Science Journal of Business and Management
2016; 4(1-1): 29-35
http://www.sciencepublishinggroup.com/j/sjbm
doi: 10.11648/j.sjbm.s.2016040101.15
ISSN: 2331-0626 (Print); ISSN: 2331-0634 (Online)

SciencePG
Science Publishing Group

Ethics in the Age of Cyber Crime and Cyber War

András Keszthelyi

Keleti Faculty of Business and Management, Óbuda University, Budapest, Hungary

Email address:
Keszthelyi.Andras@kgk.uni-obuda.hu

To cite this article:
András Keszthelyi. Ethics in the Age of Cyber Crime and Cyber War. *Science Journal of Business and Management.* Special Issue: Ethical Challenges in the 21st Century. Vol. 4, No.1-1, 2016, pp. 29-35.doi: 10.11648/j.sjbm.s.2016040101.15

Received: November 30, 2015; **Accepted**: December 7, 2015; **Published**: September 3, 2016

Abstract: We have been given new challenges by the “Information Age”. In the virtual world of cyber crime, cyber warfare and Big Brother, where the power of formal law is doubtful, where club law dominates, where we has had not enough time to develop well-established formal and informal rules yet, one of our greatest challenge is to form the new rules for the new world or, better to say, for ourselves. I have been collecting ICT related news for a long time. In this paper I provide a set of problematic fields and questions. These questions should be answered by ourselves, the sooner the better. It depends on us now whether we can form the new world of well-established rules, both written and unwritten, based on eternal human values – or the one in which human values will not play, a world without civilisation and culture. Now it is time to decide what kind of a basis the ethics of this new world will have, or whether it will have any ethics at all.

Keywords: Ethics, ICT Ethics, Computer Ethics, Cybernetics, Paradigm Shift

1. Introduction

“Unwritten rules do exist and those people who sometimes make the written rules a little bit softer must strictly keep them.” (Rejtő)

“We must catch a glimpse of the shadows of technical development, too, from the point of view of the prosperity and development of the human society. (...) Engineers must be responsible for the social impact of their work, too, but they can bear this responsibility only if they can take part even in the management of the production as well.” GézaPattantyús-Ábrahám, famous Hungarian mechanical engineer says. (Legeza, 2013.)

Natural ethical rules (lexmoralisnaturalis) do exist, such as protecting life, for example, and these rules are permanent, do not change and cannot be overridden, not even by so-called democratic votings. In addition to them there are subjective ethical rules created by mankind and these rules can change from time to time. Into this group the codes of ethics of different jobs go.

Computer networks started at the very end of 1969. More than twenty years later the world wide web started. Some time after the millennium the internet changed: from a computer network it became a virtual world of the so-called Z-generation (and of elder generations as well;). A technical tool became an integral part of our everyday life: most of us (or at least most of the younger generation) cannot even imagine their life in a net-free world. The impact of the internet on the society is of so great importance as the steam engine was at the beginning of the industrial revolution. Or perhaps greater. This is a paradigm shift.

Nowadays, because of the spreading of the new technology and its becoming integral part of our everyday life we face with a paradigm shift. Old rules of the traditional (physical, analogue) world do not work any more.

If your car has been stolen, you will recognize it because you cannot find it in its place. This statement is true in the reverse direction, too: If your car is at the place where you left that you will know that is has not been stolen (yet). In the computerized world it is not necessarily true: you log in into your computer, you find all of your data there and it does not mean that your data have not been stolen – perhaps many times. Nor does it mean that your computer is only yours.

You cannot guarantee that your personal computer is yours, not even if you can keep it under continuous physical supervision, even if there are no network interfaces in it. (Sanger, 2014).

Virtual identities can more easily be stolen, so it is harder to believe the identity of your clients in the virtual world than in the physical one, let those “clients” be persons or computers.

If your car has been stolen there is at least one thing you may be sure of: the thief was physically a) on the spot b) in person c) at the moment of the theft. In your computer has been broken into the attacker need not be anywhere at any time for sure.

