RIGHT TO PROPERTY IN CONTEXT OF CYBER CRIMES: CONTEMPORARY DEVELOPMENTS IN US AND UKRAINE

By
Kateryna Krakhmalova

Submitted to
Central European University
Department of Legal Studies

In partial fulfillment of the requirements for the degree of
Master of Laws in Human Rights

Supervisor: Professor Vladimir Pavic

Budapest, Hungary
2008

Apart from purely academic reasons, my inspiration for writing this thesis has been to thank to all those, who made my year in Budapest so Cozy, Exhilarating and Unique – who made it a CEU year:

To my Professors, who challenged me to think,

To my family, who taught me to care,

And, above all,

To my friends, whom I will always remember:

Asel Junusova

Zmicier Koroteyew

Rustam Rasulov

Katka Vargova

Sasha Svitych

Tanya Batanova

Katia Gvozdiova

Munara Omuralieva and

David Zedelashvili

List of Abbreviations

CoC, Convention	Convention on Cybercrimes
CoE	Council of Europe
EU	European Union
FBI	Federal Bureau of Investigations
G8	"The Great Eights" group of countries
OECD	Organization for Economic Cooperation and Development
US	The United States of America

Table of Contents

Introduction

It's hard to find any other topic that with such speed roots in our daily lives, as cyberspace. "Virtual environments" are used in medicine for helping asocial neurological patients with Asperger's syndrome; in politics, where in Second Life are tested electoral technologies; in military virtual training of Iraq campaign; in linguistics for effective language learning within cultural context through a project called Tactical Language; in commerce and entertainment, just to name a few.[1]

Objects, sold in US on-line are worth of $ 100 millions of real dollars revenue, with transactions in-environmental trade worth of 1.5 billion in primary, and over $ 880 million dollars in the secondary market annually.[2]

Now imagine, that cyber criminals in US alone, according to the FBI data, were damages estimated as $239 millions in a year[3], and 97 % of these crimes are never in fact detected.[4]

Would you entrust your money in such uncertain enterprise? How many entrepreneurs are restraining themselves from engaging in such risky business, how many of them do take risks, but suffer huge losses and how many great social projects you perhaps could have financed with that lot of money, which go cyber-stolen?

United States of America is the country with the most hosts in the world, and 13 key servers in the world are controlled by the US Commerce Department, not giving away this

[1] Joshua A.T. Fairfield, *Virtual Property*. 85 B.U.L.Rev. 1047 (2005), pp. 1059-1062

[2] Ibid. p. 1063

[3] FBI 2007 Internet Crime Report, available at http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf, as accessed on 19.11.2008

[4] T.O. Conner, *Cyber crimes: the Internet as a Crime Scene*. Accessed on 22.11.2007 at http://faculty.ncwc.edu/toconnor/315/315lect12.htm , para. 1

privilege even to UN bodies like UN International Telecommunications Union and only letting foreign governments have their own servers.[5] So that's classical example of the cyber monster to discover. Another one is Ukraine – one of the largest European countries with young cyberspace intellectual potential, facing cyber challenges typical for the region.

But this whole work would be apparently useless if I were just to compare and praise cyber regulations of these two countries. Despite the fact, that both countries persistently try to combat cyber crimes, many old solutions simply don't work and new ones can hardly keep up with ever-growing imagination and skills of cyber criminals. Is there any possible way to secure property rights in cyberspace that would make it flourishing and safe place to invest money and effort in, universal enough to be with the same easiness transplanted to both American common law federal and Ukrainian civil law unitarian system?

In order to answer this question, we first of all need to identify what already has been researched on the matter.

This topic emerges on crossroads where intersect informational technology and communications, criminal law, and socio-economic category of property. So in order to research it properly, we need to take a look at it from all three different perspectives and generate complex interdisciplinary vision.

In order to achieve maximum objectivity in understanding of property and property rights, it was very helpful to turn to rather detailed work of G.E. van Maanen and A.J. van der Walt, who edited proceedings of the International Colloquium 'Property Law on the Threshold of the 21st Century, which has taken place in August 1995 in Maastricht,

[5] Ibid. para 6

gathering 26 leading experts in the field.[6]It not only describes origins and theories of property, but also contains comparative study of right to property in different national legal systems, including common law one, international property human rights aspects and levels of protection.

