EUROPEAN

POLICY BRIEF

FP7 RESEARCH PROJECT FOR NEW EUROPEAN CRIMES AND TRUST-BASED POLICY

POLICY BRIEF: CYBERCRIME

Contributors: Maria Yordanova, Dimitar Markov, Todor Galev (CSD), Mike Hough and Gillan Hunter (BBK), Stefano Maffei (UNIPR)

MAY 2015

KEY FINDINGS

- The spread of information technologies has significantly changed the nature of criminality. The Internet offers unlimited transnational opportunities for communication, access to information, and various online markets and services but it can also be a site of unlawful activity and malicious attack. ***Cybercrimes*** **threaten human rights and national and international security yet much of these illicit activities are uncontrolled by existing legislation**.

- Cybercrime evolves as technologies are developed and there is **no commonly agreed definition or classification of cybercrime either in law or stemming from academic research**. The prevalence of cybercrime across the European Union is difficult to estimate as there are no comparable cross-national data about illegal cyber activities. Further, national and European surveys of crime victimisation tend not to examine cybercrime.

- **Public confidence both in cyber-security and in the authorities' ability to effectively control cyberspace remains low**, according to FIDUCIA surveys. A minority of victims of cybercrime report their crime to the police, though anxiety about victimisation is widespread. Of particular concern is the relatively high proportion of respondents who have encountered materials promoting racial hatred or religious extremism.

- People express **most moral condemnation of activities such as sharing child**

pornography and least condemnation of illegal downloading, of music or film for example.

- Political and legislative measures are of limited effect. International effort remains fragmented; there is no consensus even about which cyber activity to criminalise. Cross-national policy coordination and international cooperation is poor.

- There is much potential for self-regulation and the development of public-private partnership to improve internet security and decrease the opportunities for cybecrime.

BACKGROUND

The FIDUCIA research project (New European Crimes and Trust-based Policy) is funded primarily by the European Commission through the Seventh Framework Programme for Research and Development. It aims to shed light on three crimes that have attracted much attention in the last decade as a consequence of developments in technology and increased mobility of populations across Europe: the trafficking of human beings, the trafficking of goods, and cybercrime. In addition, FIDUCIA examines the increasing criminalisation of migrants and ethnic minorities.

The **central idea behind the project is that public trust in justice is important for social regulation as it leads to public acceptance of the legitimacy of institutions and in turn compliance with the law** and cooperation with the legal authorities. While the concepts of trust and legitimacy are highly relevant to responding to "conventional" forms of criminality, they are especially pertinent to our FIDUCIA crimes and form the basis of our recommended policy model - or set of principles - for applying a trust-based policy for control and deterrence.

A focus of this work is the scope for better aligning formal and informal systems of regulation and the extent to which it is possible, or desirable, to infuse criminal justice systems with a normative element, so that people comply with the law less because it is in their self-interest and more because they think it is the right thing to do.

This Policy Brief summarises key findings from the FIDUCIA cybercrime survey, conducted in selected member states, but it also provides an overview of existing data and research on the prevalence of cybercrimes and the public attitudes towards them. The role of current national and European legislation, policies and practical measures are assessed in terms of their deterrent or preventative effects and the potential role for cross-national cooperation and self-regulation to control or prohibit cybercrime are reviewed.

EVIDENCE AND ANALYSIS

Defining cybercrime

The term *cybercrime* covers a variety of illegal activities and while there is no universally accepted definition, these are generally classified in two ways: 1) crimes which involve offences against computer systems and data, including illegal access, interception or

interference with data or data systems and the misuse of devices and; 2) "traditional" crimes that become cybercrimes when they are committed using a computer, such as computer-related forgery or fraud or offences relating to the distribution via the internet of child pornography. Cybercrimes increase as new technologies develop and the consequences of so called traditional or conventional crimes, are amplified by the potential reach of the Internet.

