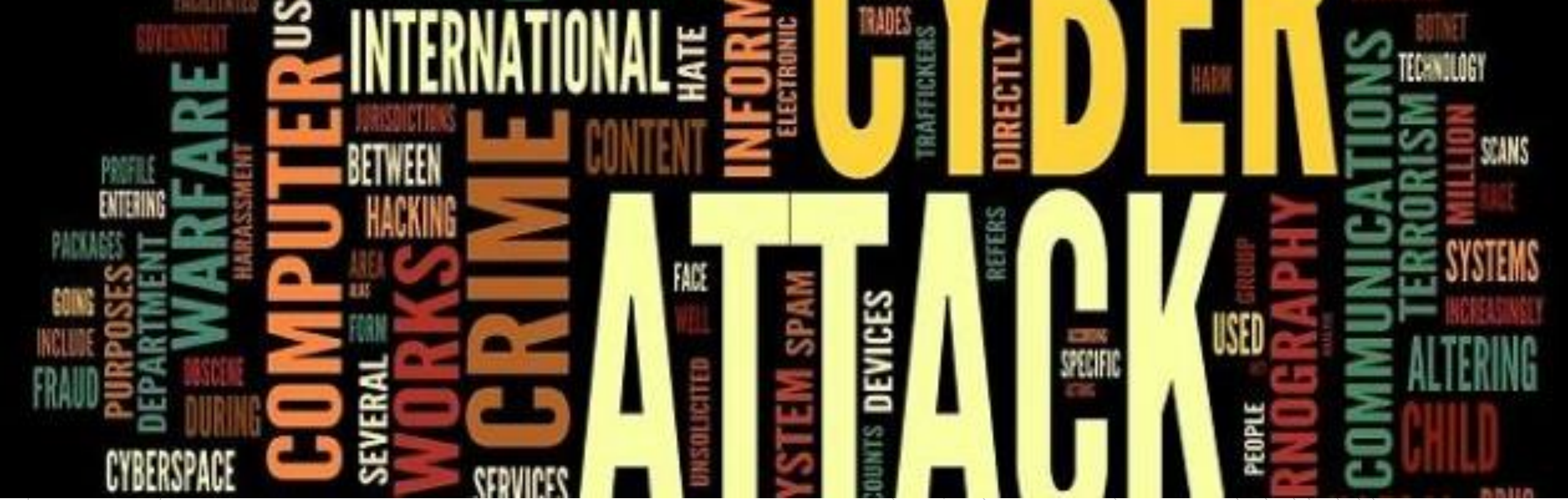


Illegal Cyber Activities

Luka Miletić

Balcan Criminology Course – Inter University Center Dubrovnik 2017

Cyber crime – what does it mean?

- Term that covers a broad scope of criminal activities by means of a computer.
- Referred to the act of performing criminal act using cyberspace as the communication media.
- Appears as a consequence of rapid globalization, low cost of mobile phones and easy access to Internet.

Categories of cybercrimes

- **A) Type I**: a single event from the perspective of the victim.
- **B) Type II**: on-going series of events, involving repeated interactions with the target. For example: computer related frauds, cyber defamation, cyber harassment, child predation, identitiy theft, extortion, travel scam, stock market manipulation, planning or carrying out terrorist activities, insurance frauds, blackamail, credit card frauds, email spoofing, spamming, software piracy etc.

Categories of cybercrimes

- **Cybercrime against:**
  - **1. idividuals** – individual persons are affected. The goal is to exploit human weakness like greed and naivety: cyber porn specially child-pornography, violation of privacy, harassment of a person through e-mail spoofing, hacking, cyber stalking, defamation etc.
  - **2. property** - intellectual property crimes, cyber vandalism, transmission of malware that disrupts functions of the computer system,
  - **3. government, organizations, society** - use of electronic media and the cyberspace to threaten the international governmetns and the citizens of a country - unauthorized access of computer, password sniffing, malware attacks, industrial spying etc.

Categories of cyber criminals

- Depending on the motivation factor the cybercriminals can be classified as under:
  - **1 Type I**: hobby hackers or the politically motivated hackers who are hungry for recognition,
  - **2 Type II**: not hungry for recognition, these include the psychological perverts, financially motivated hackers or organized criminals,
  - **3 Type III**: disgruntled or former employees seeking revenge.