Another work from Netherlands, by Theo R.G. van Banning, called The Human Right to Property, is dissertation, which among other valuable contributions in the area very clearly addresses question, bothering many human right skeptics: why should we talk about such materialistic, associated with wealth and disregard to the needy and the vulnerable, pragmatic topic, in comparison with seen as much noble causes like peace keeping and children rights, as right to property? [7] And not only talk but research ways of protecting it.

After understanding basics of property right, we need to narrow it down, find out where in legal framework it overlaps with informational technology and telecommunications and criminal law.

If regarding the legal literature on property main problem was right choice among indefinite variety of sources, multiplied on century's long history of writings about right to property, which made it relatively settled and uniform, here the challenge is quite opposite. Law on informational technology is my peer, which in its adolescence experiences lack of reliable information, confusion over disagreement of theories and search for authorities, because authority takes years to build. So the best way to cope with this area of research is to consult Internet and journal articles, exercising reasonable judgment about content of Internet ones (because everybody can write them, from

[6]E. van Maanen/ A.E. van der Walt (ed.), *Property Law on the Threshold of the 21st Century* (1996).

[7] Theo R.G. van Banning, *The Human Right to Property* (2002). School of Human Rights Research Series, Volume 14. See p.2-7, 167-218 (Chapter 7).

respected scholar to school boy), and monitoring research of more experienced colleagues, done in their thesises. In this regard I have found particularly helpful article by Joshua A.T. Fairfield in Boston United Law Review about virtual property[8], and Master thesis of CEU student Mirjana Todorovska about intellectual property in the Internet[9], because exactly these types of property are infringed by cyber crimes.

And if to talk about specific aspects of protecting right to property in the cyberspace, it was more than useful to explore internet-banking, which especially suffers from the cyber criminals, through the thesis of another CEU student – Ulla Belovas with her Legal Aspects of Internet Banking[10], and through interactive encyclopedia-like Workbook "Analyzing E-Commerce and Internet Law" prepared by the group of the specialists in the field.[11]

After that when we go in tailoring the topic and filtering relevant literature, it is necessary to say couple of words about cyber crimes, for this thesis is designed to research not all infringements to right to property, but only the ones done by the virtue of cyber crimes. Edward A. Cavazos and Gavino Morin in their book Cyberspace and the law: Your Rights and duties in the On-line-World do outline some[12], as well as place relevant US statutory documents, but this good-quality work has traditional cyber law flaw: it's already out of date. Fresher look on the subject presents Stuart Biegel in his Beyond Our

[8] Ibid.1

[9] Mirjana Todorovska, *Protection of the Intellectual Property on the Internet* (2003).

[10] Ulla Belovas, *Legal Aspects of Internet Banking (*2003).

[11] J.D. Brinson, B. Dara-Abrams, D. Dara-Abrams, J. Masels, R.McDunn, B. White, *Analyzing E-Commerce and Internet Law* (2001).

[12] Edward A. Cavazos, Gavino Morin, *Cyberspace and the Law: Your Rights and Duties in the On-line World* (1994). See Chapter 7.

Control? Confronting the Limits of Our legal System in the Age of Cyberspace;[13] in "human", understandable terms about complexities of cyber-law talks Jonathan Bick in the book 101 Thing You Need to Know About Internet Law.[14]

Unfortunately, the key problem in this field is lack of contemporary clear definitions[15], which in criminal law with its *nullum crimen poena lege* gains crucial significance: new ways of committing old cyber crimes and invention of totally new ones appear so rapidly, that even statutory documents, without even mentioning books, don't have chance to keep up, and as a result major damages to property rights in the Internet go unpunished and unrecovered.

Of course, the matter is not so hopeless, because almost as soon as emerged Internet, started to appear ways of protection property rights against cyber crimes, [16]but obviously, something in the current system of property protection in cyberspace doesn't work, if it can boast only with 3% of all cyber crimes, that are just simply detected.[17] And how many out of this "impressive" number are in fact investigated, punished and remedied?

