Youth Pathways into Cybercrime

Research leads:
Professor Mary Aiken,
Professor Julia Davidson
& Dr Philipp Amann

October 2016

EUROPOL EC3 European Cybercrime Centre

UCD Geary Institute for Public Policy
Research, Analysis, Evidence

Middlesex University

Youth Pathways into Cybercrime

Research Leads:

Professor Mary Aiken, Professor Julia Davidson & Dr Philipp Amann

Research Manager: Dr Jeffrey DeMarco

Consultants: Dr Pavel Gladyshev & Dr Selga Medenieks

Research Assistants: Ciaran Haughton and Giulia Perasso

October 2016

Funded by

PALADIN℠
CAPITAL GROUP

1. Introduction

This research project was established to draw together existing, recent evidence on online behavior and associations with criminal and antisocial behavior amongst young people. Specifically, it was designed to explore the trajectories and pathways that lead to ‘cyber-criminality’ through a series of mixed-methodological endeavors and the integration of theoretical frameworks across criminology and psychology, including cyberpsychology and computer science. The potential pathway from technology talented curious youth, to cyber juvenile delinquent, to lone cybercriminal to organized cybercrime was considered.[1]

Given the complex nature of online activities and behaviors, the inclusion of stakeholder experts from policing, industry and cybersecurity backgrounds was considered essential in terms of exploring developmental aspects of online criminal offending. Young people are increasingly committing and being drawn into cyber-criminality.[2] For example, in 2015, a UK telecommunications company had a security breach and lost valuable data. Five suspects were arrested in connection with the investigation, all aged between 15 and 20 years of age.[3] The company has subsequently reported that the data breach has cost the firm up to £60 million; an estimated 101,000 customers have left the company following the hack.[4] In October 2016 the company was fined £400,000 for theft of customer details and their failure to implement basic cybersecurity measures. The UK Information Commissioner's Office, which imposed the fine, said security was so poor that the attack succeeded "with ease", which is notable given the age of those arrested.[5]

In 2014 Wang Zhengyang, a 13-year-old boy who's been dubbed China's 'hacking prodigy' hacked into a school computer system to get answers to his homework. In a separate case, a British teenager who worked as a ‘hacker for hire’ was spared a prison sentence after having orchestrated cyber-attacks targeting global institutions from his bedroom. This teenager was just 13 when he joined a network of online hackers.

It is clear that young people have been recently arrested in hacking cases. In the behavioral sciences, it is well established that impulsivity and risk-taking behavior increases throughout the formative teenage years. Indeed, there have been reports of the increasing involvement of youth in criminal activity online for some time now. In 2015, the Australian Bureau of Crime Statistics and Research reported that cyber

[1] Mary P. Aiken, *The Cyber Effect* (New York: Random House Spiegel & Grau, 2016).
[2] Lia Harris, “Rise in child and teen fraud arrests mainly due to increase of internet-based crimes”, *Daily Telegraph*, April 11, 2015, http://www.dailytelegraph.com.au/news/nsw/rise-in-child-and-teen-fraud-arrests-mainly-due-to-increase-of-internetbased-crimes/news-story/fc620acdb8379e30ab46f17493e40475, accessed September 2016.
[3] “Fifth arrest in TalkTalk investigation”, Metropolitan Police, http://news.met.police.uk/news/fifth-arrest-in-talktalk-investigation-139221?utm_campaign=send_list&utm_medium=email&utm_source=sendgrid, accessed September 2016
[4] Danielle Correa, “Costs of TalkTalk breach amount to £60m”. *SC Magazine UK*, February 04, 2016, http://www.scmagazineuk.com/costs-of-talktalk-breach-amount-to-60m/article/470968/, accessed September 2016.
[5] “TalkTalk fined £400,000 for theft of customer details”, http://www.bbc.com/news/business-37565367

fraud offences committed by people under 18 years of age had jumped by 26 per cent in the previous two years, and 84 per cent in the previous three years.[6] In a recent survey conducted by an online security company, roughly one in six teenagers in the US, and one in four teenagers in the UK, reported that they had tried some form of Internet 'hacking'. Law enforcement have noted that young people, particularly IT literate boys, are increasingly committing cybercrime offences ranging from money laundering for criminal gangs, to hacking, to use of remote access Trojans (RATs) – that is, malware that can log keystrokes, lift passwords, encrypt files and hold them for ransom, and is used for everything from blackmail to financial fraud.[7]

However, many of these young people are ignorant about the severe custodial sentences that such crimes carry, as well as the possibility of extradition to the US to stand trial in the case of crimes committed against a US company or agency.

This is an international problem which has a considerable cost implication, it is estimated that crimes in cyberspace will cost the global economy $445 billion in 2016;[8] however, it should be noted that such estimates are typically very rough, due to underreporting, different definitions of what cybercrime is, difficulty in assessing damages (e.g. loss of reputation), and so forth. These crimes are growing in terms of scope, sophistication, number and types of attacks, number of victims and economic damage. In September 2016 a multinational internet technology company disclosed a massive hack which had taken place in 2014, in which at least 500 million user accounts were compromised – this hack has been described the biggest data breach in history.[9] Many security and police professionals spend their time analyzing the technical and mechanical aspects of cybercrime, dissecting malware and exploit tools, forensically analyzing code and techniques. However, few actively focus on the social and psychological aspects: who for example is the attacker, what motivates them, and more importantly how and when did this deviant behavior begin? Understanding the behavioral and developmental aspects of cyber-criminality is becoming increasingly important, and underlies the necessity of a shift in focus from sanctions to deterrence and prevention.

This research project was undertaken as there is an urgent need to understand the pathways that lead some young people into cybercrime, in order to develop effective prevention and intervention strategies. Additionally, there is a need to promote alternatives, positive (and legal) ways of channeling

[6] Lia Harris, "Rise in child and teen fraud arrests mainly due to increase of internet-based crimes", *Daily Telegraph*, April 11, 2015, http://www.dailytelegraph.com.au/news/nsw/rise-in-child-and-teen-fraud-arrests-mainly-due-to-increase-of-internetbased-crimes/news-story/fc620acdb8379e30ab46f17493e40475, accessed September 2016.

[7] Over 90 Arrested in Global FBI Crackdown on Blackshades RAT http://www.darkreading.com/over-90-arrested-in-global-fbi-crackdown-on-blackshades-rat/d/d-id/1252912

[8] Harriot Taylor, "An inside look at what's driving the hacking economy". *CNBC*, February 5, 2016, http://www.cnbc.com/2016/02/05/an-inside-look-at-whats-driving-the-hacking-economy.html, accessed September 2016.

[9] Alfred Ng and Laura Hautala, "Yahoo hit in worst hack ever, 500 million accounts swiped" https://www.cnet.com/uk/news/yahoo-500-million-accounts-hacked-data-breach/, accessed September 2016.

young talent toward careers in the tech sector. This White Paper aims to present the findings from a research study which explores young people's pathways into cybercrime. The paper briefly presents the key findings and goes on to highlight the implications of this work for policy, industry and police practice. It is envisaged that the research findings will inform the work of professionals within key infrastructures under threat from particular types of cyber-criminality (i.e. fraud and financial crimes against industry), will contribute to educational awareness in the home, in schools and colleges particularly for vulnerable young people, as well as inform the development of training and best practice for policing across a range of roles and cyber-offences.

Ten semi-structured interviews were conducted with a range of stakeholders, case studies were considered and a rapid evidence assessment[10] of current and recent relevant literature was undertaken.

[10] Rapid evidence assessments https://www.gov.uk/government/collections/rapid-evidence-assessments

2. Defining Cybercrime

Cybercrime, which has also been called “computer crime”, “digital crime”, “Internet crime”, and “high-tech crime”, is commonly understood to include a broad range of criminal activities that use computers, digital devices, and the Internet. Despite almost forty years of incidents, cybercrime still does not have a universally accepted definition in literature. Most authors classify cybercrimes based on the role of technology and criminal modus operandi. We have adapted a general framework and set of definitions[11] [12] [13] to set the context for the current work and will consider and explain cybercrime as:

- *Computer crimes (or “true” cybercrimes), such as hacking, denial of service, and production of malware, in which computer systems and networks are the target of criminal activity;* and
- *Computer related crime, in which computers serve as instruments of otherwise non-digital crime, such as forgery, fraud, sexual abuse of children, or copyright infringement.*

Although other broad categories of cybercrime have been proposed (e.g. computer as a place of crime) as well as different classification approaches (e.g. cybercrime classification based on the level of technological sophistication), they have not been widely adopted. Table A provides a non-exhaustive summary of some key forms of cyber-criminality, with a focus on the language, discourse and understanding of some key forms and actions of contemporary hacking behavior and activities.

Table A: Common definitions of hacking and related cyber-criminality

Cybercrime	Description
Hacking	In the context of cybercrime, hacking is an umbrella term that applies to a variety of human activities that interfere with the proper operation of computer systems and networks. Most legal systems, however, do not use the term *hacking* due to its ambiguity. A list of more specific hacking behaviors is criminalised instead. The U.S. Computer Fraud and Abuse Act defines a number of criminal offenses related to hacking that include: • computer espionage • computer trespassing with the aim to obtain data • computer trespassing that interferes with the intended computer use • damaging a protected computer by various means including malware • threatening to damage a protected computer • trafficking in passwords and other hacking tools.

[11] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (London, UK: Elsevier Inc., Third edition, 2011).

[12] Grainne Kirwan & Andrew Power, *The Psychology of Cybercrime: Concepts and Principles* (IGI Global, 2011).