The prevalence of cybercrime

The extent and nature of cybercrime, and in turn the economic losses or social harms to the European Union resulting from these crimes, are **impossible to calculate**, although it can be assumed that they are likely to be increasing. Information about the prevalence of cybercrime across Europe is limited as not all countries collate routine data on all illicit cyber activity nor agree which cyber activities should be prohibited. Of 42 European countries which contributed to the *European Sourcebook of Crime and Criminal Justice Statistics* (2010), only around half could provide arrest (26) or conviction (19) data relating to cybercrime. There are also the usual problems that beset attempts to make cross-country comparisons, including inconsistencies in how a crime is defined or recorded in national statistics. Often **no reference is made to the modus operandi of an offence**, meaning for example, that it is impossible to determine what proportion of recorded fraud offences were committed using the internet. Even accounting for these various issues, recorded crime data provides only a partial picture of actual prevalence.

The results of surveys among the public about their use of the Internet and their confidence in cyber-security, conducted in various EU countries, are brought together in *The Special Eurobarometer 404 on cyber-security* (2013). These findings show that despite country differences in the frequency and type of Internet use (e.g. use of online banking services varies by country) there is a high level of concern about becoming a victim of cybercrime. Such a finding is reiterated in the FIDUCIA cybercrime survey.

The FIDUCIA cybercrime survey

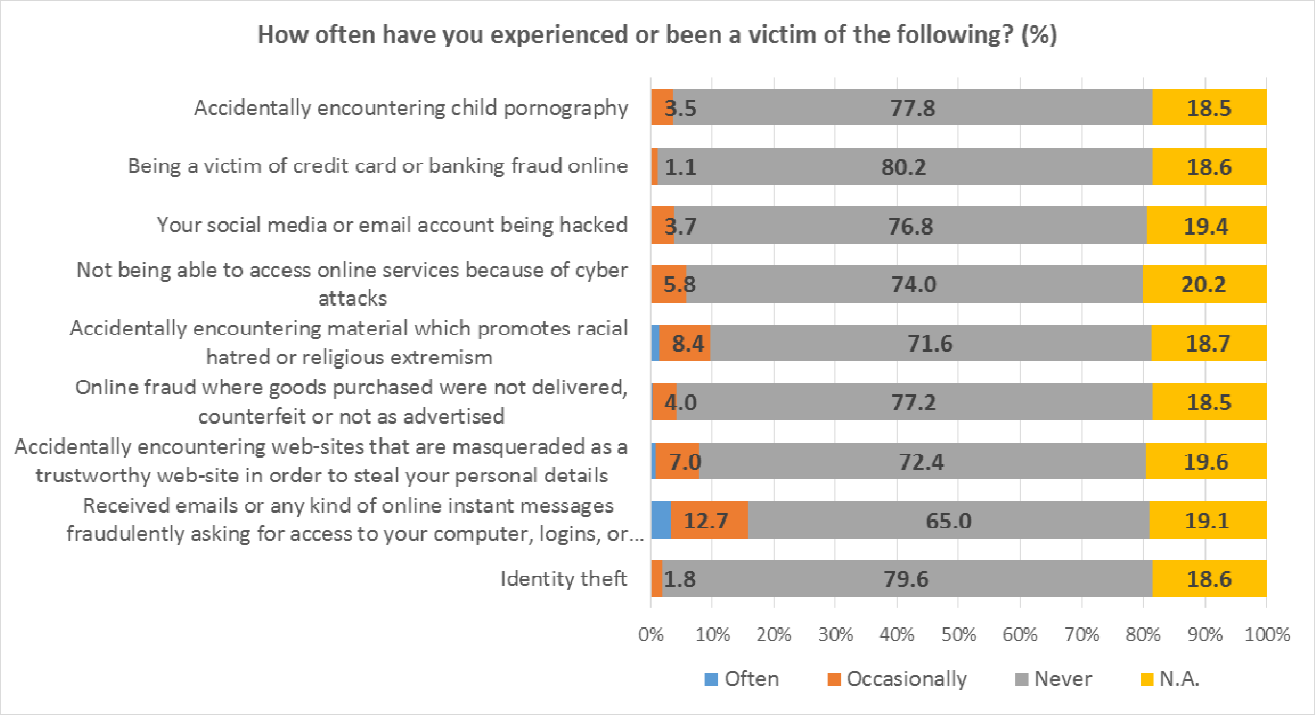
The FIDUCIA survey, available at the time of writing for three Member States (Bulgaria, Finland, and Italy)[1] examined extent and nature of Internet use, experience of cybercrime and confidence in cyber-security. The respondents in Bulgaria, Finland and Italy reported using the internet primarily for e-mail, reading online news and social networking. Online banking was in fifth place, with 24% of respondents reporting having used the internet for this purpose at least once a week in the preceding 12 months, while other online activities requiring payments (e.g. buying goods online or using online administrative services) had been used by less than 2% of respondents during that same time period.