When a traditional bomb blows up it ruins the surrounding area and itself. A computer virus, or malware in general, can be found, may be analysed, altered and then it can even be sent back to its original senders. (See the different clones of Stuxnet virus.)

In these circumstances we have some problems of theoretical importance. 1. Can you even recognize that your computer has been broken into? 2. If yes, can you identify the attacker? 3. If yes, can you prove it? 4. Can the law protect your data and your virtual world?

In addition: when you copied a music cassette (in a double cassette deck with high speed dubbing;) the quality of the copies was poorer and poorer. Even playing the cassette (or LP) decreased the quality of the analogue data holder. Analogue copying is a slow, quality-reducing, relatively expensive activity. In the digital world all the copies of a book or a song or a movie are of equal quality, the copying process needs nearly zero time and cost. To send the copies to any part of the world also needs nearly zero time and cost.

So the paradigm is changing. The new, so-called virtual, world is coming into existence just now. The new era has brought us a lot of interesting questions and problems we must ask and must find answers for them, not only in particular but in general as well. What are we supposed to do in a lot of new situations? What are the concepts of wrong and right conduct in the new, virtual world?

2. The Beginning of ICT Ethics

The revolutionary new technology, the penetration of the new media, its becoming part of everyday life has caused a lot of social and cultural problems and new questions. As the formal (written) law can only follow the changes with less or rather more delay, ethics becomes more important in these times. Professor Pattantyús was right, his statement cited above is valid even today – and not only for mechanical engineers but IT-people as well.

The birthday of the new era, naturally, cannot be decided unambiguously but if we are forced to select at least a year, probably the round 2000 could be named. The web project started in 1990, eBay in 1995, PayPal and Google in 1998, Facebook in 2004, YouTube in 2005 while the first electronic computer were built under and closely after the second world war.

Ethical questions and problems soon appeared. Probably the first discussion of some ethical problems and rules were the Three Laws of Robotics by Isaac Asimov who published his science fiction short story Runaround in 1942 in Astounding Science Fiction. In this short story the Three Laws of Robotics were introduced:

"A robot may not injure a human being or, through inaction, allow a human being to come to harm.

A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.

A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws." (Asimov, 1950)

As the robots in Asimov's short stories have positronic brains and in very different circumstances they somehow act nearly like human beings, these Three Laws can be considered the first introduction of some ethical or moral problems and questions that may appear in a automated (and computerized) world. Even if these short stories are not scientific publications in the original meaning of the expression.

Then Norbert Wiener, mathematician and philosopher, professor at MIT, was among the first people who drew our attention to the new ethical problems. In his book "The Human Use of Human Beings: Cybernetics and Society" (published in 1950, revised and reprinted in 1954) he wrote about "the task of educating people about possible harms and future benefits that might result from computing and communications technologies." (Hoven – Weckert, 2008). His works in computer ethics were ignored for decades, probably because he did not begin to use new keywords such as "computer ethics" or "information ethics". The common use of these expressions were begun in (or by) the works of Maner.

A little bit later, at the end of the 1970s, Walter Maner proposed to study the different ethical problems caused by the use of computers. By the middle of the 1980s computer ethics became an independent scientific field.

In 1985 Moor's paper "What is computer ethics?" was published. He realized that, after the industrial revolution, a new revolution was going on, a computer revolution. He speaks about the "logical malleability and informational enrichment" of computers, i.e. "Computers are general purpose machines like no others. That is why they are now found in almost every aspect of our lives and that is why a computer revolution is taking place." (Moor, 1998) He also uses the "global village" expression in this paper, at the time of the very dawn of the internet.

After 9/11 ethics becomes more important. "for national intelligence agencies, human rights at times – but particularly post-9/11 – have presented a problem that lay in the way of realizing goals framed in relation to state security and, on such occasions, had to be overcome." (Omand, 2013.).

3. Questions ICT-Ethics Should Answer

While normative ethics describes the moral course of action, applied ethics investigates what people are supposed, should (or prohibited) to do in specific situations. Some of these specialized fields are rather old, such as engineering ethics, while other fields are rather new, ICT-ethics for example. The specialized fields of ethics evolve as life brings newer problems and questions. Especially true this is for the ICT field of ethics, because a new world order always raise a lot of new problems. Some of them follow here.