Cybercrime motives

- Pursuing free flow of information:
  - in cyberspace, people who hold the view that the Internet is a public place, and thus everyone has the right of obtaining information, are not rare.
  - Realizing free expression of ego:
    - hackers also have the possibility of hacking for the sake of their ego, for proving a self that is different from the selves of others.
    - Curiosity of seeking new knowledge:
      - many computer and Internet users are motivated to acquire knowledge from the devices, information and new space.

Cybercrime motives

- Testing system security:
  - technical primacy is one of the most important answers to the question “what do hackers hack for?”
- Hacking out of hatred:
  - hatred may come into being for a variety of reasons,
  - Hacking for acquiring financial gains or avoiding payment:
    - embezzlement methods may include information selling without the right to do so, electronic theft of credit-card numbers, emblezzling from employers,

Cybercrime motives

(Not motivated but) influenced by psychological depression,

Sexually motivated misuse

The most frequently prosecuted forms of sexually motivated misuse of information systems are the recording, depositing, transmitting, and trading of child pornography.

Behaviours in cybercrimes – identity theft

- The imposter pretends to be the other person and uses their information without their knowledge to commit theft of fraud – loss of money, but also: loss of credit, reputation, and information that is extremely difficult to restore or fix.
- Perpetrators most generally follow the following three states.
  - **Stage 1. Discovery**: perpetrators gain information and verify information,
  - **Stage 2. Action**: perpetrators accumulate documentation and conceive cover-up or concealment actions,
  - **Stage 3. Trial**

Identity theft

- Trial:
  - **First dimensional actions** – small thefts to test the stolen information,
  - **Second dimensional actions** – larger thefts, often involving personal interaction, without much chance of getting caught,
  - **Third dimensional actions** – largest thefts committed, occurs after perpetrators have confidence that their schemes are working.

- Victims often do not realise they have become victims until they apply for financing, review their accounts, or receive an alert from a financial institution

- Thieves have been known to:
  - 1 steal wallets, purses and backpacks to find out personal information,
  - 2 rummage through garbage to identify personal documents (known as dumpster diving)
  - 3 engage in shoulder sufring i.e. watching a person from a nearby location,
  - 4 steal files or bribe employees to gain access to employee or customer files,
  - 5 record customers credit or debit card information from card readers etc.

Credit card fraud

- An unauthorised use of someone's credit card
  - most credit card frauds can be related to existing account or new account. New account fraud entails the creation of a new credit account using a fraudulent identity and subsequent illegal use.

Credit card fraud

- These are some methods of credit card fraud:
  - **1 skimming** - stealing information off a credit card during a legitimate transaction,
  - **2 counterfeit cards** - occurs when the criminal steals legitimate credit card information, through skimming or other methods, and makes a fake card,
  - **3. phishing** - occurs when a web page is designed to look like a legitimate site where victims enter in personal information such as user names, passwords, and credit card details.

Practical example

- On 22nd of October 2012, V. R. had stolen VISA debit card of R. A. as its owner. At the ATM/cash mashine of Raiffeisen Bank Austria, he used the PIN of the card and took 671,11 € or 5.000,00 kn. He was accused for 2 criminal acts. First for larceny and second for computer fraud. At the first instance he was convicted to 6 months in prison for larceny and 8 months in prison for computer fraud. Total, as a single sentence, he was sentenced to one year in prison, which was replaced with work for common good.
- At the appellate instance he was freed of charge for computer fraud and convicted to 6 month in prison for larceny, which were replaced with work for general good.
- ATM is considered to be a computer because it requires entry of PIN in order to work.

Cybercrime in Croatia

- Criminal code (Official Gazette 125/11, 144/12, 56/15, 61/15)
  - Article 270 (1)
  - Computer Forgery:
  - Whoever, without authorization, develops, installs, alters, deletes or makes unusable computer data or programs that are of significance for legal relations in order for them to be used as authentic, or whoever uses such data or programs shall be punished by imprisonment not exceeding three years.
  - Article 271 (1)
  - Computer Fraud:
  - Whoever, with an aim to procure unlawful pecuniary gain for himself or a third party, installs, alters, deletes, or makes unusable computer data or programs or in some other way alters their use and in such a way causes damage to another person shall be punished by imprisonment for six months to five years

