational and ethically-relevant techno-social system. Thus, it should be studied as a
standalone dynamic ecosystem of code and values. One of the envelope questions of Web Science is “what changes need to be incorporated in the Web ecosystem to best serve humanity?”

1. The facets of the Web

While the Internet was introduced 20 years ago, the Web has been its “killer” application with more than 2 billion users worldwide accessing some trillion Web pages. The Web shortened the time that is necessary for an innovation to become mainstream technology. It took 38 years for telephone technology to reach the threshold of 50 million users, while television needed 13 years, Internet 4 years, iPod 3 years and Facebook just 2 years.

Searching, social networking, video broadcasting, photo sharing and micro-blogging have become part of everyday life whilst the majority of software and business applications have migrated to the Web. Web is evolving from a simple fileserver to an enormous database of heterogeneous data. The fundamental hyper-linking property that enables positive network effects in document sharing (Web 1.0) is rapidly expanding to social spheres (Web 2.0) and URI-based semantic linkages among data (Web 3.0) (Vafopoulos, 2011a, 2011b).

The Web has been initiated as a software system of interlinked hypertext documents accessed via the Internet. With a browser, Users access Web pages that may contain text, images, videos, and other multimedia and navigate between them using hyperlinks.

The Web constitutes an information space in which the items of interest, referred to as resources, are marked up by a set of rules (i.e. HTML), identified by global identifiers (URI) and transferred by the
Hypertext Transfer Protocol (HTTP). They could be considered as “contemporary forms of what the Greeks of antiquity called hypomnemata” (i.e. mnemotechnics) (Stiegler, 2010). The Web has become the most successful and popular piece of software in history because it is based on a technical architecture, which is simple, free or inexpensive, networked, based on open standards, extensible, tolerant to errors, universal (regardless hardware and software platform, application software, network access, public, group, or personal scope, language and culture operating system and ability), powerful and enjoyable.

Human participation in massive scale upgraded the Web from a piece of software to a living ecosystem, which affects Users and non-Users both in everyday and life-critical decisions. In the last decade, the transformative power of the Web stimulated its study as a standalone techno-social ecosystem (Berners-Lee et al., 2006; Vafopoulos, 2011c).

### 2. Web as a research space

The emergence of Internet and later the Web, has had an important influence on the research agenda of social and economic studies. The massive participation of Users in a variety of functions created a new terrain of field experiments and analysis concerning consumer behavior, market structure and policy implications. New forms of economic data (e.g. co-purchase networks, real time linked data from Eurostat etc.) enabled researchers to conduct new or existing investigations with less cost. For instance, the estimation of demand for thousands different products is now feasible with only a few weeks of time-series data from Web mass merchants (Chevalier & Goolsbee, 2003). Yet, the available data for research are just a tiny fraction of the collected data from Search Engines, mass merchants,
social networks and others in the Web. In contrast to physical and life sciences, where massive amounts of open data revolutionized fields like biology and physics, this is not happening for economic and social research (Lazer et al., 2009). The exclusive exploitation of behavioral data in the Web is an issue of prime importance with scientific, economic and social aspects. First, it limits academic research inside the “walled gardens” of companies and government agencies, excluding open scientific research and dialogue. Second, companies that hold data and afford to analyze them have built comparative advantages against (potential) competitors, or they are simply selling them for high profit. Finally, privacy and security risks (e.g. personal data leaks, almost-full profiling practices) create negative externalities in the personal and social level, which are not compensated. It is possible that the exclusive and limited data exploitation will become (if it has not already been) the major source of negative externalities in the online world, a form of “digital pollution” similar to the environmental catastrophe resulting from heavy industry operations in the traditional economy.

3. The Web as an object of study

The enormous impact, scale and dynamism of the Web in time and space exceed our abilities to observe and measure its evolution process. The complex interplay of social and technological entities occurring simultaneously in the micro and macro level calls for a huge and systematic research effort in order to understand it, model its stylized facts, and engineer its future uses in more prosperous ways. Apart from Economics, Web-related studies can be found in many other disciplines such as Computer and Information science, Mathematics, Social and Law studies, to name few.
The common characteristic of these studies is the lack of focus in the Web as a techno-social and standalone artifact. Usually, they refer to conventional questions and apply existing methodologies in their field. But the Web changes some of the underlying assumptions of the human society. The Web depreciates the cost and the institutional barriers to increase the practical potential to exploit the inputs and outputs of the information economy. Peer production emerges, as the third mode of production, a third mode of governance, and a third mode of property. Thus, it is crucial for the future of the online part of our new life to select the fundamental issues, to set new priorities and to concentrate, organize and expand the efforts of Web study.

The trans-disciplinary field in this direction has been entitled “Web Science”. Web science is taking the Web as its primary object of study. It is focused in the significant reciprocal relationship among the social interactions enabled by the Web’s design, the scalable and open applications development mandated to support them, and the architectural and data requirements of these large-scale applications (Hendler, Shadbolt, Hall, Berners-Lee, & Weitzner, 2008). One of the envelope questions of Web Science is “what changes need to be incorporated in the Web ecosystem to best serve humanity?”

Practically, every discipline is focusing its research efforts on the most important issues during specific periods of time. Nowadays, economists put their efforts to discover new ways for estimating systemic risk because of the severe financial crisis (Vafopoulos, 2012a); biologists try to find new personalized treatments for chronic and fatal diseases after encoding DNA, and so forth. Concerning the Web ecosystem, scholars are facing two major research challenges:
1. To preserve and expand the fundamental right of equal and universal online access to information against restrictive political actions and oligopolistic business practices and
2. To accelerate socio-economic development by facilitating life-critical functions in the developing world and by enabling the publication, interlink and re-use of valuable datasets and services in the developed world.