3.1. Copyright – Music, Movie, Software

As it is described above analogue copying music, movies or even books is (was) a time consuming process that decrease the quality level, too. There were pirated copies in those times, too, sometimes even in a business-like manner, but it was physically limited by the analogue technology. This limitation does not exist in the digital world of computer networks. What is more, everybody has the tools to make and distribute as many copies of an album or individual songs or movies (or anything digital) as they want.

Record labels try to fight against the consequences of the new technology even today but it is important to see that they have not enough tools, technical and legal, for that fight in general. Pirate sites could be identified, found and closed, even their owners could be made pay compensation and could even be sent to jail. Pirate Bay, Megauploadare well-known examples. After p2p (torrent) technology had been invented the situation became more complicated. It is impossible to criminalize a whole society, where everyone can download (and share) any music and movie.

Big companies have the power to provide deterrent examples. See, for example, the filesharing case of Capitol Records v. Thomas-Rasset, in which social worker Jammie Thomas-Rasset was sentenced to one and a half million US dollars for sharing two dozen songs on a p2p network. More details of the case can be found on the homepage of Electronic Frontier Foundation (EFF, 2012).

On the other hand the role of record labels also changes: the new business model in music industry is that bands themselves publish their music for free on their homepages or on YouTube, as a promotion to recruit (more) people to their concerts. Because selling CDs make nearly no profit for bands except the most famous ones.

"... papers using actual file-sharing data, suggest that piracy and music sales are largely unrelated. In contrast, there is clear evidence that income from complements has risen in recent years. For example, concert sales have increased more than music sales have fallen." (Oberhozer-Gee, Strumpf, 2009).

In Hungary a recent research found that about three quarters of the movies that could be accessed via torrent trackers were not available in cinemas at all or only very long time ago. (Bodó, Lakatos, 2010) So, in short, it is simply not true that one downloading equals to one less cinema ticket.

Software is very different from music and movies especially because digital music and movies are new alternatives of ancient, analogue carrier/storage techniques while computer software is not a modern alternative of some older stuff.

The situation with books is similar to movies. There are a lot of books that cannot be bought in hard cover nor in paperback and they will not be printed by the publisher company any more in the future. Should they be lost forever for the newer generations?

It is good, obviously, for the individual person to download music and/or movies. The ethical questions are: Is it good to download and share music/movies for the society? And for the music bands and the film studios? Is it possible that free file-sharing makes greater benefit for the whole society than the possible and theoretical losses of the industry? If software is used to make money, for example an engineer uses AutoCAD, it is obvious that the software should be bought. But what if you want to test it whether it fits for your special purposes? What if a student wants to study how a particular software works?

3.2. Content Filtering

Content filtering or censorship is at least as old as literacy. It has always that way that some people decides what information the others may and/or must not receive. Sometimes it is useful and correct, for example it the duty and responsibility of parents do decide what they children are allowed to read or watch on TV. It is as obvious that there are rules to mark materials broadcasted on TV if they are not supposed to watch by underage children.

The internet brought new challenges in this field, too. It is significantly harder to provide a perfect content filtering on the internet than it was in the world of printed materials. There are not too many printing houses while there are billions of computers connected to the internet and each of them may provide any (kind of) contents.

The typical situations and ethical questions are the following.

Parents decide what contents their children are allowed (and not allowed) to access. It is not the right of the parents but rather their duty to provide the proper circumstances for their children not only in the physical world but in the virtual as well. No public ethical questions, private ones may occur.

At enterprises the management may decide the rules of the internet usage of the employees. In general, employees are supposed to work at their enterprises and on the equipment provided by their firm. It may be checked whether the rules are kept, in general. But what in case of BYOD, when employees "bring your own device" and the official and private use of user devices cannot be delimited?