Croatian Bureau of Statistics 2016

CONVICTED ADULT PERPETRATORS BY CRIMINAL OFFENCES IN 2016	
Total	13, 412
Against computer systems, programmes and data	**99**
Unauthorized access, Art. 266, Para. 1	**4**
Unauthorized access, Art. 266, Para. 2	**1**
Obstruction or work of the computer system, Art. 267, Para. 1	**1**
Unauthorized interception of computer data, Art. 269, Para. 1	**2**
Unauthorized interception of computer data, Art. 269, Para. 1, in relation to Art. 273, Para. 1	**1**
Computer forgery, Art. 270, Para. 1	**3**
Computer fraud, Art. 271, Para. 1	**81**
Computer fraud, Art. 271, Para. 2	**5**

Child pornography

- Type of sexual exploitation,
  - any visual depiction of sexually explicit conduct involving a minor (less than 18 years of age) that includes engaging in graphic bestiality, sadistic or masochistic abuse or sexual intercourse.
  - Virtual child pornography - a type of massively multiplayer online game where a virtual world is simulated. These virtual environments have faced moral criticisms to include accusations of child abuse and child pornography in virtual depictions of avatars, some that may appear as minors or have childlike features.

Child pornography

- Child pornography is often traded using electronic forums, newsgroup advertisements, social media, and email spam.
- For example: in the USA it has been reported that public Twitter accounts have been used to share imagery of a young boy being raped.
- Another case involved an individual who used Tumblr to find and share child pornography described by a local district attorney as images of "…children being raped. In this case, the person was caught, found guilty and sentenced to three years in prison. After a local media request, Tumblr made a statement, saying, "Tumblr does not tolerate inappropriate content involving minors, and has taken aggressive efforts to prevent and combat child exploitation.

Child pornography – what makes it difficult for law enforcement to apprehend?

- **1 Photoshop** - can make it difficult to prove whether a digital image is that of an actual child,
- **2 Strong encryption** - Criminals will visit web servers with encrypted proxy services and view and transport illegal pictures and videos via encrypted virtual private networks,
- **3 Peer-to-peer networking** - today, significantly advanced distributive technologies include peer-to-peer networking and cloud computing. Peer-to-peer networking involves the linking of two or more computers in order to share digital files, including music or video.

Practical example

- K. D., in his mid-twenties, got in touch with a less than 15 year old girl convincing her that he is a professional photographer and that he wants to help her to become a model. While they were chatting on Facebook he asked her to send him her erotic pictures and invited her to come to his apartment. He intentionally chose her Facebook profile because he had noticed that she was vulnerable because of her destructive and sad lyrics of english songs she had been posting on Facebook. Moreover, while communicating, he finds out that her mother is in pshyciatric hospital and that she lives with her foster family. He had convinced her and invited her to his apartment where he raped her.
- Eventually, the Supreme Court of Republic of Croatia sentenced him for three criminal acts. He was sentenced for rape to 5 years in prison, 7 months in prison for fraud, and for abuse of children in pornography he was sentenced to 1 year in prison. The single punishment was 6 years and 3 months in prison.