[13] Alexander Seger, “Cyber Crime and Economic Crime” in M. Edelbacher, P. Kratcoski and M. Theil, eds, *Financial Crimes: A Threat to Global Security* (Boca Raton, FL: CRC Press, 2012).

	The Council of Europe Convention on Cybercrime (2001) similarly defines a list of five offenses related to hacking: • unauthorized access to computer systems and networks • unauthorized interception of transmitted or displayed data • unauthorized data interference, such as data deletion, alteration, suppression, deterioration, etc. • unauthorized hindering of system operation (denial of service) • making or possessing hacking tools, such as malware, remote access exploits, databases of stolen passwords, etc. The key requirement of the above criminal offenses is the absence of authorization and – in some cases – the dishonest intent or attempt to bypass security controls. It is perfectly legal, for example, to attempt hacking into a computer system with proper authorization to test system security. This form of security testing is called **penetration testing**. The term **white hat hacker** applies to individuals that perform authorized hacking for benign purposes. The term **black hat hacker** refers to criminal hackers.
Illegal access	A form of hacking that involves intentional access to a computer system or network without right. In some jurisdictions, it may have to involve bypassing of security mechanisms and/or a dishonest intent.
Illegal interception	A form of hacking that involves intentional, unauthorized interception of non-public transmission of data via computer system or network. In some jurisdictions, it may have to involve bypassing of security mechanisms and/or a dishonest intent.
Data interference	Activities that involve deliberate modification, suppression, or destruction of computer data without right. In addition to hacking this also includes cyber vandalism.
System interference	This includes various forms of denial of service and constitutes any intentional, serious hindering of system operation without right
Malware writing	**Malware** is an acronym for *malicious software.* It is a class of computer programs designed for one or more of the following functions: gaining and maintaining control of a computer without the knowledge or permission of the legitimate operator; collecting, altering, or destroying information stored the victim computer; covertly monitoring activities of the legitimate operator; covertly installing and running new applications. 'Malware-as-a-Service' is one of the services offered in the underground market. Malware specifically designed to covertly gain and maintain control of a computer is called **Remote Access Trojan** or **RAT**. It is usually delivered in the form of a benign document which gains control of the system when the document is opened by the unsuspecting victim. Delivery via e-mail is also a common attack vector.
Botnet operation	Botnet operation is a form of hacking. Botnet is a collection of computers and other Internet enabled devices that have been subverted by the hacker (or a group of hackers) and can be remotely controlled. Botnet is used to perform other cybercrimes, such as collecting information about legitimate owners of the subverted systems, stealing system resources (for bitcoin mining, hosting criminal websites etc.), and running DDoS attacks. The creation and operation of a botnet requires sophisticated malware that is able to infect new computers, control distributed operation of the botnet, and protect the identity of the botnet operator. The resources of many botnets are offered for rent on Darknet marketplaces.
Website defacement	Website defacement is a form of hacking. The end goal of website defacement is the replacement of legitimate website content with different content that usually carries a message of political, religious, or social significance. Depending on the system, website defacement may or may not require full control over the computer system running the web site.
Ransomware attack	Ransomware attack is a form of extortion that uses malware to encrypt documents

	stored on the computer in order to deny the legitimate operator access to important documents. This type of ransomware is referred to as cryptoware. While the most prolific ransomware families currently fall under this category, there are other types of ransomware that do not encrypt data but e.g. block access to a computer, such as police ransomware. Once documents are encrypted, ransomware demands a ransom payment from the victim in order to release the information. The payment is usually done via an anonymous payment mechanism, such as Bitcoin.
Distributed Denial of Service	Distributed denial of service or DDoS attack is a form of hacking designed to make an Internet service unavailable to its intended users. DDoS is performed using multiple compromised systems (usually a botnet) that flood the targeted Internet service with bogus requests to exhaust its processing capacity. In one particular instance, DDoS attacks were combined with ransom requests, threating potential victims to make their web site unavailable if they did not make a ransom payment in Bitcoin.
Computer related forgery	This includes various forms of computer assisted forgery including money and counterfeiting
Computer related fraud	This includes various forms of credit card fraud, money laundering, insider trading, and many other types of white collar crimes utilizing computers and the Internet as an essential component. Both the US Computer Fraud and Abuse Act and the Council of Europe Convention on Cybercrime explicitly criminalize all forms of computer related fraud.
Child Sexual Exploitation and CSAM – Child Sexual Abuse Material/Child indecent image collection and distribution	This includes production, distribution, exportation, importation, as well as deliberate possession of child abuse materials. The U.S. legislation addresses online child pornography in parts of the U.S. Child Pornography Prevention Act of 1996 and PROTECT Act of 2003, while the Council of Europe Convention on Cybercrime (2001) explicitly criminalizes such behaviors as cybercrimes.
Computer assisted copyright infringement	Refers to computer assisted copyright infringement on industrial scale and with significant economic impact. The US legislation addressed criminalization of computer assisted copyright violations in a number of Acts that followed the Internet evolution, notably the Digital Millennium Copyright Act of 1998, and The Section 115 Reform Act of 2006.

Cyberspace exposes young hackers to the risk of experimenting with, and engaging in cybercriminal activity by presenting open, unregulated and uncensored sources that provide information, instructions and tools about code breaking, network intrusion, piracy and phishing procedures. Sources produced by skilled IT professionals are within everyone's grasp, and this research suggests that youth can engage in hacks without having a formal technical education, as simple instructions are readily available on the Internet. Increasingly the "Crime-as-a-Service" model[14] gives everyone, including not so tech-savvy people, access to the tools and services necessary to commit cybercrime.

[14] The Internet Organised Crime Threat Assessment (iOCTA) 2014 https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

2.1 Literature Review: Summary of Key Findings

The literature review involved an exploration of academic and grey literature[15] focusing upon understanding of computer and behavioral sciences and adolescent hacking behavior. The literature was drawn from a range of sources, focusing on work undertaken and policy introduced in the past five years unless the evidence was considered seminal, such as that concerning online disinhibition.[16] The purpose of the review was to consider a range of theoretical frameworks across the behavioral and computer sciences, in bringing together a succinct account of the factors influencing online hackers and exploring their modus operandi. Figure A provides an illustration of the theories and larger frameworks considered.

Four critical areas of understanding are included: criminology; developmental psychology; neurobiology; and the emerging realm of cyberpsychology. Independently, these four vast areas of research cover volumes of literature considering human behavior and activities, inclusive of youth hacking. It is the various components of these schools of research and where they overlap that will be useful to law enforcement and industry in the identification, prevention, intervention and ultimately conviction processes, and in turn the rehabilitation of youth hackers. Whereas theories of criminology may explain deviance and anti-social behavior societally;[17] developmental psychology describes elements of decision making and cognition across the formative years.[18] Neuronal connections and release of various neurotransmitters in the brain may reinforce particular behaviors[19] which are further accommodated through the cyberpsychology constructs of online disinhibition,[20] perceived anonymity and online syndication.[21]

[15] Grey Literature: information that is produced on all levels of government, academia, business and industry in electronic and print formats not controlled by commercial publishing i.e. where publishing is not the primary activity of the producing body

[16] John Suler, "The online disinhibition effect," *Cyberpsychology & Behaviour: The Impact of the Internet, Multimedia and Virtual Reality on Behaviour and Society*, 7 (3) (2004): 321–326.

[17] Majid Yar, "Computer Hacking: Just Another Case of Juvenile Delinquency?" *The Howard Journal of Criminal Justice*, 44 (4), (2005), 387–399.

[18] Michael R. Gottfredson and Travis Hirschi, *A general theory of crime* (Stanford, CA: Stanford University Press, 1990).

[19] Guangheng Dong, Qilin Lu, Hui Zhou and Xuan Zhao, "Impulse inhibition in people with Internet addiction disorder: electrophysiological evidence from a Go/NoGo study," *Neuroscience Letters* 485 (2), (2010): 138–142

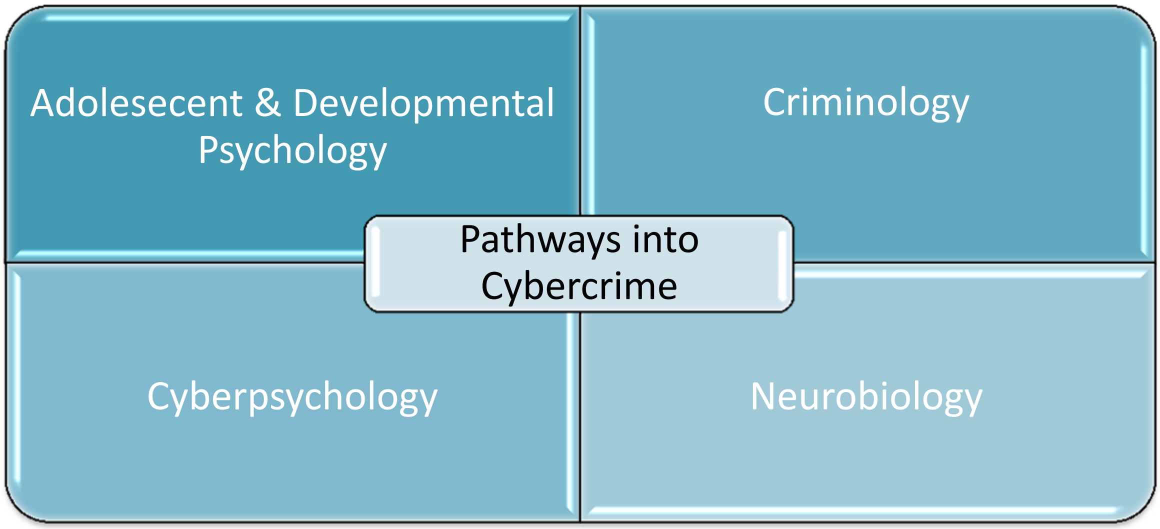
[20] Suler, above, n. 15.