Respondents' reported level of confidence in internet security varied by country. For example, those surveyed in Finland had significantly more confidence in using services requiring online payment than respondents in Italy or Bulgaria, where the proportions expressing confidence was, respectively, one-fifth (Italy) and one-tenth (Bulgaria) of the level reported in Finland. In part this may reflect the greater use and therefore experience of this type of service among Finnish respondents, which was three times higher than in Italy, and 10 times higher than in Bulgaria.

[1] The results from Lithuania, Turkey and the UK were unavailable at the time of the preparation of this Policy Brief.

Similar to survey findings focusing on 'traditional' crimes, the fear of being a victim of cybercrime far out-weighted actual victimisation (see Figure 1 for the victimisation rates reported for different cybercrimes). A third of respondents worried about becoming a victim of cybercrime compared to generally less than 10% who reported that they had been a victim. Only those who reported being a victim of e-mail scamming exceeded 10% – (16%). Despite the higher level of concern about victimisation, only 2.6% of the respondents reported having lost money due to illegal cyber activity in the preceding three years, and in 70% of these cases, the amount had been €50 or less. One significant finding, however, was the relatively high proportion of respondents, when compared to experience of other cybercrimes, who had encountered material promoting racial hatred or religious extremism (10%)[2].

Figure 1: pubic experience of cybercrime



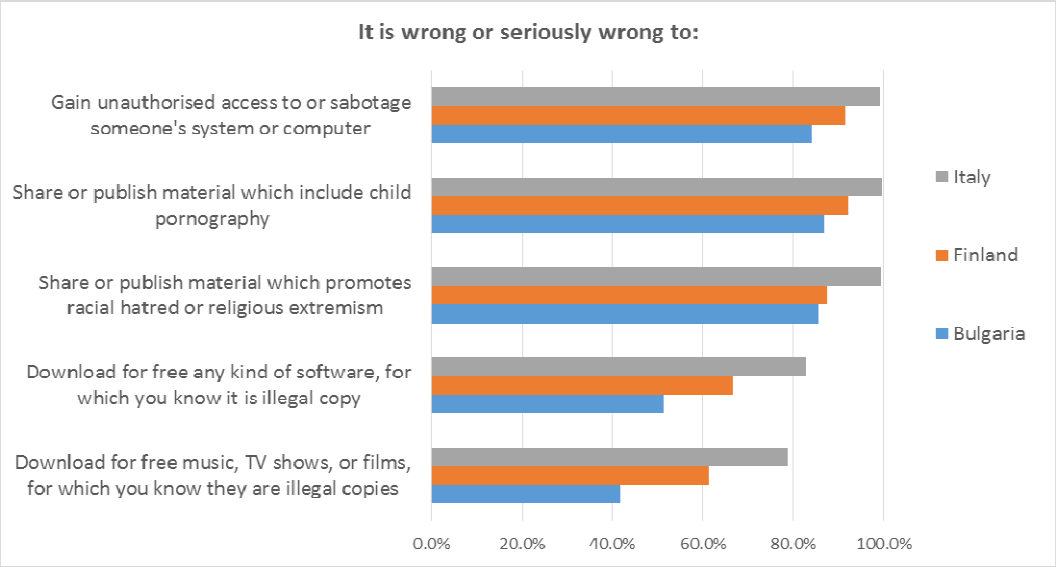
Source: FIDUCIA survey, 2014

Public attitudes to cybercrime

The FIDUCIA survey also examined attitudes towards cybercrimes by asking respondents to **assess how 'wrong' they considered different types of online illegal activity to be** (See *Figure 2*). Respondents in Italy expressed the highest level of moral censure of all types of illegal cyber activity, followed by respondents in Finland, and then in Bulgaria. There was least moral opposition to those activities concerning illegal download or theft or infringement of copyright of music or films and, as might be presumed, most outrage at those activities that violate general moral and ethical values in society, such as sharing child pornography or materials promoting racial hatred and extremism. The latter was assessed as wrong by the majority of the respondents in all three countries.

[2] Combines those who have encountered this 'occasionally' or 'often'.

Figure 2: Public attitudes to cybercrime



Source: FIDUCIA survey, 2014

Regulating cybercrime: instrumental and hybrid strategies

It is clear that legislative and other measures to control activity in cyberspace struggle to keep apace of ever-evolving cyber-activities. However, there are various international, European and national initiatives which attempt to overcome the deficiencies of existing legal regulation and to respond more effectively to problems arising. These comprise efforts to improve cross-national cooperation to control and prosecute illegal cyber activity but also to **encourage countries to share information about emerging cyber-threats and to strengthen national cyber-security**. Of note is the tension between the need for internet security in order to encourage commercial and private use, with protection of the internet as a space for innovation and the free flow of ideas, information and expression.