Elementary and secondary schools are required not only to teach the pupils but to give them intellectual, moral, and social education as well. On one hand the case of students and their schools is something like that of the employees and enterprises. Pupils are required to learn in school, so they are supposed to be under some teacher supervision both in and out of classes. What if the rules of the school are not the same as the rules of the family? Family rules should be of bigger importance but how could a school set and check different set of rules for individual pupils?

The situation in state-financed institutions, such as libraries, universities, etc. is more interesting. Where are the limits of the freedom to reach information? Should the state or the local government finance the accessing of porn sites, The Terrorists' Handbook, etc. or not? Should they make effort to prevent access to unwanted content? Where does censorship begin? What if a team would carry out a research to find information hidden in porn pictures (steganography)?

What about the Great Firewall of China?

Additionally, it it not a simple task to perform a perfect and efficient content filtering in computer networks. A blacklist of domain names or IP addresses could work well but such a blacklist cannot build up easily, there are billions of computers connected to the net... Keyword filtering is also problematic (typical porn abbreviation xxx can be fount in the name of the aic78xxx SCSI driver, the word "babes" appears as part of the name of the Babes-Bolyai University, etc.) Pictures, audio and video materials are more problematic technically, too.

3.3. Freedom of Speech, Anonymity

One can have less or more anonymity in the virtual world. In everyday situations people who use the internet can be identified even post factum, by the help of their internet service provider. Should the ISP give user data to the police? If the police provides a legal warrant? Formally yes, naturally, but what if the law is that of a dictatorship?

If the police, having the appropriate warrant, is to confiscate a server that contains the data of a large number of guiltless users, too, what the ISP as an enterprise and the system administrator as a conscientious person are supposed to do? Is it their responsibility to (try to) prevent such situations?

"Like any technology, anonymity can be used for both good and bad purposes. Many people do not want the things they say online to be connected with their offline identities. They may be concerned about political or economic retribution, harassment or even threats to their lives..." (Chertoff, Simon, 2015) Similar to a knife that can be used by Jack the Ripper and the butcher next to my house.

"Google and Yahoo! have recently attracted much negative publicity - the former for agreeing to censor results in its Chinese search engine, the latter for supplying details to the authorities on two "dissidents" - Li Zhi and Shi Tao - who were subsequently jailed." (Haines, 2006.)

What can one do against the Big Brother? "Emails from the BBC, Reuters, the Guardian, the New York Times, Le Monde, the Sun, NBC and the Washington Post were saved by GCHQ and shared on the agency's intranet." ... The journalists' communications were among 70,000 emails harvested in the space of less than 10 minutes on one day in November 2008 by one of GCHQ's numerous taps on the fibre-optic cables that make up the backbone of the internet. (Ball, 2015)

Sharing an opinion on Facebook (or in other online media) can also be problematic. Should Facebook (or any other provider) apply any kind of content filtering? If yes, what are the rules for that, if objective rules could be set up at all? Should the service provider scan all contents, in real time, should it block suspicious messages immediately? Should the local phone company apply a speech detection software and cut the call down if something, for example, not politically correct content is found? If the filtering ruleset is public, as it should normally be in democratic societies, roundabouts can easily be found... (See 3.2 Content filtering, too.) What rules should be applied when the parties (service provider, content provider, users) are located in different countries?

Should the provider (or is it allowed to) apply even traps? See traps of authorities in 3.5 Online Life and Privacy below.

Where is the border between private conversations and publication? If someone shares their opinion with their friends on Facebook, should that be considered as private? And if the friends of your friends also share that message so it will reach some thousand people? Who may be responsible (and for what)? The original author or those who shared the originally private opinion?

A pastor of a roman-catholic parish in Budapest stated in a private email message that FB blocked his messages containing his not too positive opinion about liberalism.