[21] Aiken, *The Cyber Effect* above, n. 1.

Figure A: Distinction and integration of literature in understanding youth hacking

'Storm and Stress'
Personality Theory
Ecological Systems
Moral Development
Social Learning
Theory of Planned Behaviour

Routine Activity Theory
Neutralization
General Deterrence Theory
General Theory of Crime
Theory of Reasoned Action



Online Disinhibition Effect
Anonymity/Invisibility
Minimization of status and authority online
Immersion in cyber contexts
Online syndication

Dopaminergic Reward System
Internet addictive behaviors
Pre-frontal cortex
Impulsivity and ADHD

<u>Criminology</u> – criminological theoretical frameworks view hacking as a criminal act, exploring the 'how', 'who' and 'why' of cybercrime as is the case with other forms of criminal behavior. Seminal theories such as *Routine Activity Theory, General Theory of Crime*, *Theory of Reasoned Action*, *General Deterrence Theory* and *Neutralization* provide a series of critical insights into explaining why adolescents might engage in hacking behavior.

Routine Activity Theory (RAT) explains the three necessary conditions for crime to occur in everyday life: a capable and willing ***offender***, a suitable ***target*** perceived by the offender as vulnerable/attractive, and the ***absence of guardians.***[22] These three factors converge in time and space explaining criminal behavior. Additionally, when considering Routine Activity Theory environmental aspects can be explored in terms of a geographical approach to criminality. Considering cyberspace as an environment and the web as a domain, may have explanatory value, notably NATO now officially recognizes cyberspace a

[22] Lawrence E. Cohen and Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review*, 44 (4) (1979): 588.

warfare domain.[23] [24]. **General Theory of Crime** postulates that ***social bonds*** and ***self-control*** regulates engagement in anti-social behavior and criminality, therefore the ability to forge anti-social bonds along with a lack of regulation in cyberspace may influence youth engagement in acts of online criminality and deviance.[25] The **Theory of Reasoned Action** postulates behavioral ***intentions*** as precursors to acts and the expectation of behaviors leading to specific ***outcomes***; however, it has been established that behavior can alter in cyber contexts in terms of escalation and amplification.[26] **General Deterrence Theory** states that individuals can be dissuaded from committing antisocial acts through the use of countermeasures, which include ***disincentives*** and sanctions.[27] Combined, these latter two theories have emerged in research into hacking where preliminary analysis of action and mapping of potential outcomes as well as perceived norms and the likelihood of punishment were critical in the offender's decision to engage in the anti-social acts.[28] [29] **Neutralization** argues that often offenders will ***deny*** the status of their victim as a 'worthy' victim, that is, not recognizing that they have been harmed or wronged. Alternatively, the offender may convince themselves that the victim 'deserved' what happened to them. This process of neutralization may be strengthened in the mind of the offender given the anonymity afforded by cyberspace.[30] [31]

<u>Adolescent and developmental psychology</u> – this approach assists in understanding the general behaviors and maturation of teenagers, from the ***'storm and stress'*** underpinnings of mood disruptions, impulsivity and problems with authority which can implicitly influence engagement with criminality and anti-social behavior; to ***developing morals*** and the internalization of subjective beliefs, norms, attitudes, and the establishment of identity whilst in a state of role confusion, arguably compounded by differences between real-world norms and moral judgements, and those that prevail online.[32] [33]

Fluctuations in personality and behavior may be influenced through real and virtual features of the developing youths' ***ecological systems***, particularly that of cyberspace; of importance also friends and

[23] Eric Rutger Leukfeldt and Majid Yar, "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis," *Deviant Behaviour* 37 (3) (2016).

[24] NATO Recognizes Cyberspace as New Frontier in Defense http://www.wsj.com/articles/nato-to-recognize-cyberspace-as-new-frontier-in-defense-1465908566

[25] Byongook Moon, John D. McCluskey and Cynthia Perez McCluskey, "A general theory of crime and computer crime: An empirical test," *Journal of Criminal Justice*, 38 (4) (2010): 767–772.

[26] Ryen W. White and Eric Horvitz, "Cyberchondria,"*ACM Transactions on Information Systems* 27 (4) (2009): Article No. 23.

[27] Gottfredson and Hirschi, *A general theory of crime*

[28] Zhengchuan Xu, Qing Hu and Chenghong, Zhang, "Why Computer Talents Become Computer Hackers"? *Communications of the ACM*, *56* (4) (2013): 64-74.

[29] Catherine Marcum, George Higgins, Melissa Ricketts and Scott Wolfe, "Hacking in High School: Cybercrime Perpetration by Juveniles," *Deviant Behaviour,* 35 (7) (2014): 581-591.

[30] Gresham M. Sykes and David Matza, "Techniques of Neutralization: A Theory of Delinquency," *American Sociological Review*, *22* (6) (1957): 664–670.

[31] R. G. Morris, "Computer Hacking and the Techniques of Neutralization: An Empirical Assessment" In T. J. Holt and B. H. Schell, eds, *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (Hershey, PA: IGI-Global Press 2011), pp. 1-17.

[32] Lawrence Kohlberg, *Essays on Moral Development, Vol. I: The Philosophy of Moral Development*. (San Francisco, Ca: Harper & Row, 1981).

[33] Rong-An Shang, Yu-Chen Chen and Pin-Cheng Chen, "Ethical Decisions About Sharing Music Files in the P2P Environment," *Journal of Business Ethics*, *80* (2) (2007): 349–365.

acquaintances, and ***social learning*** in a period of time when decision making can be rash and the desire to fit in and relate to one's peers or network may be overpowering.[34] [35] Elements of 'overlap' between the theories teased from criminology should now begin to clarify why adolescents may be particularly susceptible to engaging in high levels of cyber-criminality.

Neurobiology - or the study of how the brain and its components operate on an anatomical and physiological level, adds biochemical agents and processes to our understanding of engagement in youth hacking. Through the expediency in which reward and punishment occurs in cyberspace, neural connections may be activated in high densities and volumes as we navigate the cyber world.[36] ***Dopamine*** can be released quickly as vulnerable youth achieve frequent and rapid successes online, and if these successes are linked to anti-social acts, such as hacking, they will be reinforced to pursue further ends to obtain their gains: in other words the variable ratio reinforcement schedule of Internet use and abuse, and dopamine/tech use connection.[37] Frameworks of ***addiction*** assist with explaining the difficulties in cessation as well as an escalation in deviancy and targeted victimization: however, the area of Internet addictive behaviors remains under researched and under classified[38]. ***Pre-frontal cortex*** and frontal lobe functionality are intrinsically linked to (poor) decision-making and ***impulsivity***, again making links with the previous topics of criminology and adolescent psychology.[39] [40] As research continues in this area, understanding the influence of earlier use of technology at younger ages and its effect on brain development, including anti-social behavior, is critical in the development of an understanding of pathways into cybercrime and the interactions between the various theories and constructs discussed. Recent research points towards structural features of the brain and associations with conduct disorder, and patterns of behavior defined by issues with authority and poor impulse control.[41] It will be critical to see if the utilization of technology on the developing brain and its synaptic connections influences behavioral conditions, and causes increased susceptibility to engaging in anti-social behavior.

Cyberpsychology - is a relatively new area, which has much to offer in understanding youth hacking and broader anti-social/criminal behavior**.** The ***Online Disinhibition Effect*** illustrates elements of disembodiment, which links back to ***neutralization*** and why individuals may be more prone to acting

[34] Robert G. Morris and George E. Higgins, "Criminological theory in the digital age: The case of social learning theory and digital piracy,"*Journal of Criminal Justice 38* (2010): 470-480.

[35] Urie Bronfenbrenner, *The ecology of human development: Experiments by nature and design*. (Cambridge, MA: Harvard University Press, 1979).

[36] Mattias Brand, Kimberly S. Young and Christian Laier, "Prefrontal control and Internet Addiction Disorder: a theoretical model and review of neuropsychological and neuroimaging findings," *Frontiers in Human Neuroscience*, Volume B, (2014): Art. 375.1.

[37] The Center for Internet and Technology Addiction, http://virtual-addiction.com/about-us/, accessed September 2016.

[38] Nick Nykodym, Sonny Ariss & Katarina Kurtz, "Computer Addiction and Cyber Crime," *Journal of Leadership, Accountability and Ethics,* (2008): 78-85

[39] Chih-Hung Ko et al., "Altered gray matter density and disrupted functional connectivity of the amygdala in adults with Internet gaming disorder. *Progress in Neuro-Psychopharmacology and Biological Psychiatry, 57* (2015): 185-192.

[40] Guangheng Dong et al., above, n. 18

[41] Graeme Fairchild, Nicola Toschi, Kate Sully, Edmund J.S. Sonuga-Barke, Cindy C. Hagan, Stefano Diciotti, Ian M. Goodyer, Andrew J. Calder and Luca Passamonti, "Mapping the structural organization of the brain in conduct disorder: replication of findings in two independent samples", *Journal of Child Psychology and Psychiatry* (2016): 1-83

anti-socially whilst in cyberspace.[42] Integrating ***anonymity/invisibility*** and ***minimization*** whilst being totally ***immersed*** online, the intersection of all the theories and constructs discussed becomes much clearer.[43] [44] [45] Online Syndication is another recent construct that may have explanatory value in terms of youth criminal behavior online. The hypothesis is that earlier anti-social and criminal behavior was somewhat bound or capped by the laws of proximity and domain – now, within a few clicks, psychologically immersed, under the cover of anonymity, fuelled by disinhibition and impulsivity, like-minded cyber juvenile delinquents can find each other, and syndicate online to rationalize, normalize, socialize and facilitate their cyber-criminal behavior.[46] Cyberspace is a medium in which questionable behaviors, with uncertain agents, can allow the testing of boundaries and unregulated influence of potentially harmful or damaging acts, which may seem attractive, with high gains and little consequences for the youth themselves.