The *Council of Europe Convention on Cybercrime* (2001, entry into force 1 July 2004) seeks to obtain consensus about how to define cybercrime but also to create the basis for international cooperation to investigate and prosecute cyber-criminals. The *Convention* establishes provisions for mutual legal assistance and extradition procedures within the EU. Defining cybercrime is difficult because there is no consistency among member states as to which cyber activities are proscribed by law. For example, not all states have criminalised trademark violations or racist, homophobic or xenophobic acts committed through computer systems and therefore such acts, where no consensus exists, have been excluded from the Council of Europe Convention.

The *Cybersecurity Strategy of the European Union* (2013) aims to ensure a high level of network and information security (NIS) across the EU, which in turn is hoped to encourage economic growth by improving people's confidence in buying goods and services via the Internet. Member states are encouraged to adopt the NIS strategy and to designate a competent national authority with adequate financial and human resources to prevent and respond to cyber risks and incidents. **This type of EU-wide cooperation also acts as an early warning system among member states.** This work is supported through the *European Network and Information Security Agency* (ENISA) and the *European Cybercrime Centre* (EC3) both of which have management boards, where member states are represented, and offer platforms for coordination of activity at the EU level. Cooperation between the EU and

various international bodies (e.g. the United Nations, the Organization for Economic Cooperation and Development and G8) is also pursued in order to develop and ensure international consistency in policies and practices relating to cyber-threats.

At **the national level,** initiatives have sought to improve coordination and increase expertise in the area of cybercrime. For example, in some member states specific government posts have been introduced to take a national lead on cyber-crime, for example in Germany a Commissioner for International Cyber Policy was appointed in 2013, and national governments have targeted commercial businesses and the state sector, including education, to encourage increasing cyber-security. Other national activities have been aimed at awareness-raising among internet users about cyber-threat. For example, The Police Crime Prevention Program in Germany educates citizens about cyber-attack (e.g. phishing, viruses, trojans, networks and cyber-bullying) and how to prevent these kinds of attack and The Finnish Innovation Fund (Sitra), operating under the Finnish Parliament, aims to create international ground rules for dealing with cyber-attacks, and for improving people's understanding of cyber-security.