The other day the headquarters of FB was attacked and a "Facebook Dislike" message was painted on its walls. The motivation of the attacker group is not yet known. Facebook in Germany is said to be cracking down harder on sexual content than on hate-mongering while "Facebook has said it would encourage «counter speech» and step up monitoring of xenophobic commentary." (The Local, 2015)

3.4. Whistleblowing

There are numerous (or countless) examples of how different government agencies do their best to be able to eavesdrop on all electronic communications of not only important leaders of enterprises and states but on all people of the world. See the case of the Hacking Team, a "firm made famous for helping governments spy on their citizens left exposed" (Ragan, 2015) Fin Fisher, Fin Spy software tools of Gamma International also should be mentioned here. Last year Gamma was hacked and a lot of its documentation was published and that drew attention to the spying activities of so-called democratic governments against even their own citizens.

Is it ethical to ruin the privacy of all of the citizens by any government? Is it ethical to publish any information regarding these activities, such as Edward Snowden did it? Is it ethical or not to publish documentation that describe the tortures in Guantanamo carried out by the democratic United States on people who have been kept in prison since 2002 without a sentence? WikiLeaks published the information. Is that publication ethical or not?

"I don't want to live in a world where everything I say, everything I do, everyone I talk to, every expression of creativity and love or friendship is recorded." – "The documents he revealed provided a vital public window into the NSA and its international intelligence partners' secret mass surveillance programs and capabilities. These revelations generated unprecedented attention around the world on privacy intrusions and digital security, leading to a global debate on the issue." (Free Snowden, 2015.).

Whistleblower Edward Snowden used Lavabit's email service to communicate. Lavabit promised a secure service to its users. When the scandal broke out the police, naturally, wanted to get access to Snowden's mailbox. They provided a search warrant to grab all of the company's SSL keys what meant that they would have become able to decrypt the mail traffic of all the nearly half a billion Lavabit users. Instead of the one Edward Snowden.

“Lavabit's CEO, Ladar Levison, compelled to hand over the five SSL private keys, did so in printed form, using a 4-point font spread across 11 pages. Law enforcement were not chuffed. After handing the keys over, Levison promptly shut his 10-year-old business down in August in order to protect customers' data.” (Munson, 2014).

3.5. Online Life and Privacy

The problem of the different accounts of dead people becomes stronger day by day. Facebook, for example, has more than one billion users. Perhaps thousands of registered users die every day leaving a lot of accounts behind. On one hand it is strictly regulated how the movable property and the real assets should be handed over to the heirs. On the other hand the virtual heritage of the dead is not regulated at all. The heirs usually cannot get access to the inherited accounts.

Should service providers handle accounts of dead people the way as the other, physical properties are handled? Can the heirs be given full access to any accounts of the dead? What was the will of the late user? Password protected accounts can be considered something like our thoughts and memories? If someone wants their accounts to be part of the heritage perhaps they ought to write down their login credentials and make it be part of their physical heritage. Good idea but seems to be a bit complicated.

Google introduced its Inactive Account Manager service to solve this kind of problem. After the inactivity of a period of time set by the user Google will send an email to the trusted contact also was set by the user (when they were alive) containing the information about the inactivity and, optionally, about the different types of account data the trusted contact will be given access to.

Should accounts in the virtual world be handled as part of the “normal” heritage and should the heirs be given access to them exactly as to the bank account of the late person, or not? Is Google's solution the better way?

Are traps of authorities ethical? “A man in Australia is believed to be the first to have been convicted as the result of an undercover sting in which charity workers posed online as a 10-year-old Filipina.” (Crawford, 2014) May a boy be arrested if he masturbates on young Olsen twins poster?

What law should be applied if the service provider is an enterprise in one country, the data center is in a second country while the user is the citizen of a third country? “It's been fighting the issue in court since August, when it refused to comply with a warrant for a user's email that was stored in a Dublin data center.” (Vaas, 2014).

“US school students in the state of Illinois may be forced to hand over their Facebook or Twitter passwords if they're suspected of cyberbullying or of otherwise breaking school rules.” (Vaas, 2015) Is it ethical? Who decides and how whether rule breaking did happen at all and who made the rules themselves? May the students be forced to hand over their latch keys, too? Without a search warrant even the police is not allowed to step into someone's house. Isn't Facebook accounts are something like virtual houses?

What if the student says “no”, or “I've forgotten the password”?