This section brings together the research findings on the intersection between psychology, technology and hacking behavior. The emphasis was placed on understanding the hacker within the realm of behaviors influenced through interactions and influences in cyberspace. It should be noted that this is a brief summary and should be considered as a resource that provides theoretical context. A full bibliography can be found in Appendix 2.

[42] Suler, above, n. 15.

[43] Noam Lapidot-Lefler and Azy Barak, "Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition," *Computers in Human Behaviour*, *28* (2) (2012): 434–443.

[44] Julia Schüler and Jeanne Nakamura, "Does Flow Experience Lead to Risk? How and for whom?" *Applied Psychology: Health and Well-Being*, *5* (3) (2013): 311–331.

[45] Mark Slouka: War Of The Worlds: The Assault On Reality http://www.spikemagazine.com/1297war.php

[46] Aiken, *The Cyber Effect* above, n. 1.

3. Key Findings

This section presents key findings from the stakeholder interviews. Two groups of stakeholders were targeted for the collection and analysis of information: those with a behavioral science perspective on adolescent hacking (interviews 1-5); and a group of experts from a computer science and cybersecurity perspective (interviews A-E). Information supporting the findings is referenced below using the number (1-5) and line or letter (A-E) and time code corresponding to the relevant transcript.

3.1 Individual Characteristics:

1. Adolescent (predominantly) **(SHA, 12:21; SHE, 21:58; SHE, 01:16)**
2. High IQ **(SH1, 23-24)**
3. Highly computer literate and highly curious about technology **(SHD, 17:12; SHC, 15:48)**
4. Broad range of social classes **(SH3, 59-64)**
5. May be male, socially isolated but commonly networked with a groups of similar adolescents **(SHA, 12:21; SHE, 01:52)**
6. Some vulnerability, socially awkward and withdrawn

> *'…[adolescent hackers] extremely intelligent young person, probably slightly vulnerable, socially awkward and withdrawn, very keen in understanding how computers work … [they] might have a slight grievance against society if [they've] been down the black hat route; or if [they're] an ethical white hat [they] may just be doing it for the challenge so they can get the experience at something they are good at…'* **(SH1, 23-27)**

7. High need for online affiliation and affirmation **(SHA, 05:03; 01:42; SHE, 03:52)**

3.2 Common Pathway Factors

Key common pathways factors identified by stakeholders are as follows (some verbatim quotes are used for illustration).

1. Interest in and aptitude for technology **(SHC, 15:48; SH1, 24-25)**
2. Willingness to engage in low level illegal internet related activity which often escalates through positive reinforcement by the network **(SHB, 21:57)**
3. Increased criminal activity online markedly different from early minor acts of online deviance **(SHC, 02:22)**
4. Derive intrinsic pleasure from increased challenge associated with higher level online criminality **(SH1, 27-31; SH3, 152-157)**
5. Importance of online reputation with peer network essential and compensates for lack of self-esteem in real world **(SH3, 150-152; SHA, 08:36)**

6. Cyber-misconducts such as digital piracy or copyright violation are often minimized, since the Internet is perceived as a place with no guardians, where law can be easily bypassed with the right skills **(SH1, 238-246)**
7. Online peer network normalises and encourages illegal behavior **(SHA, 07:49; SH2, 229:231; SHC 15:48)**
8. Behavior may become addictive **(SH2, 256-260)**
9. Hierarchies are formed within networks, and moving up the hierarchy is seen as a form of game playing and test of skill:

> *'…sort of an escalating process you are looking for another hit, or a bigger one: you are probably moving closer to addiction, in terms of getting the mood altering experience that you have to keep. [Because] the tolerance increases the scope to get a response…'* **(SH2, 128-135)**

10. Financial gain may not be the goal; goals could include social affiliation, increased online reputation:

> *'…there's a sort of counter-culture, where hacking has a social purpose beyond financial gain…and that involves crime and that's it…a sort of sporting element, with some of them …they are competing with each other, testing each other, they challenge each other and test themselves…'* **(SH2, 8-80)**

11. Building reputation scores online becomes so important that young hackers can invest copious amounts of cognitive and emotive resources:

> *'…building reputation scores, because in the online world reputation scores are really, really important. And building trust; the [youth] get a sense of belonging and achievement by building these reputation scores…'* **(SH3, 150-152)**

3.3 Case Study Examples

The two case studies presented below have been selected as appropriate and congruent with the findings emerging from this research. They are non-exhaustive but of assistance illustrating our definitions and analysis of pathways, engagement and consequences of youth hacking behavior. Please note, names have been changed to protect the identity of these young offenders.

Cybercrime Example 1: Teenage hacking of online forum

A family of economic migrants from Eastern Europe settles in another European country. The family has a teenage son, Luke, who spends a lot of time on the Internet. Luke learns about hacking from the popular media and visits Russian-language hacking forums to get more information. Luke knows that access to online forums is controlled by a combination of username and password. He learns that user login details are stored in a hidden database at the backend of web forums. While most users have limited access to it, the forum administrator has unrestricted access and his username and password is the key to the data about other users.

Luke is thrilled by the challenge of hacking into websites. He starts learning hacking skills by asking questions on forums and experimenting with freely available hacking tools. Luke learns about Hydra, a network logon cracker program that automatically tries username and password combinations from a large list of known usernames and passwords to “lockpick” access to the target website. Hydra frequently succeeds, because users tend to choose simple passwords and reuse them on different websites.

Luke starts using Hydra to hack into web forums. At first he uses a list of usernames and passwords publicly available on the Internet, but once he succeeds in getting administrator access to a forum, he expands his list with the contents of the compromised forum database, which makes Luke more effective at hacking other online forums.

Although Luke's technical skills are not very advanced, the combination of freely available hacking tools, tutorials and advice from other hackers allowed Luke to be an effective hacker for a time. His hacking is eventually discovered by the administrator of a popular online forum and Luke is apprehended by the police.

Cybercrime Example 2: Teenage sextortion using RAT

Jack is a well-mannered boy from a stable family. He attends a prestigious U.S. high school where he attains consistently high grades in math and science. He has an inquisitive mind and quickly develops a deep interest in computing that leads him to some basic understanding of hacking techniques. At the same time, being socially inept, he develops a fantasy of spying on girls via their computers' webcams. By viewing Youtube tutorials Jack learns that this can be achieved easily using the Blackshades remote access trojan.

The Blackshades application has a user-friendly graphical interface designed for hackers with minimal technical knowledge. Once the desired functionality is chosen, Blackshades generates an executable program – the remote access trojan – that needs to be run on the victim's computer to seize control of it. Once the victim's computer is infected, the hacker can access it remotely through Blackshades to run programs, observe the victim through the webcam, and eavesdrop through its microphone. The trojan can be delivered to the victim in many ways including, for example, an email attachment pretending to come from a trusted friend.

Jack manages to install the trojan into the laptop of a female student attending the same school. Through lucky circumstances he is not discovered. Jack enjoys the adrenaline rush of it combined with the ability to fulfill his erotic fantasies. He continues to infect computers of other female students and gradually becomes more confident in his hacking. At some point he contacts one of his victim via email and uses her private pictures to extort sexual favors. The victim contacts the police, who are able to track and arrest Jack based on his electronic communications.

4. Implications

4.1 Implications for Prevention

1. **Decision-making:** Interventions around hacking should focus on the concept of young people's decision-making abilities.

> *'…[we need to show young hackers] the positive, prosocial paths, or prevent them from going down the malicious side, that can [help rehabilitate] and if they then choose to [hack] anyway, then it happens, and we couldn't have done anymore…'*
> **(SH1, 440-442)**

> *'…[need] to develop pathways that we can push people down, they are already started on that illegitimate pathways. What pathways will give them that challenge that will divert them away from the illegitimate side…'* **(SH3, 184-186)**

Assuming that self-challenge is one of the main reasons why young people escalate through hacking-skill hierarchies, offering challenging pathways towards ethical achievement could potentially deter many young IT skilled youth from committing cybercrime. Their specific needs for self-esteem and social affiliations could be satisfied at the same time, diverting them away from online illegality and deviance.

2. Public health approach: Report stakeholders have suggested parallel approaches that speak to youth about the public interest, and a public health approach. A call is made to deal with the advancing threat of cyber-criminality and the related risks to children and youth is made, in a similar manner to applied public health approaches utilized in the past for other dangers:

> *'…technology is so widely used in society today that the kids need to be educated of the dangers…in the same way that they are educated to the dangers of drugs and alcohol…'*
> **(SH1, 139-141)**

Historical educational programs surrounding issues such as substance abuse and smoking may be re-evaluated and applied to the current area of cybercrime, hacking and online risks as could more current educational awareness programs which have focused upon youth Internet safety.