4. The Web as an ethically-relevant space

The Web has been built on the Internet stack, enabling the interlinkage of digital beings. Despite the fact that it shares some common characteristics with its underlying technologies, creates a new feasibility and actuality space. The Web is sufficiently unusual, transformative and necessary to human existence, and as such it requires more systematic philosophical thinking to describe its ethically-relevant properties. Initial motivation behind the development of the Web was based on ethical principles like esteem, pride, excellence, absence of guilt, rewards, and indignation (O’Hara, 2010). Originally it was more a closed “Aristotelian world” than a space governed by rules, roles, hierarchies and deliverables. We believe that the above-mentioned virtues are the core driving forces of its exponential impact. These classic values that inspired the inventor and early Web Users and supported its massive dissemination, have now become more specific in practice.

It becomes the time for science to pay back the debt to the Web and provide an epistemological “antidote” to these issues. On this campaign, Philosophy should be in the front line by forming the main questions and setting the research framework. Recent research efforts (Vafopoulos, 2012b, 2012c; Vafopoulos, Stefaneas, Anagnostopoulos, & O’Hara, 2012) initiated the dialogue for a
theory about existence and the basic functions in the Web that will serve as a bridge between philosophical engineering and applied science (e.g., economics, computer science).

Scholars should look deep in the heart of the Web creation, to propose and engineer perspicacious solutions that will benefit the entire society. The quest for new requirements should directly address the needs, and promote human values. Web issues and ethics should be thoroughly investigated in order to become a handy compass for Users, entrepreneurs and governments to direct their decisions towards prosperous ways.

The Web is a unique piece of technology not only because of its breakthrough technological innovation, but mainly because it provides a new basis for expressing human creativity, and reveals “inactive” parts of human nature. Apart from understanding its morality, it is an inspiring challenge to transfuse the essence of our experience and the values of the Web to reassess concepts like freedom, choice, participation, inequality, and development. We agree with (Wark, 2004) that “It is not just information that must be free, but the knowledge of how to use it. The test of a free society is not the liberty to consume information, nor to produce it, nor even to implement its potential in private world of one’s choosing. The test of a free society is the liberty for the collective transformation of the world through abstractions freely chosen and freely actualised.” The role of Web science could be to elaborate and specify the motives, attitudes and engineering of this new version of utopia.

*List of references at pages 77-78.
CHAPTER 3

THE PROVISIONS OF THE GREEK PENAL CODE AND SPECIAL CRIMINAL LAW STATUTES RELATED TO CYBERBULLYING

George Nouskalis
Phd, Lecturer in Penal Law, Aristotle University of Thessaloniki,

INTRODUCTION

Since there is not a legal definition of cyberbullying in Greece it is worthy investigating the relative provisions of the Greek Penal Code about the conducts which constitute a similar harassment, as much of what constitutes the most important types of minors’ bullying with online means can be addressed with some of recent amendments of (cyber) criminal law¹.

In this paper I try to make clear that in order to propose a theoretical model of a potential codification of cyberbullying

elements it is necessary to define the limits between the different forms of -sexual or not- cyberharassment and cyberbullying.

**Provisions of Greek penal law**

*A) Greek Penal Code (GPC)*

**I. The Provisions of Violation of Computer Programs which are Secret [Article 370 (b) GPC]**

Article 370(b) paragraphs 1–4 were added in the Greek Penal Code in Chapter 9 with the 1805/1988 Act, under the title “Violation of secrets”. According to this:

1. Whoever, without authorization, copies, uses, discloses to another person, or in any way violates data of a computer or a computer program, which belong to the realm of state secrets, privates secrets, business secrets, trade secrets privacy, shall be punished by imprisonment from three months to five years. Private computer data or programs should be considered and all the data and programs that the legal holder keeps them secret with justified interest, especially if the owner had taken security measures.

2. If the offender is in the service of the legal holder of the data, or the secret computer data and programs have a great economic value, the act shall be punished by imprisonment from one year to five years.

3. If the secret computer data and programs belong to the realm of military or diplomatic secrets, or of the security of the state, the act shall be punished according to Articles 146–147.

4. The offences of paragraphs 1–2 are prosecuted only upon complaint.
The basic concept of the provision is the protection of private secrets, when these secrets are of substantial significance to the business or enterprise of another or they belong to the realm of scientific or state secrets. The protected legal interest is the privacy and not the confidentiality or integrity of computer systems.\textsuperscript{2} There is no requirement for infringement of security measures, but the act of infringement is only an indication for the legislator to consider as secret the protected computer data and programs.

According to the above provisions, necessary material element of the offence is the concept of ‘secret computer data and programs’. The ‘justified interest’ of the legal holder of the secrets is only an indicator of the existence of privacy. The above element required for the criminal offence according to Article 370B is not a computer-specific one. In order for the offence to be committed, the criminal provision is not concerned with the value of the computer data or programs but is applicable in any case that the ‘legal holder’ keeps them in privacy.\textsuperscript{3}

In order for the offence to be punished, the offender should know that he is not authorized to commit the above acts against computer data and programs and that these objects belong to the realm of secrets. The negligence is not enough to establish the offence. The kind of intention required is not only the purpose to use, copy, or to disclose the computer data and programs (\textit{dolus directus}) but also the acceptance by the offender of the above result as necessary or as possible by-product of his act (\textit{dolus eventualis}).

\textsuperscript{2} See Milonopoulos, \textit{op. cit.}, pp. 93–94.
II. The Provisions of Unauthorized Access to any Computer Data [Article 370(c) (2–4)]

Article 370(c) (2–4) were added in the Greek PC in Chapter 9 with the 1805/1988 Act, under the title “Violation of secrets”. According to this:

“2. Every one who obtains access to data recorded in a computer or in the external memory of a computer or transmitted by telecommunication systems shall be punished by imprisonment for up to six months or by a fine from 2,900 to 15,000 €, under condition that these acts have been committed without right, especially in violation of prohibitions or of security measures taken by the legal holder. If the act concerns the international relations or the security of the State, he shall be punished according to Article 148.