Who is, should be or should not be the real owner of data if an enterprise is sold? “In the event that WhatsApp is acquired by or merged with a third party entity, we reserve the right to transfer or assign the information we have collected from our users as part of such merger, acquisition, sale, or other change of control. In the (hopefully) unlikely event of our bankruptcy, insolvency, reorganization, receivership, or assignment for the benefit of creditors, or the application of laws or equitable principles affecting creditors' rights generally, we may not be able to control how your personal information is treated, transferred, or used.” (Whats App, 2012).

“If the ownership or control of all or part of our Services or their assets changes, we may transfer your information to the new owner.” (Face Book, 2015).

Facial recognition has been developed to an unimaginable level of quality and there are cameras everywhere in the streets, millions of photos are stored and not only in Facebook. Facebook's “Deep Face is so accurate that there is barely a difference between its ability to identify a person and that of a real human being. The software's algorithms are able to determine whether two different photographs feature the same person with an accuracy rate of 97.25%, regardless of the angle of the shot or the background lighting conditions.” (Munson, 2015/B) And that Deep Face is a publicly known software. Will (is) it be good if Facebook's photo database could be searched thoroughly with human accuracy, not to speak about other photo databases?

3.6. Technical Field

Governments try their best to have the (not public) possibility to be able to get access to any kind of stored data or data traffic that users think to be confidential. Among these efforts the perhaps the most dangerous is to try to force software developers not to implement strong encryption in their products. In other words: they ought to build in backdoors for the government agencies.

“Securing cyberspace is hard enough without shooting ourselves in the foot with government-mandated vulnerabilities.” (Munson, 2015/A) British prime minister David Cameron is a leader of struggle against strong data encryption in Europe (Vaas, 2015/B) and so is Barack Obama, president of the US. “Furthermore, the Commission will launch in 2015 an EU-level Forum with IT companies to bring them together with law enforcement authorities and civil society. Building upon the preparatory meetings organised in 2014, the Forum will focus on deploying the best tools to counter terrorist propaganda on the internet and in social media. In cooperation with IT companies, th e Forum will also explore the concerns of law enforcement authorities on new encryption technologies.” (European, 2015).

These backdoors might be forced into encryption softwares not only by the force of formal laws but in the background as well.

NSA could manage to insert a special program code into the firmware of about a dozen hard drives by which it could (and can?) get access to any contents stored on the disk. (GReAT, 2015).

As it has been revealed by Snowden, the RSA, Inc. applied a flawed random number generator in its most frequently and widely used cryptographic program library, after NSA had arranged a ten million dollar contract with the RSA, in secret, obviously. (Menn, 2013) This means that the NSA, knowing the vulnerability in the key generation process, can crack all the public key encryptions that uses the random number generator of RSA, i.e. all major applications.

As (Ball, 2013) writes, "The agencies (...) have adopted a battery of methods (...) include covert measures to ensure NSA control over setting of international encryption standards, the use of supercomputers to break encryption with 'brute force', and – the most closely guarded secret of all – collaboration with technology companies and internet service providers themselves."

What might have been (may be, are) included in these "covert measures" we can only guess. The True Crypt free software, the quasi industry standard disk encryption program, stopped last year after it had been providing strong disk encryption for a long time. Its developers shut down the project suddenly on 28 May 2014, stating that it was insecure.

Hackers of NSA and GCHQ, according to secret documents provided to the press by Snowden, could manage to get access to the encryption keys of the largest SIM-card manufacturer Gemalto. Setting up fake cell towers and using the stolen keys the intelligence agencies could (can) intercept a lot of mobile communication. (Scahill, Begley, 2015).

The main question and problem is not that whether it is good that governments have such spying possibilities from their position of force. That is a "normal" question of privacy that arises day by day. A more serious question is: What if the access to the secret governmental backdoors became known for other parties? Try to imagine when the got access to the SSL encryption used in, among others, netbanking.

4. Conclusion

"The rest of us have to grapple with reality – what balance of surveillance and darkness are we prepared to tolerate on the web?" (Stockley, 2015).