> *'… in schools, the concentration on safer Internet to keep kids safe should also include a message about not being an offender online'* **(SHA, 34:38)**

As a first step, education could spread information to raise awareness and engender a sense of responsibility towards one's own behaviors in cyberspace. Structuring good, peer-based learning systems, and using key players and successful role models may assist with preventing the pursuit of more anti-social means and activities online:

> *'…appropriate role models are really important… young people are in the [penetration] testing industry and we can get them to talk to other young people who are perhaps going down the wrong path…'* **(SH3, 243-246)**

3. Stranger danger: Approaching dangers in cyberspace should not be seen differently from approaching dangers in the real world. Education for children in the past has commonly warned about 'strangers'[47] and their intention, and a similar approach to educational awareness raising could be taken here.

> *'…in the past [all over the world] there was a focus on education in stranger danger, so why can't we have another focus on the dangers of cyberspace and cybersecurity?'*
> **(SH1, 277-279)**

Additionally it may be of interest to look at the results of programs such as Estonia's web constable concept, which is about policing in cyberspace[48]. Finland and other countries have similar programs. Actual police work is carried out online, including prevention, awareness and general cybersecurity-related advice. It may also be interesting to investigate the cultural implications of adopting an online policing approach, that is, country-specific attitudes to cooperation regarding online presence of law enforcement. The recent Europol IOCTA 2016 report points to positive aspects of collaboration "A number of positive changes have been happening within government and law enforcement. Locally and internationally, law enforcement agencies are finding new ways to efficiently collaborate on investigations involving the internet across borders and jurisdictions[49]"

4. Role models: Providing ethical role models can constitute a fundamental step for education and prevention. Young hackers newly involved in cybercrime, could benefit from communicating with 'white hat' hackers working, for example in industries' penetration tests. Using examples of rehabilitated peers may prove useful in helping young people to employ their IT skills in a more positive way:

> *'…one of the vacuums we have in the digital era is role models for people to aspire to and demonstrate competences, success…[important to practice] creating other challenges for those energies…help [youth hackers] find some other successful positions in the future…'*
> **(SH2, 289-297)**

5. Cybersecurity qualifications: Linking cybercrime prevention to education begins with the introduction of cybersecurity competence within the education system, since the school environment should provide a good, first place to build knowledge and awareness around this issue, This educational initiative should not just focus on teacher training in cybersecurity, but should also include training in cyber skills that are necessary for pupils to fully participate in all the advantages of cyberspace.

> *'…working with new extended projects qualifications, an EPQ that is being released. There's going to be a [cybercrime/cybersecurity] module in that, so we are starting to align [strategies] with education and what people are taught at school…'*
> **(SH3, 209-212)**

[47] Maria Murumaa-Mengel, "Drawing the Threat A Study on Perceptions of the Online Pervert among Estonian High School Students", *Young*, *23*(1) (2015): 1-18.
[48] 'Web Constable' Receives 30 Reports Daily http://news.err.ee/v/news/varia/65783300-ede9-492c-866f-86b89c4d63b1/web-constable-receives-30-reports-daily
[49] Europol Internet Organised Crime Threat Assessment (IOCTA) Report https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016

6. Cyber-awareness/safety programmes: Stakeholder strategies to prevent juvenile hacking crimes have centred overwhelmingly on awareness and early education programmes directed at children and vulnerable groups (such as youth on the autistic spectrum). It was suggested that on-going and future cyber-awareness/safety programmes and law enforcement outreach schemes should incorporate hacking awareness and cybercrime deterrent information focusing on consequences of cybercrime for both themselves and victims:

> *'There is a, a shared responsibility to educate our youngsters of the risks - but also that the use of the Internet and technology might be criminal, and deter them from becoming cybercriminals using those tools.'* **(SHC, 30:50)**

7. Developing skillsets: Encouraging youth curiosity and diverting skills into alternative constructive and lawful uses is also imperative. Similar campaigns for senior-school and university-age youth might also be of value:

> *'…trying to reach them at the school, explaining the consequences that these [activities] may have in their future. That, try to promote the curiosity in them and try to, try to open their mind to white hacking…'* **(SHD, 10:06)**

Schoolteachers should receive training to engage with youth appropriately but all sectors of society should participate, to reflect a shared interest in the problem, and to reach as broad an audience as possible. Digital and social media avenues should be utilized, too, to promulgate the message of deterrence, avenues utilized should be the ones that youngsters currently prefer (e.g. traditional social media or web sites may not be the most appropriate channels in terms of reaching a broad audience). 'Gamification' should also be considered as a means of spreading the message.

A visible online law enforcement presence should be instituted where it is not already in place and/or online community policing carried out by youth:

> *'…there should be online police, that there should be young police officers whose fulltime job is to go around forums and chatrooms and expose them, you know, like a cyber beat, and to be contactable and to be a positive influence in these worlds, you know.'*
> **(SHA, 26:13)**

4.2 Implications for Practice

Human factors

1. Online activity: Human factors play a critical role in forming hacking pathways.

> *'…parents do say he/she is not getting into trouble because he/she is upstairs at their computer. But actually…that is the wrong approach to take. Doesn't mean [they are] not getting into trouble…'* **(SH3, 267-269)**

In order to disseminate knowledge about juvenile cybercrime as a real threat, it is important for parents to be aware of their own youth's online activity and risk:

> *'…education becomes difficult because it's not just the kids. You have got to educate the parents. And that is where it becomes hard. We have got them for that time; small amount of time, whereas the parents are seeing them every day…'* **(SH1, 283-286)**

2. **Monitoring and awareness**: Education around these issues should involve children and parents inter-generationally. Parents play a key role in monitoring children's online activities daily in order to protect and teach them about cyber-misconduct and cyber-victimization. However, during the week most youngsters spend time in environments where parents are not present, and arguably this should therefore perhaps be a shared responsibility. Problems arise when parents underestimate the risks of cyberspace or withdraw from IT communication since they may lack the interest or proper skills. These factors can lead to a gap between generations that only education can address.

4.3 Technology-factors

1. Context: An interesting contribution to the current discussion regards the role of technological factors in enabling and providing a context in which youth feel able to hack:

> *'…[the internet] does create a nice environment where people can learn and they feel safe…that's a challenge for [law enforcement], trying to increase the perception of risk…'* **(SH3, 74-75)**

Over the past two decades, the online environment has been perceived as a new frontier for learning, communication, connectivity and exchange. At the same time, perceptions of risk have become blurred and confusing. One of the main challenges for authorities is to increase society's awareness on cybercrime exposure, beyond popular cyber utopianism and uncritical enthusiasm about IT.

2. Enabling factors: Free or black market software, as well as the abuse of user-friendly encryption and anonymising tools and services, such as TOR and crypto currencies, are principal enabling factors to hacking – Darknets on the Deep Web facilitate sourcing and distribution. More rarely do individuals develop their own sophisticated tools to carry out elaborate, large-scale attacks.

> *'…a lot of these tools that you need to do that are available online and can be, you know, you either get them for free or you purchase them for a small amount.'* **(SHB, 3:17)**

> *'I think that's certainly also something that adds to, you know, the broader misuse of these technologies, the fact that it's becoming so 'user-friendly' almost, you know, to use them and commit crime.'* **(SHB, 11:48)**

4.4 Implications for Law enforcement

1. Role of policing: Hacking is a threat for society and law enforcement, and requires that the threat be faced head-on. Once local police begin intervening in cases of youth hacking, their role will be critical as, this is a global problem that requires local solutions.

> *'…local and regional policing [need] the resources to buy in and to be able to have an [appropriate] response…we need to have a local police response where police are happy to talk with young people, to warn them about the consequences of [hacking and cybercrime] and being able to point them in the right [direction] to use their cyber-skills for good…'* **(SH3, 225-231)**

2. Consequences and Supporting Youth: In fact, informing youth about the gravity of cybercrime in terms of consequences and directing them onto the ethical hacking pathways is the first step to encourage them towards using their cyber-skills in a positive way.

> *'…don't think [adolescents see their online behaviorbehavior] as a huge risk factor because there isn't a law enforcement presence online like there is on the street. So young people frequent environments online…where they can learn about cybercrime and cybercrime techniques… '* **(SH3, 69-72)**

Stakeholder respondents suggested that some youth who become involved in hacking are vulnerable, socially isolated and have low self-esteem. It is important that this is recognized in criminal investigations, and that law enforcement employ policy and practice protocols that have been developed for vulnerable youth. In the UK, for example, multi-agency working is seen as the key to the early and effective identification of risk to vulnerable youth, and to preventing those risks from escalating. Ideally these relationships bring about improved information sharing, joint decision making and coordinated action. Multi-agency models - the most common of which is the Multi-Agency Safeguarding Hub (MASH) - aim to improve the safeguarding response to vulnerable children and vulnerable adults through high quality and timely safeguarding action.

The Home Office has collated a national picture of what good multi-agency arrangements look like, including through MASH, co-located assessment or specialist teams. Whilst multi-agency working is critical in protecting children and vulnerable people, all agencies continue to retain their individual duties to identify, protect and support a child (section 11 of the Children Act 2004) or vulnerable person. It is therefore essential that practitioners collaborating during the criminal justice process are made aware of the nature of this particular form of offending and understand associated vulnerabilities.

3. Minimization and status of authority online: As discussed in the literature through the criminological framework of general theory of crime theory, cyberspace can be perceived as a place lacking guardians, where authority is minimized or forgotten.[50] [51] [52] It is important to combat this misconception, and fully inform young people about the online environment, specifically in terms of the legal consequences of

[50] Moon et al., *A general theory of crime and computer crime,* 772.
[51] Suler, *Online disinhibition effect*
[52] Europol, *The Internet Organised Crime Threat Assessment (iOCTA)*, The Hague (2014).

cybercrime. Additionally, they should be made aware of the psychological harm and consequences that certain antisocial behavior online can cause.