Therefore flaws in the current system of property protection against cyber crimes are the main concern of this thesis. In identifying advantages and disadvantages in comparative study of Ukrainian and American cyber legal frameworks, as well as supranational systems in which this countries participate, we will through the normative research and empirical findings try to design flexible and dynamic contemporary

[13] Stuart Biegel, *Beyond Our Control? Confronting the Limits of Our legal System in the Age of Cyberspace* (2001).

[14] Jonathan Bick, *101 Things You Need to Know About Internet Law* (2000).

[15] See also Ibid.3

[16] Organization for economic co-operation and development, *10 Computer-related crimes: analysis of Legal Policy.* (1986).

[17] Supra note 3.

legislative response to cyber criminals, endangering one of the most fundamental socio-economical, civil and even political human rights at the same time – right to property.

In order to address the above mentioned issues in the most effective manner, I would discuss right to property in context of cyber crimes in US and Ukraine step by step in two chapters.

The first one will address theoretical aspects of right to property: how it relates to cyber crimes, what is its legal nature and types and why in US and Ukraine we mean different things under the same notion of "right to property". Also this chapter will give brief introductory meeting with the world of cyber crimes.

Second chapter will focus on two levels of normative protection of property in cyber space. Begin with international: UN, OECD, EU and G8 systems an devote special attention to CoE Convention on Cyber Crimes (as not only leading international instrument on the matter, but also fundament of Ukrainian and US Cyber law legislation, because it has been incorporated in both domestic legal systems), and continue with national level.

Concluding part of the thesis will offer author's views on contemporary challenges and perspectives on legal aspects of property in context of cyber crimes.

Chapter I – Right to property in cyber space: theoretical overview

A. Where does right to property fit within the cyber crimes?

From the first glance connection between the right to property and cyber crimes may appear quite remote and superficial. However, if to deepen into the legal theory, it turns out to be direct, coherent and even uniform in terms of various schools of legal thought, who by majority agree on the matter[18]. Let us take a closer look at logical braird of law and situate topic on the field.

Cyber crimes in terms of structure are exactly the same as all other types of crimes.

Dangerous for society, guilty deed, named in criminal law, committed by delictocapable[19] physical person of defined age[20] in order to be qualified as a crime, has to consist of four elements: subject, subjective side, objective side, object.

The object of crime is in the most correct way defined as certain societal relations, which infringe particular group of crimes. [21]

[18] Here I am referring to Ukrainian schools of legal thought. Presented below structure with slight variations is the same in every single book on theory of criminal law – in Bazhanov M.I., Stashys V.V., Tatsij V.Ya., *Criminal Law of Ukraine* (2005),Maryshevs'kyj P.S., Andrushko P.P., Shapchenko S.D., *Criminal Law of Ukraine* (2000), Mel'nyk M.I., Klymenko V.A., *Criminal Law of Ukraine* (2004) to name a few, so I consider it to be common knowledge and do not give in list of references.

[19] Capable of being held responsible for wrongful deed – that is mentally sound, conscious of own action.

[20] See Art. 11, 18 of the Criminal Code of Ukraine adopted on 05.04.2001 (valid from 01.09.2001) № 2341-III, available on the official website of Ukrainian Parliament at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14

[21] Gotin O.M. *Criminal responsibility for issuing of bad quality products in conditions of market economy (problems of theory and practice)*: Dissertation of Candidate to Doctor of Legal Sciences: 12.00.08. – Lugansk, 2003. – p. 44, cited in Azarov D.S. *Crimes in the sphere of computer information (criminal-law research)*: Monography. – K.:Atika, 2007. – p.43

[20] Azarov D.S. *Crimes in the sphere of computer information (criminal-law research)*: Monography. – K.:Atika, 2007. – p.62

Object of crimes usually has three vertical dimensions: main, additional and facultative [direct] objects of crime(s). When we apply these theoretical dimensions to the sphere of cyber crimes, main [direct] object of the crime will be "separate relations in the sphere of computer information, which emerged and exist for exercising by certain person(s) informational activity regarding computer information and which were substantially damaged by particular crime or placed in danger of such damage".[22] Facultative [direct] object of the crime, as shows its name, is present not always, pretty much only in such instances, where we have crossed several spheres and respectively types of societal relations, for example, when was unlawfully "hacked" protected medical information of the patient with AIDS, it will be also relations in the sphere of medical law for it is duty of doctors in view of specificity of illness, to make sure such information is kept maximum secure and confidential. And finally, the additional [direct] object of cyber crimes will be the property relations.[23]

Concept of property relations is not universal; however it has four universally accepted aspects: [24]

1) subject of property relations

2) object of property relations

3) rights

4) acquisition of right

With all respect to the scholars, who in heated debates established consensus over these four aspects, I can't help criticizing it. First of all, because aspect of "rights" already

[23] Ibid.