After all: in a quickly changing world (see: paradigm shift) the importance and relevance of ethics is significantly higher than in a traditional world where the written and unwritten rules are not only well-known but well-established and, what is more, accepted by the society. This means that the role of education, both formal and informal, is stronger than ever, both in schools (and even at enterprises) and in family.

Formal education is more important in the ICT field because in a new world that changes faster than any other fields in the past we need more knowledge to decide between the must, the possible or acceptable and the unacceptable.

Unfortunately, even basic knowledge in this field seems to be imperfect. The level of of the present-day students' knowledge, at least here in Central Europe, is far from being ideal, as two surveys of Kiss prove that. (Kiss, 2011, 2012a, 2012b).

The subject knowledge in alone is not enough and/or may be obsolete. Training and teaching is an important investment both in the fields of ICT and general ethics. A better strategy is to develop the culture of using ICT, especially its security-related sub-fields. Individual factors influence individual behaviour in relation to organisational safety and security. Good culture means less opportunity for risk behaviour as described in (Lazányi, 2014). Nowadays the most important question is if we can develop a livable world for our children, a world in which important rules do exist for all of us.

References

[1] Ball, J. (2013). Revealed: how US and UK spy agencies defeat internet privacy and security. The Guardian, 06. 09. 2013. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[2] Ball, J. (2015). GCHQ captured emails of journalists from top international media. The Guardian, 19. 01. 2015., http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post.

[3] Bodó, B. - Lakatos Z. (2010) Afilmek online feketepiacaés a moziforgalmazás [Online black market of movies and cinema distribution] In: Szociológiai Szemle 20(3): 34-75. Online (in Hungarian): http://www.szociologia.hu/dynamic/szocszemle_2010_3_all.pdf.

[4] Chertoff, M. – Simon, T. (2015).The Impact of the Dark Web on Internet Governance and Cyber Security. In: Global Commission on Internet Governance, paper series: No. 6., Feb. 2015. https://ourinternet-files.s3.amazonaws.com/publications/GCIG_Paper_No6.pdf.

[5] Crawford, A. (2014). Webcam sex with fake girl Sweetie leads to sentence. BBC News, 21.10.2014., http://www.bbc.com/news/technology-29688996.

[6] EFF (2012).Capitol v. Thomas.Electronic Frontier Foundation, 11. 09. 2012. https://www.eff.org/cases/capitol-v-thomas.

[7] European, C [ommission]. (2015). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – The European Agenda on Security. 28. 04. 2015. http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

[8] Facebook (2015).Data policy. 30. 01. 2015. https://www.facebook.com/privacy/explanation.

[9] Free Snowden – In Support of Edward Snowden, The Courage Foundation, https://www.freesnowden.is/.

[10] GReAT (2015). Equation: The Death Star of Malware Galaxy. Securelist – Kaspersky Lab, 16. 02. 2015. https://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/.

[11] Haines, L. (2006). Google and Yahoo! take a beating. In: The Register, 16. 02. 2006. http://www.theregister.co.uk/Print/2006/02/16/china_committee/ and related materials.

[12] Hoven, J. - Weckert, J. (ed.) (2008). Information Technology and Moral Philosophy.Cambridge University Press, 2008.

[13] Kiss, G. (2011), A Comparison of Informatics Skills by schooltypes in the 9-10th grades in Hungary, in: International Journal of Advanced Research in Computer Science, Volume 2, No. 2, pp. 279-284.

[14] Kiss, G. (2012a), Measuring Computer Science Knowledge Level of Hungarian Students specialized in Informatics with Romanian Students attending a Science Course or a Mathematics-Informatics Course, in: TOJET: The Turkish Online Journal of Education Technology, Volume 11, Issue 4, pp. 222-235. Oct. 2012.

[15] Kiss, G. (2012b), Measuring Hungarian and Slovakian Students' IT Skills and Programming Knowledge, in: Acta Polytechnica Hungarica, Volume 9., No. 6, 2012, ISSN: 1785-8860, pp. 195-210.

[16] Legeza, L. (2013). Mérnökietika [Engineers' ethics], 2nd ed., Budapest.