4. Cybersecurity supply: Insufficient capacity is one of the main challenges faced by cybersecurity stakeholders. Recruiting and retaining personnel with the necessary knowledge and expertise to reach young people must be a priority.

> *'…because of the fact that the industry usually pays better, it's very hard to maintain good people or retain good people. So I think for us to do our work better, I think, you know, having the people with the right skillset and being able to retain them is a big challenge.'* **(SHB, 35:29)**

5. Protocols and precautions: Technology can be used to free resources for more complex investigations. Legal and other pressure, e.g. through insurers, should be brought to bear on individuals and companies to take cyber precautions; cybersecurity protocols should be mandatory for new software and applications before release to the market.

> *'…in an ideal world, we would also have standards. We would have a framework that would define…for new software that comes along, that…these products need to meet certain standards, that in an ideal world, cybersecurity or online security or security becomes part of the norm…'* **(SHB, 35:29)**

4.5 Policy Implications

The current research is adopting a societal focus on the issue and is critical in highlighting the importance of government led initiatives to ensure system wide change and adaptation.

> *'…producing a Parent Zone website, with the [Department of Education] on cybersecurity…'* **(SH1, 13-14)**

The Department of Education is producing online material to spread information to parents on the theme of cybersecurity. The aim is prevention on simultaneous levels as illustrated in the next paragraphs.

> *'…we have an ambivalent relationship with hacking because if you are successful as a hacker, you may end up working for the NCA or a security firm…'* **(SH2, 177-179)**

Arguably any policy approach should adopt a multi-tier/faceted approach using the most appropriate communication channels, and employing suitable language that reaches young people and gets the message across. This multi-faceted approach should also be based on a public-private-partnership model that includes industry and academia in raising awareness as well as preventing and protecting.

This approach should be combined with competitions such as 'Hackathons' where again industry would be an important partner. Another concept to consider would be gamification, using popular gaming platforms and even games to deliver key messages.

When it comes to educating older generations, 'grass roots' approaches could be considered where younger generations teach older generations, for example the Kyle Academy project in Ayrshire, Scotland, where 1st year students participated in a 12-week cyber security and digital awareness project to bridge the social demographic by teaching basic cybersecurity to parents and grandparents.

4.6 Implications for Parents/caregivers

As discussed in the literature, lack of parental mediation regarding internet use is positively related to children's risky online behavior. On the other hand, family cohesion has been demonstrated to be a protection factor again cyber-criminal involvement. It is notable that IT constantly in progress, may be considered a field causing generations to part in terms of skills and interest. Current data are also considering family-related factors:

> *'…parents just need to understand that there are risks that their children take an interest in cybercrime and by understanding those risks, they can talk to their children about the potential consequences…also taking an interest in the skills they are generating, but encouraging them to use their skills for [good]…'* **(SH3, 252-257)**

Spreading knowledge about hacking among digital immigrants (parents) may prevent cyber-misconduct among digital natives (sons and daughters), reducing inter-generational gap effect.

> *'…a large communication campaign called 'Cyber-Choices', about trying to explain to parents what the risks are for the children getting into cybercrime and what we want is for parents to understand that their children can use their skills for positive…'*
> **(SH3, 176-179)**

Campaigns have been put into practice in order to spread knowledge about the issue among families, but in particular to encourage skilled youths to exploit their talent in IT- related work in general, including ethical hacking pathways.

Parents and children need to be educated as to what constitutes a cybercrime such as hacking, It is clear when a youth breaks a shop window that a crime has been committed; however, exploratory behavior online in the form of hacking can be less clear. Instructional and educational precise definitions should be formulated, along with a clear delivery of how victims are harmed, legal implications, and consequences of the behavior.

5. Recommendations

5.1 Industry Recommendations

It is recommended that Industry:

1. **Facilitate** the development of positive, legal pathways that inspire young people, cultivate and harness their technology skills, possibly through the provision of educational workshops/seminars, internships, youth industry placements and mentoring programmes;

2. **Support** the development of general educational awareness programmes for young people that could be designed on the basis of the detailed data gathered in this study;

3. **Collaborate** with law enforcement and policy makers to ensure that where feasible, the online environment where young people are most likely to encounter other hackers or become involved in criminal activity contains warnings about the illegality of this behavior and the serious consequences of being caught. As previously stated, hackathons and other forms of competition where youngsters receive recognition for their talent should be considered, along with gamification as an important delivery mechanism. Investment is required to develop technology solutions to technology facilitated problem behavior (for example; automatically delivered network warnings at the onset of a cyber-intrusive event) and develop software that can specifically profile juvenile/experimental hacking behavior and issue appropriate warnings;

4. **Champion** - large organisations producing online games, such as Microsoft, should through their social corporate responsibility budgets develop cyber champion programmes to harness the talents of very gifted computer literate youth to highlight and reward positive pathways. These programmes could be based upon competitions at school level and could carry a prestigious award on successful completion.

5.2 Interventions with Young People and Awareness Raising

1. **Awareness raising** to inform all young people and parents about hacking and cybercrime through general awareness raising programmes in schools;

2. **Educate** young people about cyber security, cybercrime and the law - this could include e-learning, micro-learning, gamification and relevant topics in school curricula.

3. **Identify** young people most at risk and work with them to raise awareness about the possible consequences of illegal online behavior;

4. **Development** of a cyber-peer mentoring programme developed and delivered by young people who have been hackers to the most at-risk groups, identified through awareness raising work in collaboration with law enforcement and industry partners;

5. **Ensure** that awareness raising and educational initiatives extend to parents through programmes and campaigns;

6. **Disseminate** - National advertising campaigns (traditional and digital media) should highlight the serious consequences of hacking amongst young people. Online resources should be made available to parents, schoolteachers and youth to educate and inform.

7. **Support**- Practitioners working with vulnerable youth should be trained to enable an understanding of hacking behavior and should be equipped to respond to their specific support needs.

5.3 Policy Recommendations

1. **Impact:** It is essential that governments and government agencies begin to acknowledge and recognise the extent to which vulnerable young people are becoming involved in illegal internet related activity, and the potential impact when discovered that this may have upon the lives of young people and their families;

2. **Policy:** It is imperative that comprehensive policies focused upon deterrence, prevention and rehabilitation are developed that consider potential loss to industry, but that also consider the needs of often vulnerable young perpetrators, and victim protection;

3. **Practice:** This should no longer be viewed as an industry problem but rather as a shared problem with responsibility for prevention and awareness raising resting with many key stakeholders including government agencies, NGOs and charities responsible for the welfare of children and young people, education, law enforcement, social services, industry as well as academia. The responsibility however falls upon governments to ensure that a central platform is provided to facilitate discussion, policy and practice development through organizations such as the UK Council for Child internet Safety, for example, in the UK context. Most countries will have similar organizations;

4. **Justice and the law:** Appropriate training and education for law enforcement and the judiciary is required. It is essential that criminal justice response including law enforcement investigation and sentencing practice is based upon new and emerging empirical research such as that provided here, in the development of policy guiding practice. Practical guidelines are required regarding appropriate interviewing and detention protocols given the potential vulnerability of these young offenders.

5.4 Research Recommendations & Next Steps

1. **Metrics:** It is imperative that technology talented youth are identified at the first possible opportunity in the educational system. Metrics for I.Q, E.Q and C.Q exist, yet there is no early developmental metric to assess technology skills – this research team recommends the urgent development of a Technology Quotient (T.Q) scale with a view to early stage identification of these valuable skillsets, and subsequently nurturing and rewarding them through the educational system;

2. **Theory:** Many psychology and criminology theories have been conceptualized, tested and validated in real world environments – there is therefore an urgent need to empirically re-evaluate these theories in cyber contexts. They may need to be modified, or new theories may need to be conceptualized and tested (for example Routine Activity Theory in cyberspace, and Online Syndication);

3. **Research:** further research is urgently required to explore youth cognitive processes and motivation to engage in hacking. While a considerable amount has been written regarding the motives of hackers,[53] much of this has been theoretical in nature, with relatively little empirical work. Research should be trans-disciplinary incorporating developmental, physiological, affective and sociological aspects of the behavior with a view to understanding and staging evidence-based interventions. (For example, research exploring hacking and internet addictive behaviors, and hacking tested according to Theory of Planned Behavior, which may have predictive value);

4. **Innovation:** There is a need to develop forums to collaborate with industry in terms of developing software and hardware to incorporate appropriate concepts and safeguards 'by design';

5. **Evaluation:** There seems to be an increasing amount of 'good' practice delivered by law enforcement and the education sector in providing youth with cyber-resilience and awareness. However, many of these initiatives occur in relative isolation to each other and have focused upon online safety in the context of abuse and risk, rather than online financial crime and hacking. More communication and knowledge sharing needs to occur to share practice, and evaluations need to be rolled out to measure outcomes and impact at EU-level and internationally;

6. **Training:** Principles of 'Achieving Best Evidence' within criminal justice proceedings must be integrated into work undertaken with regard to adolescent hackers. This will assure appropriate information is gathered in understanding elements of risk and engagement with online anti-social behavior. In turn, the information will inform future prevention and intervention practice, and will provide a range of stakeholders with descriptive, rich and rigorous data and understanding for their own practice as the threat and extent of youth cybercrime evolves. Rank and file law enforcement officers will need additional 'baseline' training across dealing with cyber juvenile delinquents in terms of detection and arrest, along with understanding key principles of cybercrime victimization and offending, including a more detailed perspective and introduction to the role of computers and technology in facilitating hacking and other forms of cybercrime. We must avoid a potential generation of law enforcement officers becoming 'un'-synced with the communities they are meant to protect, engage and support, in real world and in cyber contexts;

7. **Prototype:** There is a clear need to urgently act upon the key findings from this preliminary, ground breaking research. This work was based upon interviews with stakeholders who work closely with young hackers but does not include any interviews with this group; unfortunately it proved very difficult to gain access given the short research time frame. Funding for the second stage of this work will be sought to work proactively with industry and educators and reformed young hackers to develop a prototype educational awareness programme for young people that will be piloted and evaluated in a small number of schools.