[24] Wolfgang Mincke. In *Property Law on the Treshold of the 21st Century*. – p. 651

includes acquisition of rights, and there is no reason why it should be viewed separately let's say from loss or transfer of rights. And secondly, I object this four-aspect structure on the grounds that it doesn't include duties, only rights, which according to the general theory of law are so intertwined that co-exist mutually.

Therefore I would adopt three-aspect model of property relations, namely

1) subject of property relations

2) object of property relations

3) content of property relations[25]

This way definition of property relations (as well as other legal relations) becomes consistent: property relations, are legal relations in which subjects participate in order to receive objects through rights and duties, which form content of such relations. But of course, such model is also far from being perfect, at least regarding the terminology, which is confusing and can be easily mixed with the elements of the crime itself.

As obviously central right of property relations is the right to property. Thus we come to the bottom of our logical braird and link right to property with cyber crimes.

B. Legal nature of right to property: scope and types

1. Different right to property in the nutshell

Definition of right to property has at least two dimentions: international and national. And at the second level there will be as many variants of local application of those international standards, how many legal systems we have, for each legal culture has gone

[25] Again, this three-aspect model can be considered common knowledge, because at least in Ukraine and Russia legal scholars (for example Kelman M.S.,Murashyn O.G., Khoma N.M., General Theory of State and Law (2000), Skakun O.F. Theory of State and Law (2006), Tsvik M.V., Tkachenko V.D., Petryshyn O.V., General Theory of State and Law (2002) from Theory of State and Law, as well as in Criminal Law, Civil Law, Administrative Law, Financial Law are almost unanimous in teaching such model.

through own phases of development and has been shaped by unique political, historical, economical conditions.

Continental system of law (Civil Law), to which belongs Ukraine, enhances political component of right to property. So difficultly won and encrypted in written law, it has achieved status of almost sacred right, which has to be protected and preserved. It is static and shall remain as such, this is why it is regulated by uniform, stable and difficult to amend normative-legal acts (like Constitutions, Codes, Decrees, Laws and Regulations), which have to be obeyed by all who apply them, including judges; and why it has to be concentrated in hands of only one person (either physical or legal, including state), which has three exhaustively defined competences to possess, use and dispose.[26]

Therefore system of property protection is one-pillar, uniform, and clear in application, as we will see in Chapter II in more detail.

On the other side of the coin we have Anglo-Saxon, or Common Law system, that places great value on economical aspects of property rights. (Yes, rights, because unlike civil law system, there is not one of them). Key concept of this system is economic expediency. It is dynamic, flexible and multi-faceted. There is nothing wrong with having ownership divided among many persons, and living list of rights-components of ownership subject to change and development. Let it be eleven for now, and the judges will create new in precedents, as main building bricks of new regulations in common law.

Anglo-Saxon concept of property is greatly efficient. For as it has been formulated by R. Coase[27], with defined so property and zero transactional costs, structure of manufacturing

[26] Idea expressed in this and next paragraph is merger of my thoughts on civil law understanding of property and reading of the book Basylevych V.D., *Intellectual property* (2006), pp.78-140.

[27] Coase R.H., *Institutional Structure of Manufacturing*. (Nobel prize lecture) (1991), in ed. by Williamson O.E., Winter S.G. *Nature of the Firm. Origins, Evolution and Development.* (2002)

remains the same effective regardless of the change of owners. The system functions by itself, without any regard to rulers and regimes. And functions well.

But unfortunately, there is no tub of honey without spoon of tar.[28]

Because if something is not defined, it can not be fully protected, especially with regard to criminal law, which by its nature has to have final narrow-tailored codified definitions. And crimes against property are slipping through little loopholes of flexibility, left in the system to remain living and breathing, and many misconnected institutions to the utmost try to coordinate efforts to prevent it from happening.