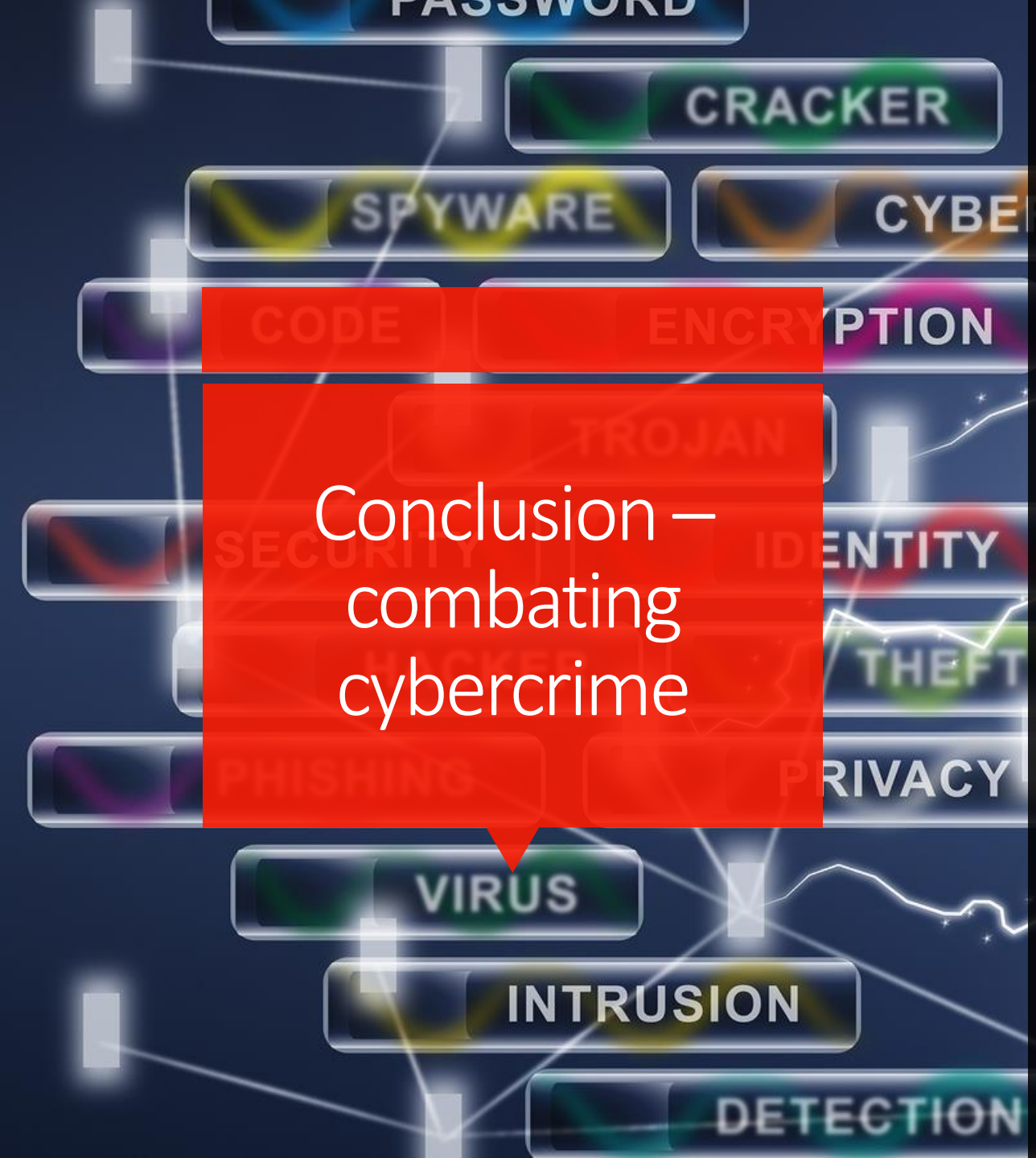
Child pornography in Croatia

Criminal Code (Official Gazette, 125/11, 144/12, 56/15, 61/15)

- Abuse of Children in Pornography
- Article 163
- (1) Whoever panders, recruits or induces a child for the purpose of distribution of child pornography, or whoever organizes or enables its distribution, shall be punished by imprisonment for one to eight years.
- (2) Whoever unauthorized records, produces, offers, presents, shares, imports, obtain for himself or another, sells, gives, distributes or possesses pictures, audiovisual material or other objects of a child pornographic nature, or whoever intentionally take part in child pornography via information and telecommunication technology, shall be punished by imprisonment for one to eight years.
- (3) Whoever, by force or by treat, deception, fraud, abuse of authority or when a person is in a position dependent towards him/her due to harsh material, family, social, health or any other conditions or circumstances, forces or induces a child for the purpose of distribution of child pornography, shall be punished by imprisonment for three to twelve years.

Croatian Bureau of Statistics

CONVICTED ADULT PERPETRATORS BY CRIMINAL OFFENCES IN 2016	
Total	**13,412**
Abuse of children in pornography, Art. 163, Para. 1	**14**
Abuse of children in pornography, Art. 163, Para. 2	**18**
Abuse of children in pornography, Art. 163, Para 3	**1**
Introducing pornography to children, Art. 165, Para 1	**1**



Conclusion – combating cybercrime

- 1 improve security awareness by providing adequate resources to secure transactions and equip system operators and administrators;
- 2 improve coordination and collaboration by enabling systematic exchanges between the private sector and law enforcement including joint operations;
- 3 take steps to ensure that technology does not outpace the ability of law enforcement to investigate cyber-crime;
- 4 broadly criminalise the conduct (including juvenile offenders) and focus on all violators big and small;
- 5 strengthen international initiatives by updating existing treaties and agreements to recognise the existence, threats and transnational nature of high-tech computer-related crimes;
- 6 the development of forensic computing skills by law enforcement and investigative personnel and mechanisms for operational cooperation between law enforcement agencies from different countries,

Croatian Security-Intelligence Agency – Public Report 2017

In 2016 the Agency detected at least 7 state-sponsored cyber attacks on the protected information and communication systems of the state bodies of the Republic of Croatia.