3. If the offender is in the service of the legal holder of the data, the act of the preceding paragraph shall be punished only if it has been explicitly prohibited by internal regulations or by a written decision of the holder or of a competent employee of his.

4. The offences of paragraphs I–IV are persecuted only upon complaint.”

In order for the unauthorized access offence to be committed, two material elements call for detailed consideration. The first one is the concept of access. The above provision of the PC constitutes ‘pure’ hacking, which refers only to the unauthorized accessing of computer data. As a reaction to ‘hacking’, the formal sphere of secrecy in the area of data protection was acknowledged as a new object of legal protection, and the action of ‘unauthorized access’ of data was penalized, although some experts have expressed the view that the mere act of obtaining unauthorized access should not be
The basic concept of the provision is that unauthorized access to computer data is often the preliminary to general criminal offences to traditional objects of penal law.

There is no requirement for infringement of security measures, but the act of infringement is only an indication for the unauthorized access to computer data recorded in a computer or in the external memory of a computer or transmitted by telecommunication systems, which means that data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner. The statute does not require a certain result of the ‘access’, but the offence should not committed only with the mere act of sitting at a computer keyboard. The offender should have the possibility to copy, move to any storage, alter or erase the computer data.

Next comes the question of whether access is unauthorized. This matter should be considered only by reference to the intentions of a party entitled to determine the concept of ‘authorization’. The offender is not authorized to have access to the computer data, when he is not entitled to control access or he has not the consent to access the computer data. In order for an offence to be established, the offender does not need to overcome some security measures, although if this happen, then he could not allege effectively that he has authorization for access. The existence of an authorization to access or of consent of the computer controller does not mean only a justification for the offender but the non-existence of an offence.

In order for the offence to be punished, the offender should know

---

that he is not authorized to have access to the computer data. The negligence is not enough to establish the offence. The kind of intention required is not only the purpose to gain access, but also the acceptance by the offender of the above result as necessary or as possible by-product of his act. If the offender is not aware that access is un-authorized, the offence is not committed.

III. Crimes against sexual freedom and dignity of children (Article 337 par. 3-4 GPC)

Article 337 paragraphs 3–4 were added in the Greek Penal Code with the 3727/2008 Act, in order to protect the legal interest of sexual freedom and dignity of persons underage of 18 and implement the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. According to this:

a) Any adult who intentionally contacts, through the Internet and other information and communication technologies, a child under the age of 15 years and offends his or her sexual freedom and dignity with sexual gestures or requests, shall be punished by imprisonment from 2 to five years. If the perpetrator repeats the before mentioned crime or he resulted in meeting the child shall be punished by imprisonment from 3 to five years.

b) Any adult who intentionally contacts, through the Internet and other information and communication technologies, a child appeared to be under the age of 15 years and offends his or her sexual freedom and dignity with sexual gestures or requests by shall be punished by imprisonment from 1 to 5 years. If the perpetrator repeats the beforementioned crime or he resulted in
meeting the child shall be punished by imprisonment from 3 to 5 years.

**B) Special criminal statutes**

**I. The Personal Data Protection Ac**

Pursuant to Article 22, paragraphs 1–9 of the Data Protection 2472/1997 Act:

“anyone who fails to notify the Authority, according to the provisions of Article 6 of this law, of the establishment or the operation of a file or any change in the terms and conditions regarding the granting of the permit referred to in paragraph 3 of Article 7 of this law will be punished by imprisonment for up to three (3) years and a fine amounting between 2,900 and 15,000 €.

2. Anyone who, in breach of Article 7 of this law, keeps a file without permit or in breach of the terms and conditions referred to in the Authority’s permit, will be punished by imprisonment for a period of at least one (1) year and a fine amounting between 2,900 and 15,000 €.

3. Anyone who, in breach of Article 8 of this law, proceeds to the interconnection of files without notifying the Authority accordingly will be punished by imprisonment for up to three (3) years and a fine amounting between 2,900 and 15,000 €.

Anyone who proceeds to the interconnection of files without the Authority’s permit, wherever such permit is required, or in breach of the terms of the permit granted to him, will be punished by imprisonment for a period of at least one (1) year and a fine amounting between 2,900 and 15,000 €.
4. Anyone who unlawfully interferes in any way whatsoever with a personal data file or takes notice of such data or extracts, alters, affects in a harmful manner, destroys, processes, transfers, discloses, makes accessible to unauthorised persons or permit such persons to take notice of such data or anyone who exploits such data in any way whatsoever, will be punished by imprisonment and a fine and, regarding sensitive data, by imprisonment for a period of at least one (1) year and a fine amounting between 2.900 and 30.000 €, unless otherwise subject to more serious sanctions.

5. Any Controller who does not comply with decisions issued by the Authority in the exercise of the right of access, pursuant to paragraph 4 of Article 12, in the exercise of the right to object, pursuant to paragraph 2 of Article 13, as well as with acts imposing the administrative sanctions provided under c, d and e of paragraph 1 of Article 21 shall be punished by imprisonment for a period of at least two (2) years and a fine amounting between 2.900 and 15.000 €. By the sanctions referred to in the preceding sentence shall also be punished any Controller who transfers personal data in breach of Article 9 as well as the person who does not comply with the court decision referred to in Article 14 of this law.

6. If the perpetrator of the acts referred to in paragraphs 1–5 of this Article purported to gain unlawful benefit on his/her behalf or on behalf of another person or to cause harm to a third party, then s/he shall be punished confinement in a penitentiary for a period of up to ten (10) years and a fine amounting between 6.000 and 30.000 €.