[17] Menn, J. (2013). Exclusive: Secret contract tied NSA and security industry pioneer. Reuters, Edition U. S., 20. 12. 2013. http://www.reuters.com/article/2013/12/21/us-usa-security-rsa-idUSBRE9BJ1C220131221.

[18] Moor, J. (1998). Reason, Relativity, and Responsibility in Computer Ethics. Computers and Society, March 1998

[19] Munson, L. (2014). Lavabit appeals contempt of court ruling surrounding handover of SSL keys. Naked Security, Award-winning security news from Sophos, 29. 01. 2014. http://nakedsecurity.sophos.com/2014/01/29/lavabit-appeals-contempt-of-court-ruling-surrounding-handover-of-ssl-keys/.

[20] Munson, L. (2015/A). Apple, Google and others urge Obama to say no to backdoors. Naked Security, Award-winning security news from Sophos, 20. 05. 2015. https://nakedsecurity.sophos.com/2015/05/20/apple-google-and-others-urge-obama-to-say-no-to-backdoors/.

[21] Munson, L. (2015/B). Facebook's Deep Face facial recognition technology has human-like accuracy. Naked Security, Award-winning security news from Sophos, 06. 02. 2015. https://nakedsecurity.sophos.com/2015/02/06/facebooks-deepface-facial-recognition-technology-has-human-like-accuracy.

[22] Oberholzer-Gee, F. – Strumpf, K. (2009).File-Sharing and Copyright. NBER's Innovation Policy and the Economy series, volume 10. ed. Joshua Lerner and Scott Stern. MIT Press. 2009. Online: http://www.unc.edu/~cigar/papers/File-Sharing_and_Copyright_2009-05-16.pdf.

[23] Omand, D. (2013). Ethics and Intelligence: A Debate. In: International Journal of Intelligence and Counter Intelligence, Volume 26, Issue 1, 2013 p/pp. 38-63.

[24] Ragan, S. (2015). Hacking Team hacked, attackers claim 400GB in dumped data. CSO Online, 05. 07. 2015. http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html.

[25] Sanger, D.E. (2014).N. S. A. Devises Radio Pathway In to Computers. The New York Times [online], 2014. 01. 14. http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html.

[26] Scahill, J. – Begley, J. (2015). The Great SIM Heist – How Spies Stole the Keys to the Encription Castle. The Intercept, 19.02. 2015. https://firstlook.org/theintercept/2015/02/19/great-sim-heist/.

[27] Stockley, M. (2015). The Dark Web: anarchy, law, freedom and anonymity. Naked Security, Award-winning security news from Sophos, 20. 02. 2015. https://nakedsecurity.sophos.com/2015/02/20/the-dark-web-anarchy-law-freedom-and-anonymity.

[28] The Local (2015). Vandals attack German Facebook headquarters. The Local – Germany's News in English, 13.12.2015. http://www.thelocal.de/20151213/vandals-attack-german-facebook-hq-with-rocks-and-paint

[29] Vaas, L. (2014). Microsoft deluged with support in its email privacy battle against US government. Naked Security, Award-winning security news from Sophos, 17. 12. 2014. https://nakedsecurity.sophos.com/2014/12/17/microsoft-deluged-with-support-in-its-email-privacy-battle-against-us-government/.

[30] Vaas, L. (2015). School rule-breakers to hand over Facebook and Twitter passwords.Naked Security, Award-winning security news from Sophos, 17. 12. 2014. https://nakedsecurity.sophos.com/2015/01/23/school-rule-breakers-to-hand-over-facebook-and-twitter-passwords.

[31] Vaas, L. 2015/B). David Cameron wants to ban encrypted apps like iMessage and Whats app. Naked Security, Award-winning security news from Sophos, 14. 01. 2015. https://nakedsecurity.sophos.com/2015/01/14/david-cameron-wants-to-ban-encrypted-apps-like-imessage-and-whatsapp/.

[32] Whats App (2012). Terms of Service – In the Event of Merger, Sale, or Bankruptcy.07.07.2012. http://www.whatsapp.com/legal/.