The private sector and public-private cooperation

The **private sector has an active role in addressing threats and increasing cyber-security**. Although uptake is voluntary, business and non-governmental organisations are the driving force for initiating non-legislative measures for self-regulation of the Internet via codes of conduct and ethics for good practice. These often include mechanisms for sanctioning inappropriate online behaviour through complaints from other Internet users (an example is the Society of Electronic Communications in Bulgaria) or extrajudicial mechanisms for solving disputes (such as Confianza online in Spain). The private sector also provides financial resources and technical expertise to support law enforcement and national governments to reduce harm from cybercrime; this includes, for example, assisting governments to implement programmes which are more resilient to cyber-attack.

Public and private co-regulation is encouraged by the European Union and through domestic policies. There are various examples of this including from the United Kingdom, *the Certified Professional Scheme (2012)* which was established by the private sector and has created standards to quality assure both information provided via the internet but also professionals working in both government and private networks; and *Guiding Principles on Cyber Security (2013)*, which were co-developed by the government and the internet industry to inform, educate and protect the customers of internet service providers. There are also groupings that encourage cooperation **between the public and private sector to combat illegal activity on the internet**, such as the Virtual Community Police Team in Finland, the National Cyber Security Council in Germany, the Turkish Industry Association, and the Public Council on Safer Internet Use in Bulgaria.

One area of **public/private partnership activity** within the EU involves initiatives to protect children and young people from cyber-threat. These include education and awareness-raising activities, targeted campaigns and events addressing children, teachers and parents as well as general users of Internet and mobile services to promote safe use of the internet and to increase user confidence in cyber-security. For example, web sites, (often part of the international network led by INHOPE), instruct on techniques for self-regulation and programmes to offer protection. Some web sites maintain hotlines for receiving online reports of illegal and harmful content and other cyber-criminal behaviour. Further, the European mobile industry has adopted the European Framework for Safer Mobile Use by Younger

Teenagers and Children and this has been incorporated into national codes of conduct in almost every Member State.

Trust and normative measures to combat cybercrime

Legislation lags behind cyber-activity but even so, the international scope of the Internet – it crosses many jurisdictions - makes legislation difficult to implement or to enforce. In such a context, non-legislative activities, including self-regulation become increasingly important. We
have reported above the role of partnerships between the public and private sectors, especially internet service providers, to develop, agree and adopt high standards of cyber-security and best practices to create a safer internet that is unfavourable to criminality. These kinds of activities can serve to increase the levels of trust between Internet users and the authorities.

Some of the noted approaches have clear trust-based or normative elements. For example, the awareness-raising efforts being made to reduce the vulnerability of some internet users by disseminating information about how to avoid risks but also encouraging the reporting of illegal or inappropriate activity and providing the mechanisms through which these kinds of complaints can be easily made and dealt with. **The FIDUCIA survey results, for example, showed a clear cross-national consensus about which cyber activities were perceived by the public to be immoral.**

Although currently, public-private partnerships are focused mainly on information sharing, these partnerships have encouraged the development and uptake of various non-legislative initiatives and this has helped to engender some consensus concerning best (and worst or inappropriate) practice, which over the longer-term may increase the potential for cross-national legislative and enforcement activity against cybercrime.

POLICY IMPLICATIONS AND RECOMMENDATIONS

Cybercrime is an increasing global threat that requires a global, pre-emptive and dynamic response. The efforts of various international organisations should be integrated through conventions and other international agreements as these provide a strong foundation for cross-national policy and cooperation. Consensus within the European Union as to the scope of activities and behaviours which constitute cybercrime will be necessary to ensure more effective law enforcement; European standards on cybercrime could be based on reasonable but not excessively broad definitions to allow for coverage of new forms of cybercrime as technologies are developed but also to consider approaches other than criminalisation in responding to different forms of wrongful behaviour on the internet.

International public-private partnerships are crucial to promoting and implementing policies against cyber-threat and member states should continue to promote self-regulation amongst businesses and other sectors. Models for self-regulation and non-legislative measures serve as a starting point for further developing trust-based policies.