7. If the acts referred to in paragraphs 1–5 of this Article have jeopardized the free operation of democratic governance or national security, then the sanction imposed shall be confinement in a penitentiary and a fine amounting between 15.000 and 30.000 €.
8. If the acts referred to in paragraphs 1–5 of this Article were committed as a result of negligence, then imprisonment for a period of at least three (3) months and a fine shall be imposed.

9. For the purposes of the present Article, if the Controller is not a natural person, then liable shall be the representative of the legal entity or the head of the public authority or agency or organization, provided s/he also carries out in effect administrative or managerial duties.”

The basic form of the offence above is the unlawful interfering of personal data and the unlawful acts of data processing in Article 22(4) of the 2472/1997 Act. The other defined offences are aggravating or mitigating circumstances of the basic form. The basic concept of the above penal provisions is that any act of data processing is unlawful and shall be punished, except that there is a ground of justification, like the consent of the data subject or the permission of the Data Protection Authority or some of the justifications that defines the statute in a ‘closed system’ in Articles 4, 5, 7 and 7(a) of the 2472/1997 Act.5

The required mental element for the offender to be punished is all forms of intention, except the offence in Article 22(6), which requires the special intent to gain a benefit, and the offence in Article 22, paragraph 8, which penalizes the acts in paragraphs 1–5 when the offender acts negligently.

Pursuant to Article 2(a) of the above Act, ‘personal data’ mean any information relating to the data subject. Personal data are not considered to be the consolidated data of a statistical nature whence data subjects may no longer be identified. The statute defines ‘data processing’ in Article 2(b):

5 See G. Nouskalis, Cyber Law in Greece, p. 235, supra, fn. 2
‘Processing of personal data (“processing”) shall mean any operation or set of operations which is performed upon personal data by Public Administration or by a public law entity or private law entity or an association or a natural person, whether or not by automatic means, such as collection, recording, organization, preservation or storage, modification, retrieval, use, disclosure by transmission, dissemination or otherwise making available, correlation or combination, interconnection, blocking (locking), erasure or destruction.’

II. Article 253(A) (I) - Code of Criminal Procedure (CCP)

Mostly on the occasion of investigations into white-collar crime, prosecuting authorities have to analyze computer-stored bookkeeping data. In addition to this, perpetrators in the field of organized crime increasingly make use of computer systems and transfer data to computers abroad via telecommunication networks in order to render access more difficult for the prosecution authorities. Therefore, the use of computers in almost all areas of life frequently confronts prosecution authorities with computer-stored means of evidence, even on the occasion of investigations into ‘classic’ forms of crime.

Problems exist with the questions of whether and to what extent prosecuting authorities have the right to search computer systems, to seize data, to intercept and record telecommunication between computers, to have access to telecommunication data and to electronically supervise computers. A particular problem is presented by access to data which are stored at another location, possibly even abroad, in a telecommunication network that branches out in all directions. Additional problems are those of data protection in
criminal procedure. Because it exploits technology, cybercrime can create problems for investigators who must obey procedural rules crafted to deal with the investigation of crime in the ‘real world’ of physical space, not the virtual world of cyberspace. Procedural law may, for example, only provide authorization to search for and seize tangible evidence. Since the prosecution of cybercrimes usually requires collecting and analyzing intangible evidence, this omission can be a serious problem for investigators.

Greece has signed but not ratified the Convention on Cybercrime of the European Council. However, the Greek Parliament passed the 2928/2001 Act, which added Article 253(a) to the Code of Penal Procedure (CPP). Due to this article, the investigating magistrates can collect, only for charging with an offence under Article 187 of Penal Code about ‘organized criminality’, and combine any personal data, according to the provisions of 2472/1997 Personal Data Protection Act, which implemented Directive 95/46 EU. Law 2472/1997, in Article 7(a) (1) (6) grants the competent judicial authorities, the power to collect and process and personal data, if this measure is necessary for the investigation of any criminal or civil case.

According to the provisions of the above-mentioned provision and of Article 4(1–7) of Law 2225/1994, as well as the 3917/2011 Act implementing the Data Retention Directive 2006/24/EC, concerning the secrecy of communications, it is possible the interception of communications and traffic data for law enforcement. The purpose of the above surveillance is to investigating some very serious crime provided in the Penal Code such as child pornography. The interception may lawfully be conducted only under the terms – about the persons and the time of the interception – of a decision
issued by the judicial council, after a proposal and a hearing of the Public Prosecutor. The interception is lawful only if the judicial council considers that the detection of the case or the finding of the person accused is impossible or very difficult without the interception. The measure of interception could be valid not only against the accused person but also against persons that receive or transmit messages from the accused person.

**CONCLUSION**

The fact that the digital technology can contribute to the development of a notion of cyberbullying by offering new views about new legal interests cannot be contested. The critical challenge for the legislator is to codify the relative empirical and sociological assets in order to provide an effective set of legal remedies against cyberbullying. Jurisprudence also addressing the new legal problems has to establish a feeling of safety for the so called netizens.
PART 2

Cyberbullying in Greece: Empirical data
CHAPTER 4

CYBERBULLYING PREVALENCE IN GREECE: FINDINGS FROM A SCHOOL-BASED STUDY

Haralambos Tsorbatzoudis¹ and Georgios Angelakopoulos²
¹Professor, Department of Physical Education and Sport Sciences, Aristotle University of Thessaloniki
²Research Associate, Department of Physical Education and Sport Sciences, Aristotle University of Thessaloniki

INTRODUCTION

The suicide of three children from Norway as a result of intimidation attracted much of media attention in mid 1990’s (Olweus, 1994). In a similar vein, the news that a 13 year old British student committed suicide following offensive and insulting remarks by some of his schoolmates on the web, shocked the world. Similar incidents of suicide attempts following school violence have been also reported in Japan and Canada.