[53] Kirwan & Power, *The Psychology of Cybercrime: Concepts and Principles*

Research Team

The research was designed and led by Principal Investigator Adjunct Associate Professor Mary Aiken, Geary Institute for Public Policy, University College Dublin (UCD), and Principal Investigator Professor Julia Davidson, Middlesex University (MDX) and Dr Philipp Amann from the Europol's European Cybercrime Centre (EC3) as an initiative of the EC3 Academic Advisory Network.

The project Team included Dr Jeffrey DeMarco (Project Manager) MDX, Dr Selga Medenieks (Trinity College Dublin) – Research Consultant MDX, and Dr Pavel Gladyshev – Research Consultant UCD, with assistance from Ciaran Haughton – Research Assistant Geary Institute UCD and Giulia Perasso – Research Assistant MDX.

Funding

This research was funded by Paladin Capital Group as part of the *Pro-techno Social* initiative program.

Ethics

This research received ethical approval centrally from Middlesex University. The research subscribed to British Psychological Society and British Society of Criminology guidelines in confidentiality and anonymity. The research also subscribed to Data Protection regulations in line with university and governmental guidelines.

Stakeholders

This research would not have been possible without the participation and input of a multi-disciplinary group of stakeholders. Contributors included:

- Secondary School Principal Teacher of Computer Science
- The Tavistock and Portman NHS Foundation Trust
- The National Crime Agency
- INTERPOL
- Europol

Appendix 1: List of common terms

4Chan	**English-language Internet forum for anonymous posting and discussion of images**
/b/ (Random)	Most popular section of 4Chan, dedicated to be random "imageboard" for nearly all type of content with minimal restrictions. It is infamous as a source of gore and shock media
DDoS (Distributed Denial of Service)	A cyberattack designed to make an Internet service unavailable to it intended users. DDoS is performed using multiple compromised systems on the Internet that flood the targeted service with bogus service requests to exhaust its processing capacity
IP (Internet Protocol)	The fundamental communication mechanism of the Internet that allows multiple computer networks to be seamlessly interconnected into the global computer network via IP "gateways"
IRC (Internet Relay Chat)	An early instant messaging system. It consists of multiple "channels" that can be used for real-time text-based teleconferencing
LOIC (Low Orbit Ion Cannon)	Software application originally developed by Praetox Technologies for network stress testing that became popular as a tool for distributed denial of service attacks
NCA	National Crime Agency, UK
Script kiddie	A computer hacker relying on off-the-shelf exploitation techniques and tools ("scripts") without the deep understanding of how they work. The term "kiddie" refers to the professional immaturity of such hackers rather than their age
SQL (Structured Query Language)	A standard computer language for querying and manipulating contents of electronic databases
TOR (The Onion Routing)	A secure communication technology and an online service designed to conceal identity of its users. It relies on the use of strong encryption and a geographically distributed network of TOR "nodes" operated by volunteers
VPN (Virtual Private Network)	A secure communication service that connects a computer to a remote computer network using encrypted connection over the Internet rather than a dedicated communication link

Appendix 2: Bibliography

Aiken, M. (2016). Not Kidding. *Freud's The Brewery Journal: Cybercrime*, *6*, 49–52. Retrieved from https://issuu.com/freuds8/docs/brewery_final_single_pages/48.

Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2015). A consideration of the social impact of cybercrime: Examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, 1–19.

Ali, R., McAlaney, J., Faily, S., Phalp, K., & Katos, V. (2015). Mitigating circumstances in cybercrime: A position paper. In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference* (pp. 1972-1976).

Alonzo, M., & Aiken, M. (2004). Flaming in electronic communication. *Decision Support Systems*, *36*(3), 205–213. http://doi.org/10.1016/S0167-9236(02)00190-2.

Apler, M. (2014). "Can our kids hack it with computers?": Constructing youth hackers in family computing magazines (1983–1987). *International Journal of Communication 8,* 673–698.

Árpád, I. (2013). A greater involvement of education in fight against cybercrime. *Procedia - Social and Behavioral Sciences*, *83*, 371–377.

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth and Society*, *44*(4), 500-523.

Boyu, G. (2016). Why hackers become crackers – An analysis of conflicts faced by hackers. *Public Administration Research, 5*(1*).*

Buchen, L. (2011). Scientists and autism, when geeks meet. *Nature 479,* 25-27*.* doi:10.1038/479025a.

Caldwell, T. (2011). Ethical hackers: Putting on the white hat. *Network Security*, *2011*(7), 10–13.

Colins, F.O., Bijttebier, P., Broekaert, E., Andershed, H. (2014). Psychopathic-like traits among detained female adolescents: Reliability and validity of the antisocial process screening device and the youth psychopathic traits inventory*. Assessment 2014, 21*(2) 195–209*.*

Conrad, J. (2012). Seeking help: the important role of ethical hackers. *Network Security*, *2012*(8), 5–8.

Csikszentmihalyi, M., & Rathunde, K. (1993). *The measurement of flow in everyday life: Toward a theory of emergent motivation.* Lincoln, NE: University of Nebraska Press.

Del Rey, R., Lazuras, L., Casas, J. A., Barkoukis, V., Ortega Ruiz, R., Tsorbatzoudis, H. (2015). Does empathy predict (cyber) bullying perpetration and how do age, gender, nationality affect this relationship? *Learning and individual differences, 45, 275-281.*

DeMarco, J. V. (2001). It's not just fun and "war games"–juveniles and computer crime', *49*(3), 48–55.

Dong, G., DeVito, E., Du, X., Cui, Z. (2012). Impaired inhibitory control in Internet addiction disorder: A functional magnetic resonance imagining study. *Psychiatry Research: Neuroimaging, 203*(2-3*)*, 153-158.

Dongping, L., Li X., Yanhui W., Zhao L., Zhenzhou, B., Fangfang, W. (2014). School connectedness and problematic internet use in adolescents: A moderated mediation model of deviant peer affiliation and self-control. *Journal of Abnormal Child Psychology, 41*(8), 1231–1242.

Donner, C.M., Marcum, C., Jennings, W.J., Higgins, E., Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior, 34,* 165–172.

Donner, M. (2016). The gender gap and cybercrime: An examination of college students' online offending. *Victims & Offenders: An International Journal of Evidence-based Research, Policy, and Practice, 11*(4)*,* 556-577.

Doug Hyun, H., Bolo, N., Daniels, M.A., Arenella, L., In Kyoon, L., Renshaw, P.F. (2011). Brain activity and desire for internet video game play. Comprehensive Psychiatry, 52(1), 88–95.

Fanti, K. A, Hadjicharalambous, M., Katsimicha, E. (2013). Adolescent callous-unemotional traits mediates the longitudinal association between conduct problems and media violence exposure. *Societies, 3*(3)*,* 298-315.

Feixa, C. (2011). Los hijos en casa: "¿hacker's o hikikomoris?". *Virtualis 2*(3), 5-17.

Fishbein, M. & Ajzen, I. (1975*). Belief, attitude, intention and behavior: an introduction to theory and research.* Reading, MA: Addison-Wesl.

Fötinger, C. S., & Ziegler, W. (2004). *Understanding a hacker's mind – A psychological insight into the hijacking of identities*. Krems an der Donau: RSA Security.

Furnell, S. (2009). Hackers, viruses and malicious software. In Y. Jewkes & M. Yar (Eds.), *Handbook of Internet Crime* (pp. 173–193). New York: Willan Publishing.

Gámez-Guadix, M., Orue, I., Smith P.K, Calvete, E. (2013). Longitudinal and reciprocal relations of cyberbullying with depression, substance use, and problematic internet use among adolescents. *Journal of Adolescent Health, 53*(4)*,* 446-452.

Harvey, I., Bolgan, S., Mosca, D., McLean, C., Rusconi, E. (2016). Systemizers are better code-breakers: Self-reported systemizing predicts code-breaking performance in expert hackers and naïve participants. *Frontiers in Human Neuroscience, 10.*

Herjanto H. (2013). *Decisions to commit digital piracy: the role of emotions and virtues.* Doctoral dissertation. Auckland University of Technology: Auckland, NZ.

Hing Fong, C. (2014). *Understanding adolescents unethical online behaviors: a structural approach* (Unpublished dissertation). University of Hong Kong: Hong Kong.

Ho, L.-H., Lin, Y.-T., & Huang, C.-H. (2012). Influences of online lifestyle on juvenile cybercrime behaviorbehaviors in Taiwan. *Procedia Engineering*, *29*, 2545–2550.

Hogan, J. (2012). *Academic integrity: A study of attitudes and behaviors focused on technology & narcissism* (Unpublished Thesis). University of Arkansas: Fayetteville, Arkansas.

Hollinger, R. C. (1997). *Crime, deviance and the computer*. Brookfield, VT: Darthmouth.

Holt, H., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology*, *6*(1), 891–903.