Recommendations

- **Stronger European and international public-private partnerships are necessary** to promote and implement global and comprehensive policies against cyber-threats. There is also a need to improve cooperation between law enforcement and Internet service providers in order to enhance cybercrime prevention and investigation while respecting the fundamental rights of users.

- EU Member States should address the shortcomings in their justice system/law enforcement to overcome limited implementation of the developed instruments against cybercrime.

- Member States have to improve the **training of cyber experts and members of criminal justice system** as well as to enhance the activities for building their capacity to prevent, detect or/and investigation cybercrime.

- EU Member States need to support **awareness-raising campaigns on safer internet and potential risks targeted the public at large** and particularly specific and most vulnerable groups. They should pay more efforts to promote and protect human rights.

- EU Member States should promote the **self-regulation of businesses**, co-regulations and all relevant private/public partnerships in order to prevent cybercrime. Best models and practices of self-regulations and non-legislative measures could serve as a starting point for developing policies based on trust and persuasive measures.

- EU Member States should promote measures of guaranteeing cybersecurity and building trust in cyberspace. EU policy makers and law enforcement agencies can use the FIDUCIA survey results to design and implement better awareness measures and trust-based policies.

- Development of **trust-based policies at the EU and Member State level in relation to emerging new criminality that provide for**:

  - an appropriate **balance between reasonable restrictions** against abuses in cyberspace, and **overregulation** of cyber offences
  - adequate legislation, non-legislative and awareness measures for prevention of and the fight against cybercrime
  - increasing the awareness of internet users, including youth, regarding how to safeguard themselves and to cooperate better with the authorities in the identification of and sanctions against activities that violate shared moral and ethical values in society (in particular child pornography and the promotion of racial hatred and religious extremism)

ABOUT THE PROJECT

PROJECT NAME	FIDUCIA: New European Crimes and Trust-based Policy
COORDINATOR	Stefano Maffei, Universita Degli di Parma,Italy stefano.maffei@unipr.it
CONSORTIUM	Università degli studi di Parma – UNIPR Parma, Italy Centre for European Policy Studies – CEPS Brussels, Belgium Centre for the Study of Democracy – CSD Sofia, Bulgaria European Public Law Organization – EPLO Athens, Greece The European Institute for Crime Prevention and Control, affiliated with the United Nations – HEUNI Helinki, Finland Birbeck, University of London – BBK London, UK Magyar Tudomanyos Akademia Tarsadalomtudomanyi Kutatóközpont – MTA TK Budapest, Hungary London School of Economics and Political Science – LSE London, UK Max Planck Institute for Foreign and International Criminal Law – MPI–CC Frieburg, Germany Teisės Institutas – TEISE Vilnius, Lithuania The Chancellor, Masters and Scholars of the University of Oxford – Oxford Oxford, UK Ankara Strateji Enstitusu Dernegi – ASI Ankard, Turkey Universidad de Salamanca – USAL Salamanca, Spain
FUNDING SCHEME	European Commission's Seventh Framework Programme – COOPERATION Collaborative project, SSH.2011.3.2-1, Criminal behaviour and policy responses in the European Union
DURATION	February 2012 – May 2015
BUDGET	EU Contribution: €.2.7 million
WEBSITE	www.fiduciaproject.eu

FOR MORE INFORMATION Contact: Maria Yordanova maria.yordanova@online.bg; Todor Galev todor.galev@online.bg

FURTHER READING

FIDUCIA: New European Crimes and Trust-based Policy. Volume 1. Edited by: Stefano Maffei & Lenga Markopoulou
http://www.fiduciaproject.eu/publication/11/publication-of-the-i-year-findings-volume-1

FIDUCIA: New European Crimes and Trust-based Policy. Volume 2. Edited by: Stefano Maffei & Lenga Markopoulou
http://www.fiduciaproject.eu/media/publications/12/FiduciaV2_web.pdf