„Globally, the incidence of cyber-security attacks is on the rise. Although most cyber attacks are related to cyber-crime, trends point to the increase in the incidence and severity of cyber attacks on the information systems of critical infrastructure.”

Conclusion

- While the process of "globalisation" continues to accelerate, a fully global response to the problems of security in the digital age has yet to emerge and efforts to secure cyberspace has been reactive rather than proactive.
- Controlling crime involving digital technology and computer networks will also require a variety of new networks: networks between police and other agencies within government, networks between police and private institutions, and networks of police across national borders.

References

- 1 Bhavna Arora, (2016) „Exploring and Analyzing Internet Crimes and Their Behaviours", Perspectives in Science 8, 540-542,
- 2 Xingan Li, (2017) „A Review of Motivations of Illegal Cyber Activities", School of Governance, Law and Society, Tallinn University, Estonia,
- 3 Roderic Broadhurst, (2006) "Developments in the global law enforcement of cyber-crime", Policing: An International Journal of Police Strategies & Management, Vol. 29 Issue: 3, pp.408-433, https:// doi.org/10.1108/13639510610684674 Permanent link to this document: https://doi.org/10.1108/13639510610684674
- 4 Damla Kuru, Sema Bayraktar, (2017) "The effect of cyber-risk insurance to social welfare", Journal of Financial Crime, Vol. 24 Issue: 2, pp.329-346, https://doi.org/10.1108/JFC-05-2016-0035 Permanent link to this document: https://doi.org/10.1108/JFC-05-2016-0035
- 5 Adam Salifu, (2008) "The impact of internet crime on development", Journal of Financial Crime, Vol. 15 Issue: 4, pp.432-443, https://doi.org/10.1108/13590790810907254 Permanent link to this document: https://doi.org/10.1108/13590790810907254
- 6 Chad Albrecht, Conan Albrecht, Shay Tzafrir, (2011) "How to protect and minimize consumer risk to identity theft", Journal of Financial Crime, Vol. 18 Issue: 4, pp.405-414, https://doi.org/10.1108/13590791111173722 Permanent link to this document: https://doi.org/10.1108/13590791111173722
- 7 Norm Archer, (2011) "Consumer identity theft prevention and identity fraud detection behaviours", Journal of Financial Crime, Vol. 19 Issue: 1, pp.20-36, https://doi.org/10.1108/13590791211190704 Permanent link to this document: https://doi.org/10.1108/13590791211190704

References

- 8 Gregory J. Gerard, William Hillison, Carl Pacini, (2005) "Identity theft: the US legal environment and organisations' related responsibilities", Journal of Financial Crime, Vol. 12 Issue: 1, pp.33-43, https://doi.org/10.1108/13590790510625043 Permanent link to this document: https://doi.org/10.1108/13590790510625043
- 9 Katherine J. Barker, Jackie D'Amato, Paul Sheridon, (2008) "Credit card fraud: awareness and prevention", Journal of Financial Crime, Vol. 15 Issue: 4, pp.398-410, https://doi.org/10.1108/13590790810907236 Permanent link to this document: https://doi.org/10.1108/13590790810907236
- 10 Nives Strabić, Ana Tokić Milaković, (2016) „Cyberbullying among children and its comparison to traditional forms of peer violence" Criminology & Social Integration Journal Vol. 24 No. 2, University of Zagreb, Faculty of Law, Department of Social Work
- 11 Public Report of Security-Intelligence Agency of Republic of Croatia (2017)
- 12 Bureau of Statistics of Republic of Croatia, official Internet page, https://www.dzs.hr/default_e.htm (16 October 2017)
- 13 Supreme Court of Republic of Croatia, official Internet page, http://www.vsrh.hr/EasyWeb.asp?pcpid=11 (16 October 2017)

Thank You for Your Attention!