In the past years there have been several efforts to monitor and record cyberbullying incidents in Greece, and accordingly assess the impact of these incidents on the psychological well-being of victims. In a study of the European action 'Safe Net Home' it was found that
54% of the respondents were victims of cyberbullying, reporting experienced intense harassment and blackmail. What’s important is that 40% of the victims could not identify the aggressor, thus showing that it is rather hard to identify the perpetrators of online aggression.

**Method**

The present study was supported by the DAPHNE III Program, of the European Agency for Justice, Fundamental Rights, and Citizenship. The sample of the study consisted of 997 pupils from 22 randomly selected secondary schools, in different regions of Greece (Northern and Southern Greece, mainland, islands). Overall, 487 of the respondents were males, and 510 were females. A structured questionnaire was used assessing behavioural responses of both victims and perpetrators of cyberbullying. The questionnaire derived from a previous DAPHNE project on traditional bulling and cyberbullying (DAPHNE II: Brighi, Guarini, & Genta, 2009), and new questions were added to catch up with updates in cyberbullying research and accommodate other theoretically-relevant variables. [Brighi, Ortega, Pyzalski, Scheitauer, Smith, Tsorbatzoudis, Barkoukis, Del Rey, Guarini, Plichta, Schultze-Krumbholz, & Thompson (2012), European Cyberbullying Intervention Project Questionnaire - ECIPQ. Unpublished Manuscript, University of Bologna].

**Results**

With respect to mobile phone and internet use, 50% of the pupils reported using their mobile up to two hours each day. A remarkable finding was that almost 1 out of 5 (18%) said they used their mobile phones more than five hours daily. With regard to internet, 23% reported that they use the internet for approximately two hours a day, 21% two to three hours, while 10% spend more than five hours each day for ‘surfing’ the Web.
Concerning the victims of cyberbullying, the results showed that the prevalence of cyberbullying incidents is close to 10%. However, 34% of the pupils reported that they have perceived such incidents in their friendly environment sometime in the past months. Also, the use of insulting and offensive messages was the most common form of cyberbullying, both through internet/Web media and the mobile phone (e.g., texting). Threatening messages were less prevalent forms of cyberbullying, and even scarcer were cases of hacking and stealing information from another person’s account. Cyberbullying victims reported that they mostly confronted rumour spreading in the internet, being attacked or insulted in an online game, as well as the experiencing hacker attacks to personal information (e.g., someone stealing their passwords.

Regarding the behaviour of cyberbullies, hacking personal passwords and pretending to be someone else were very common forms of cyberbullying in this study. Overall, our findings indicate which forms of cyberbullying are most prevalent, and also describe the context wherein cyberbullying incidents are more likely to occur (e.g., in online gaming or during chatting). We could argue that while some of the reported cyberbullying behaviours are expected in a particular context (e.g., attacking or offending someone in an aggressive online game), they may have totally different connotations and impact if practiced in another context. Yet, other forms of cyberbullying (e.g., hacking other people’s accounts) fall within the broader categories of online crime, and thus, are morally impermissible and legally reprehensible. The posting of personal information, embarrassing video and photographs oscillate in 6% and 4% respectively. Furthermore, the “alteration” of photographs or video is a practice that assembles low percentages among the pupils.
Finally, it emerges that only 7% of the children experienced rejection, in social networking sites, one-or-two times.

**DISCUSSION**

On the whole, this study was one of the first attempts to systematically record and monitor cyberbullying incidents in a representative sample of Greek adolescent students. The findings make it rather clear that cyberbullying is part of an adolescents’ daily life, either from the perspective of the victim, the perpetrator, or both. The most common practices of cyberbullying were identified, and students’ beliefs about the potential perpetrators were also assessed. Overall, it appears that cyberbullying in Greece is still at low levels. Instead of taking this as evidence of a relatively safe online environment, it should be noted that the ongoing expansion of new digital media may give further rise to cyberbullying and provide new channels for the perpetration of aggressive behaviours. Thus, cyberbullying in Greece could be seen as a ‘sleeping giant’, rather than as ‘another person’s problem’. In better understanding the nature and impact of cyberbullying one should further assess the emotional and semantic values adolescents attach to the various forms of cyberbullying, and accordingly shape prevention strategies.

*List of references at pages 137-142.*
CHAPTER 5

CYBERBULLYING IN MIDDLE AND HIGH SCHOOLS:
AN INVESTIGATION OF THE NATURE AND EXTENT
OF CYBERBULLYING IN ADOLESCENCE

Anastasia Kapatzia\textsuperscript{1} and Efthimia Sygkollitou\textsuperscript{2}
\textsuperscript{1}PhD Candidate, Department of Psychology, Aristotle University of Thessaloniki
\textsuperscript{2}Professor, Department of Psychology, Aristotle University of Thessaloniki

INTRODUCTION

The aim of the study was to investigate the nature and extent of adolescents’ experience of cyberbullying, and identify any gender and age-related differences. The questionnaire used was a short version of the “Cyberbullying Questionnaire” (Smith, Mahdavi, Carvalho, Fisher, Russell, & Tippett, 2006) and consisted of 34 multiple choice questions divided in two sections.

Method

Totally, 544 pupils (266 9\textsuperscript{th} graders aged 14-16 and 278 11\textsuperscript{th} graders aged 16-19) participated in the survey. Of them, 47% were
boys and 53% were girls. The selected school units were five middle schools and five high schools, and were located in Thessaloniki, second largest Greek city. The study was completed in May, 2007.