Hou, H., Jia, S., Hu S., Fan, R., Sun, W., Sun, T., Zhang, H., (2012). Reduced striatal dopamine transporters in people with internet addiction disorder. *Journal of Biomedicine and Biotechnology,* 2012*. doi:10.1155/2012/854524.*

International Telecommunications Union. (2015). ICT Facts and Figures – The world in 2015. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

Jafarkarimi, H. (2015). Individual characteristics and hacking, piracy, online gambling and pornography use among students: A study in Malaysia. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL) 5*(2), 30-34.

Jewkes, Y., & Yar, M. (2013). *Handbook of Internet Crime*. London: Routledge.

Joinson, A. (2001). Self-disclosure in computer-mediated communication : The role of self-awareness and visual anonymity. *European Journal of Social Psychology*, *31*(2), 177–192.

Johnson, F.N. & Dudek, D. (2011). Return of the hacker as hero: Fictions and realities of teenage technological experts*. Children's Literature in Education, 42*(3), 184-195*.* doi:10.1007/s10583-011-9137-0.

Jongwoo, J.K., Eun Hee Park, E., Baskerville, R. L. (2016). A model of emotion and computer abuse. *Information & Management 53*(1), *91–108.*

Juyu Yen, Cheng Fang Yen, Cheng Sheng Chen, Tze Chun Tang, and Chih Hung Ko (2009). The association between adult ADHD symptoms and Internet addiction among college students: The gender difference. *CyberPsychology & Behavior, 12*(2), 187-191. doi:10.1089/cpb.2008.0113.

Kirwan, G., & Power, A. (2013). *Cybercrime: The Psychology of Online Offenders*. Cambridge: Cambridge University Press.

Ko, C.-H., Liu, G.-C., Yen, J.-Y., Chen, C.-Y., Yen, C.-F., & Chen, C.-S. (2013). Brain correlates of craving for online gaming under cue exposure in subjects with Internet gaming addiction and in remitted subjects. *Addiction Biology*, *18*(3), 559–69.

Kyung-shick, C. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), *308–333.*

Lau, W. & Yuen, A. (2014). Internet ethics of adolescents*. Computers and Education, 72,* 378-385.

Li, B., Friston, K. J., Liu, J., Liu, Y., Zhang, G., Cao, F., … Hu, D. (2014). Impaired frontal-basal ganglia connectivity in adolescents with Internet addiction. *Scientific Reports, 4,* 331–345.

Lickiewicz, J. (2013). The perpetrators of computer crimes as a heterogeneous group. *Zagadnien Nauk Sadowych, 93,* 391-403.

Lin, T. C., Tsai, R., Sun P. C. (2011, April). What Drives a Computer Hacking? An Empirical Investigation of the Factors Influencing Individual's Intention for Hacking, International Conference on Management Learning and Business Technology Education. Meiho University. Taiwan.

Marcum, C., Higgins, G., Ricketts, M. L. (2014). Juveniles and cyber stalking in the United States: An analysis of theoretical predictors of patterns of online perpetration*. International Journal of Cyber Criminology, 8*(1)*,* 47-56.

McAfee. (2014). *Net Losses: Estimating the Global Cost of Cybercrime*. Washington DC.

Meng, Y., Deng, W., Wang, H., Guo, W., Li, T. (2014). The prefrontal dysfunction in individuals with Internet gaming disorder: A meta-analysis of functional magnetic resonance imaging studies. Addiction biology, *20*(4), 799–808.

Meyers, C. A., Powers, S. S., & Faissol, D. M. (2009). *Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches*. Lawrence Livermore National Laboratory, *7*.

Mitchell, V., Petrovici, D., Schlegemilc, B., Szoc, I. (2015). The influence of parents versus peers on Generation Y Internet ethical attitudes. *Electronic Commerce Research and Applications, 14*(215), 95-103.

Nevin, A. D. (2015). Cyber-psychopathy: Examining the relationship between dark e-personality and online misconduct (Master of Arts Thesis). *Electronic Thesis and Dissertation Repository.* Paper 2926*.*

Okenyi, P. O., & Owens, T. J. (2007). On the Anatomy of Human Hacking. *Information Systems Security*, *16*(6), 302–314.

Owen, D. K. (2016). *Motivation and demotivation of hackers in the selection of a hacking task a contextual approach* (Doctorate Dissertation). Mc Master University. Hamilton, Ontario.

Pabian, S., De Backer, C., Vandebosch, H. (2015). Dark triad personality traits and adolescent cyber-aggression. *Personality and Individual Differences, 75,* 41–46*.*

Petry, N. M., Rehbein, F., Ko, C. (2015). Brain correlates of craving for online gaming under cue exposure in subjects with Internet gaming addiction and in remitted subjects. *Current Psychiatry Reports*, *17*(9), 72*.*

Phillips, E. (2015*). Empirical Assessment of Lifestyle-Routine Activity and Social Learning Theory on Cybercrime Offending* (Master of Science Thesis). In BSU Master's Theses and Projects. Item 25.

Pinchevski, A., Durham Peters, J. (2015). Autism and new media: Disability between technology and society. *New media & society,* 1–17*.*

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

Rennie, L., & Shore, M. (2007). An Advanced Model of Hacking. *Security Journal*, *20*(4), 236–251.

Reyns, B.W. (2013). Online routines and identity theft victimization further expanding routine activity theory beyond direct-contact offense. Journal of Research in Crime and Delinquency, *50*(2), 216-238*.*

Sasson H., Mesch G. (2014). Parental mediation, peer norms and risky online behavior among adolescents. *Computers in Human Behavior, 33,* 32–38.

Sela-Shayovitz, R., (2012). Gangs and the Web: Gang members' online behavior*. Journal of Contemporary Criminal Justice 28*(4), 389–405.

Shih, F.J., Hsu, C. (2014). *Examining the adolescents of online dishinibition Internet psychological characteristics, social influence, containment theory* (Master Thesis). Department of information management. National Sun Yat Sen University: China.

Small, G. D., Moody, T., Siddarth, P., Bookheimer, S. (2009). Your brain on Google: Patterns of cerebral activation during Internet searching. *The American Journal of Geriatric Psychiatry, 17*(2)*,* 116–12.

Solmaz, M.., Belli, H. Saygili, S. (2011). Letter to the Editor. An adolescent case with Internet addiction and hacking: How are we dealing with this diverse spectrum of disorder? *General Hospital Psychiatry, 33*(4), 15-16*.*

Straub, D. W. & Welke, R. J. (1998) Coping with systems risk: Security planning models for management decision making. *MIS Quarterly,*22(4)*,* 441-469.

Umeog, B., Ojiakor, I. (2014). The Internet Communication and the Moral Degradation of the Nigerian Youth*. International Journal of Computer and Information Technology,* 3(2)*,* 450-463.

Upton Patton, D., Hong, J.S., Ranney, M., Patel, S., Kelley, C., Eschmann, C., Washington, T. (2014). Social media as a vector for youth violence: A review of the literature. *Computers in Human Behavior, 35,* 548–553.

Van der Merwe, P. (2013). Adolescent violence: The risks and benefits of electronic media technology. *Procedia - Social and Behavioral Sciences, 82,* 87 – 93*.*

Van Wilsem, J. (2013). Hacking and harassment - Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice 29*(4)*,* 437-453.

Voiskounsky, A. E., & Smyslova, O. V. (2004). Flow-based model of computer hackers' motivation. *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, *6*(2), 171–80.

Wingrove, T., Korpas, A. L., & Weisz, V. (2011). Why were millions of people not obeying the law? Motivational influences on non-compliance with the law in the case of music piracy. *Psychology, Crime & Law*, *17*(3), 261–276.

Woo, H.J, (2003). *The hacker mentality: Exploring the relationship between psychological variables and hacking activities* (Unpublished Doctoral Dissertation). University of Georgia: USA.

Yang, Z., Wang, J. (2015). Differential effects of social influence sources on self-reported music piracy. *Decision Support Systems, 69,* 70-81.

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal of Criminal Justice*, *44*(4), 387–399.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management*, *24*(4), 281–287.

Zhengchuan, X., Qing, H., Chenghong, Z. (2013). Why computer talents become computer hackers? *Communications of the ACM, 56*(4)*,* 64-74

Appendix 3: Theorized Motives of Hackers from Kirwan and Power ‘Cybercrime: The Psychology of Online Offenders

Table 3.2 Theorized motives of hackers

	Suggested motives
Taylor (1999)	Feelings of addiction Urge of curiosity Boredom with the educational system Enjoyment of feelings of power Peer recognition in the hacking culture Political acts
Kilger (n.d., as cited by Spitzner, 2003); Kilger *et al*. (2004)	Money Ego Entertainment Cause (basic ideology) Entrance to a social group Status
Lafrance (2004) – insider hacking	Economical profit Revenge Personal interest in a specific file External pressure from people or organization outside of the company (such as organized crime or a family member)
Fötinger and Ziegler (2004)	Deep sense of inferiority – power achieved through hacking may increase self-esteem
Schneier (2003)	Not for profit To satisfy intellectual curiosity For the ‘thrill’ To see if they can Reputation Respect Acknowledgement Self-actualization
Bryant and Marshall (2008) – early hackers	To prove themselves against the authorities of the network, with little malicious intent Self-esteem Peer recognition
Bryant and Marshall (2008) – later hackers	Depended on type of hacker For example, cyberterrorists motivated by ideals; professional criminals motivated by profit; internals were disgruntled

Source: Grainne Kirwan & Andrew Power, *Cybercrime: The Psychology of Online Offenders* (Cambridge University Press, 2013).