As in the longer version of the “Cyberbullying Questionnaire”, the short version provided a standard definition of bullying and described various types of cyberbullying. Questions regarding bullying included the following: being bullied (traditional form) and bullying others in school, as well as being cyberbullied and/or cyberbullying others inside and outside school in the past two months. The first section reflected several types of mobile bullying, including text messaging, picture/video clip, and bullying through mobile phones. Participants reported whether they had a mobile phone, and accordingly answered three questions: the perceived impact of cyberbullying via mobile phone; the awareness of cyberbullying incidence; and whether they were aware of mobile phone bullying incidents among their peers or in their school. In order to assess bystander effects, those students reporting awareness of cyberbullying incidents were further instructed to indicate whom they reported the incident to (if at all). The remaining questions were identical to those of the “Cyberbullying Questionnaire”. Participants circled the type of mobile phone bullying they have experienced. The second section, used the same structure as the first section of the questionnaire and addressed cyberbullying via internet (e.g., through e-mails, chat-room, instant messaging, and websites/blogging). Finally, the questionnaire assessed demographic data, such as age, gender, GPA scores and educational background of parents.
CHAPTER 5

Results

The results showed that pupils were more likely to be cyberbullied than to traditional bullying; on the other hand, bullies were more often perpetrators of face-to-face bullying than cybebullying.

Statistical analyses revealed a significant correlation between the experience of bullying and cyberbullying, as well as between bullying and victimization. It was also found that bullying victims did not tend retaliate by engaging in cyberbullying against others. Regarding gender, data analysis revealed that boys were more likely to engage in both traditional bullying \([F(1,531) = 31.34, p = .000]\) and cyberbullying \([F(1.531) = 14.20, p = .000]\) than girls. Finally, pupils in 9th grade admitted that they have been bullied in school more often (9th grade mean =1.28) than pupils in [11th grade (11th grade mean = 1.14), \(F = (1,531) = 5.72, p = .017\].

In terms of owning a mobile phone, 529 respondents answered affirmatively, and 14 negatively. For those pupils who were cyberbullied via mobile phone, phone call bullying (19.1%) was found to be the most common form of cyberbullying compared to SMS bullying (5.9%), and to a combination of SMS and phone call bullying (4.8%). Four hundred participants (73.5%) reported being internet users, and the majority of pupils reported that the most common form of cyberbullying was through chat-rooms (6.1%) and to a lesser extent through emails (2%) and instant messaging (1.8 %). The majority of cyberbullying incidents, both via mobile phones and internet, occurred outside school premises.

Compared to girls, boys admitted that they cyberbullied others via mobile phone more frequently both inside \([F = (1.531) = 11.93, p = .001]\) \((M_{boys} = 1.45, M_{girls} = 1.16)\), and outside school \(F = (1,528) =\)
13.42, \( p = .000 \) (\( M_{\text{boys}} = 1.56, M_{\text{girls}} = 1.24 \)). Regarding internet bullying, the analysis showed that more girls than boys reported being victims of internet cyberbullying both inside school (\( M_{\text{girls}} = 2.60, M_{\text{boys}} = 1.70 \)) \([F(1,531) = 26.32, p = .000]\), and outside school (\( M_{\text{girls}} = 2.68, M_{\text{boys}} = 1.79 \)) \([F(1,530) = 25.87, p = .000]\). Interestingly, girls also have cyberbullied others more frequently than boys both inside school (\( M_{\text{girls}} = 4.46, M_{\text{boys}} = 3.21 \)) \([F(1,530) = 37.07, p = .000]\) and outside school (\( M_{\text{girls}} = 4.51, M_{\text{boys}} = 3.38 \)) \([F(1,529) = 31.33, p = .000]\). Girls also reported being victims of internet bullying for a longer period of time than boys (\( M_{\text{girls}} = 5.02, M_{\text{boys}} = 3.44 \)) \([F(1,529) = 40.46, p = .000]\).

Pupils in 9th grade said that they have bullied others via mobile phone outside school more often (\( M_{9\text{th grade}} = 1.49 \)) than students in 11th grade (\( M_{11\text{th grade}} = 1.31 \)), \([F = (1,528) = 4.25, p = .040]\). Further analysis showed significant interaction between gender and grade variables only in one question; boys in 11th grade have been cyberbullied more frequently (\( M_{11\text{th grade}} = 1.43 \)), as compared to boys in 9th grade (\( M_{9\text{th grade}} = 1.18 \)), \([F(1,531) = 13.31, p = .000]\). On the other hand, girls in 9th grade have been cyberbullied more frequently (\( M_{9\text{th grade}} = 1.43 \)), as compared to girls in 11th grade (\( M_{11\text{th grade}} = 1.22 \)), \([F(1,531) = 13.31, p = .000]\). In most cases, cyberbullying incidents lasted one or two weeks.

Data analysis showed that the majority of pupils that have heard about cyberbullying incidents reported it to friends, but a substantial number of pupils didn’t report it to anyone, whereas a few students chose to reveal it to adults, especially to their teachers. It is noteworthy that the same trend is revealed for the victims of cyberbullying. Further statistical analysis showed that girls more often reported incidents of mobile phone bullying to
parents/caregivers \[\chi^2 (2) = 5.989, \ p < .050\], or chose not to tell anyone \[\chi^2 (2) = 7.732, \ p < .021\]. On the other hand, boys told about their victimization through mobile phone to their class teachers \[\chi^2 (2) = 8.301, \ p < .016\] while girls told so to their friends \[\chi^2 (2) = 7.991, \ p < .018\]. According to the chi-square statistical analysis, girls preferred to reveal cyberbullying incidents to their parents/caregivers \[\chi^2 (2) = 7.785, \ p < .020\], and were more likely to speak about their victimization through internet to another person \[\chi^2 (2) = 30.812, \ p < .000\], while boys didn’t report to anyone \[\chi^2 (2) = 32.014, \ p < .000\].

Three questions investigated the profile of those that experienced cyberbullying via mobile phone. Respondents were asked in which class the perpetrator of cyberbullying belonged in, the gender of the perpetrator, and how many pupils were involved in the incident. Amongst cyberbullying victims, 50 (9.2%) said that they didn’t know the cyberbully, 32 (5.9%) that he/she is not from school and a few others indicated that the cyberbully was from a different class. Analysis by gender indicated that girls reported that the perpetrator of mobile phone bullying was in their class \[\chi^2 (11) = 23.523, \ p < .015\] and was mainly one boy but also they reported that they didn’t know who cyberbullied them \[\chi^2 (7) = 37.259, \ p < .000\]. Boys answered that they had been cyberbullied through mobile by several girls \[\chi^2 (7) = 37.259, \ p < .000\]. Moreover, boys reported that perpetrators of internet bullying were in different grades \[\chi^2 (8) = 41.001, \ p < .000\] and that they had been cyberbullied through internet by many girls \[\chi^2 (7) = 48.654, \ p < .000\]. Girls answered that they had been cyberbullied through internet equally by one boy and several boys, \[\chi^2 (7) = 48.654, \ p < .000\]. Also 9th graders said that they had been cyberbullied by many boys \[\chi^2 (7) = 15.487, \ p = .030\].
Overall, the majority of respondents believed that in comparison to traditional bullying, cyberbullying has either the same effects or is more harmful upon the victim. Girls believed that mobile phone bullying had the same effect on its victim compared to “traditional” bullying, while boys answered that they didn’t know whether or not it had the same effect \(\chi^2 (3) = 16.961, p < .001\]. Regarding the impact of internet bullying, girls reported that it has the same effect on the victim, while boys answered that they didn’t know whether or not it does \(\chi^2 (3) = 25.288, p < .000\]. Regarding the grade of pupils, 9th graders answered that didn’t know about impact of mobile phone bullying while 11th graders believed that mobile phone bullying has less than or the same effect on its victim to traditional bullying \(\chi^2 (3) = 35.051, p < .000\]. Eleventh graders reported that internet bullying has less of an effect on the victim compared to traditional bullying while 9th graders reported that they didn’t know whether or not it had less of an effect \(\chi^2 (3) = 26.171, p = .000\].

Pupils were against the implementation of strict rules, such as banning mobile phone or internet use in school, as a strategy to prevent cyberbullying victimization. Specifically, 387 (71.1%) pupils believed that banning mobile phone will not prevent cyberbullying as cyberbullies could use mobile phones secretly, 117 (21.5%) said that the cyberbullies will use it after school and only 37 (6.8%) respondents approve the ban on mobile phone use in school premises. Finally, 113 (20.8%) pupils answered that the bullies will use internet in school secretly, 391 (71.9%) respondents thought that they will use it after school and only 35 (6.4%) approved banning internet use in school.
**DISCUSSION**

Overall, the present study provided prevalence rates of traditional bullying and cyberbullying in a sample of middle and secondary school students in Thessaloniki, Greece. The study also addressed students’ beliefs towards the nature and impact of cyberbullying, as well as towards school-based policies to tackle cyberbullying incidents.

*List of references at pages 172-174*
CHAPTER 6

CYBERBULLYING IN ADOLESCENCE.
A SOCIAL-COGNITIVE STUDY

Lambros Lazuras$^{1,2}$, Despoina Ourda$^1$

$^1$Department of Physical Education and Sport Science, Aristotle University of Thessaloniki
$^2$South-East European Research Centre (SEERC)

INTRODUCTION

Cyberbullying is an emerging form of aggression utilizing contemporary information and communication technologies (ICTs), and occurring mostly during adolescence. Cyberbullying can be seen as a ‘hi-tech version’ of traditional bullying (Patchin & Hinduja, 2006, 2010), but such a definition should be treated with caution for the following reasons. Firstly, unlike traditional face-to-face bullying, cyberbullying does not require physical strength, it is not limited by physical space, provides total anonymity to the aggressor, and makes the bullying act visible to potentially large audiences (e.g., by posting a humiliating video on Youtube that can be easily accessed by an unlimited number of users). Identifying the major
differences between cyberbullying and traditional bullying, and assessing the impact of cyberbullying on victims is a necessary first step in cyberbullying research (for instance see Li, 2007; Slonje & Smith, 2008). Nevertheless, it is equally (if not more) important to understand the psychological processes leading to cyberbullying in adolescence.

To achieve this goal, one could resort to traditional bullying research and identify potential similarities in the processes underlying both face-to-face bullying and cyberbullying. Indeed, research has shown that low levels of empathy significantly predict bullying behavior in both physical and cyber space (Jolliffe & Farirngton, 2006). Thus, empathy can be seen as a potential risk factor for bullying behaviours, independently of the means utilized (e.g., face to face confrontations or online/digital communications) by the aggressor. Another way to understand the process of cyberbullying, however, is to try to understand the fundamental mechanisms leading to such an action. Specifically, cyberbullying can be seen as an intentional, means-to-an-end action, which requires some sort of premeditation and planning. That is, the aggressor plans a certain course of action to hurt the victim, by, say, finding and posting embarrassing pictures or videos online, or merely sending anonymous threatening messages. In this line, the process of cyberbullying could be understood through the study of social psychological theoretical models of intentional behaviours. In fact, one could integrate past research findings on cyberbullying (e.g., Ang & Goh, 2010) and identify how individual traits and dispositions with a well established effect on cyberbullying (e.g., empathy), interact with related social cognitions, and jointly predict intentions to engage in cyberbullying.
The present study addressed this question by employing an integrated theoretical model incorporating empathy and psychosocial variables derived from the Theory of Planned Behaviour (Ajzen, 2002) and the Prototype/Willingness Model (Gerrard, Gibbons, Stock, Vande Lune, & Cleveland, 2008). It was expected that empathy will predict cyberbullying intentions both directly, and indirectly, through the effects of social cognitions (attitudes, social norms, risk prototypes, and self-efficacy beliefs). This study is part of a larger scale project on Cyberbullying in Adolescence, funded by the EU under the DAPHNE III Program.

Method

A cross-sectional survey approach was used and structured questionnaires were completed in the classroom during regular teaching hours by 125 secondary school students in Athens, Greece (M age = 16.57 years, SD = 0.61, 36.3% boys).

Results and Discussion

The findings partially supported our hypotheses, by showing that only affective empathy (and not the cognitive empathy facet) predicted cyberbullying intentions. However, this effect was fully mediated by self-efficacy beliefs (i.e., situational temptation); thus, showing that adolescents with lower levels of affective empathy feel that they cannot easily resist temptations to hurt someone through cyberbullying, and accordingly form stronger intentions for cyberbullying behaviour. Overall, our study shows that while empathy-related variables are important (Ang & Goh, 2010; Jolliffe & Farirington, 2006), a better understanding of the cyberbullying
process requires a more detailed analysis of the psychological mechanisms linking empathy with related cognitions and behavioural intentions.

*List of references at pages 191-194.*
PART 3

Educational perspective
CHAPTER 7

DIDACTIC APPROACHES FOR TACKLING CYBERBULLYING

Vassilis Barkoukis & Christos Panagiotou
Department of Physical Education and Sport Science, Aristotle University of Thessaloniki

INTRODUCTION

Cyberbullying is a modern form of bullying that is realized through electronic means and digital media. Similarly to traditional bullying, cyberbullying is a form of aggressive behaviour against another person. However, unlike traditional bullying, cyberbullying does not require face-to-face confrontation and the interaction between the bully (or bullies) and the victim (or victims) is typically manifested remotely through mobile phones and the internet, thus ensuring the anonymity of the aggressor(s) (Smith et al., 2008).

Although numerous interventions have been applied to tackle bullying in adolescence, the meta-analysis by Merrell, Gueldner, Ross, and Isava (2008) indicated that these interventions had, at best, moderate effects. While they modified several psychological parameters related to bullying, they largely failed to produce any
changes in actual behavior. Nevertheless, some guidelines for effective interventions have been proposed from past research. Namely, to be effective, interventions should a) be based on a solid theoretical background, b) reassure strong commitment from both the research team and the school, c) adopt a holistic perspective, d) use valid instruments and employ sophisticated statistical analyses, e) develop a safe and supportive environment for students, f) include teachers’ education on bullying, g) intervene at both individual and interpersonal level and h) involve parents (Finger, Craven, Marsh, & Parada, 2005).

Taking into consideration the conceptual similarity between traditional bullying and cyberbullying (i.e., both being aggressive acts but utilizing different means), prior experience with intervention development for traditional bullying could be used to formulate more effective interventions to tackle cyberbullying in adolescence. Furthermore, recent developments in cyberbullying research provide another useful strand of evidence that could serve as the basis for effective interventions against cyberbullying in youth.

**Educational Strategies**

The basic element of such interventions would be to adopt a holistic approach incorporating actions at both the school and class levels, as well as the proximal environment of children and adolescents (i.e., parents).

At the school level, actions aiming to prevent the manifestation of cyberbullying through education and organizational function should be employed. The basic elements of these actions should involve a) the adoption of the appropriate school climate, b) the awareness and
sensitization of students, c) the education and mobilization of parents and d) the coordination of actions at the class level.

The adoption of mastery oriented climate has been associated with adaptive pattern of students’ responses, such as increased sense of belonging, higher academic self-efficacy and academic performance (Roeser, Midgley, & Urdan, 1996). Frequent academic boards and lectures by experts on the development of a mastery oriented climate could assist educators develop and maintain mastery-oriented teaching approaches. Also, these activities will help the school authorities monitor and coordinate the actions taken at the class level. Furthermore, activities, such as lectures and presentations to students, distribution of leaflets, billboard and poster sessions, school visits to authorities and agencies related to the prevention of cyberbullying, as well as participation in cyberbullying-related projects, are expected to increase students’ awareness and sensitization on cyberbullying. In addition, it is advisable that parents are involved in these activities either actively, or as spectators providing indirect support.

At the class level, the actions employed should increase a) students’ awareness and sensitization, b) social interactions and social acceptance, c) students’ social and moral skills, d) students’ social problem solving skills, e) self-esteem and self-efficacy, f) empathy and decrease moral disengagement and g) the involvement of parents.

Participation in class projects and peer-led activities can aid in improving students’ awareness and sensitization. Furthermore, educators should establish an environment that will promote social acceptance, social interactions among students, and cooperative learning in order to increase social acceptance and provide
opportunities for the development of social and moral skills. Additionally, several practices, such as modeling cyberbullying behaviors, external feedback on students’ social skills, exchange of ideas, emotions and motives, dialogue, role playing, observing others, and anger management, are thought to be effective in developing students’ social problem skills. Also, developing an autonomy supportive environment that allows students to participate in decision making processes could further increase their self-esteem and self-efficacy. All these actions closely associated with a mastery oriented climate could assist in increasing empathy and reducing moral disengagement. Finally, discussions with parents at the class level are important, especially in the case of reported cyberbullying incidents in the class.

In addition, the cooperation of school authorities with organizations and agencies involved in bullying and cyberbullying prevention and treatment (i.e., police electronic crime unit, educational institutions, NGOs etc.) could further improve preventive strategies and achieve greater impact in changing adolescents’ perceptions and behaviours towards cyberbullying.

**Summary**

Overall, the school provides a context wherein prevention interventions could be applied and effectively tackle cyberbullying. The actions comprising these interventions should be employed consistently by the school authorities and educators, and engage parents/caregivers and the wider community.

*List of references at pages 231-235.*