It is very different. And very interesting. Because this systems can learn from each other and merge in creating the most powerful system of protection against cyber crimes ever.

2. Scope and definitions

As we already have mentioned above, both in Ukraine and US right to property is defined through its scope.

In Ukraine, as we could have expected, it is defined by law, more precisely – Civil Law of Ukraine, Art. 316 (1) of which says that "proprietary right is right of a person to a thing (property), which it realizes according to the law in own will, independently from will of other persons".[29]

Scope of right to property in Ukraine is defined by three elements: possession, use and

[28] Referring to proverb Ukrainian proverb There is no tub of honey without spoon of tar, meaning that even the biggest good may little flaws. Its English version would be Fly in the ointment or In every ointment there is a fly.

[29] Civil Code of Ukraine, available on-line at the official website of Ukrainian parliament at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=435-15, as accessed on 09.11.2008

disposal.[30] Possession means practical domination over the thing, use refers to extraction of practical qualities from the thing and disposal is ability of owner to determine legal destiny of the thing.

This means that right to property is viewed in its entirety, but consisting of three elements.

In US and other common law countries it is complex of rights to property, defined by those, who apply them, with the most inclusive list given by English scholar A.M. Honoure[31]:

1. Right to possess
2. Right to use
3. Right to dispose, which is understood a bit differently as in civil law, including only right to manage
4. Right to appropriate benefit
5. Right to remaining value – to determine whether the object will disappear during use (like eaten kilo of apples), destroyed, or sold if needed by owner
6. Right to security – to safeguard against expropriation
7. Right to have all right transferred after object if received in heritage
8. Right to be unlimited in time, unless contract states other
9. Right to be free from dangerous or harmful use - to freely choose not to use it against rights of others
10. Right to be held responsible because of redress – because property can be taken for returning the debt

[30] Supra note, in Art. 317 (2)

[31] Honoure A.M., *Ownership: Oxford essays in jurisprudence* (1961), pp. 112-1128, as analyzed in Basylevych V.D., *Intellectual property* (2006), pp 99-100, my translation

11. Right to remaining character – to return rights to property when the term of transfer of them has been agreed upon and has expired

Here it is worth to notice, that rights number nine and ten in Honore's list are present in civil law system also, but for example, in Ukraine, they are viewed not like rights, but as obligations – obligation to treat property responsible and not use it against rights of others, and obligation to perform redress if held responsible. Constitution of Ukraine proclaims that "use of property can not harm rights, liberties and dignity of citizens, interests of society, worsen ecological situation and natural qualities of land".[32]

But in general abyss between understanding of right to property in Ukraine and in US is not so huge, because harmonization of legal systems being an integral part of world globalization has been bridge to create such institutes in property law of Ukraine as operative management and commercial cognizance.

Both of these rights has been developed as curious attempt to escape from historical domination of state-centered concept of property and to allow growth of some market sprouts even in the most regulated spheres of economy.

Right to commercial cognizance is almost right to property but with limited disposal: for certain types of property owner has to give consent for such disposal and in other times can control use and good condition of property object, without interference in operative and commercial activity of the enterprise. It is worth noting, that cognizant is by law entitled to protection of his property interest even against the owner himself.[33]

[32] Art. 41 (8) of Constitution of Ukraine, available from parliamentary website www.rada.gov.ua, accessed on 09.11.2008

[33] According to Art. 136 of Commercial Code of Ukraine, available from parliamentary website at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?page=2&nreg=436-15, accessed on 09.11.2008

Right to operative management is right, according to which owner or empowered by him organ gives for non-commercial use, possession and disposal object of property but reserves right to check its condition and diligent use as well as to expunge extra property which is not used or used not according to its designation.[34]

3. Typology and classifications

Traditionally right to property is classified according to its content, taking as classification criteria right holders (subjects) and objects. We will take a look at this approach, and then, as it seems a little over-theoretical and clumsy to be applied in practice, offer one more alternative.

Subjects of right to property are:

- Physical persons[35]

- with such relation to the state as citizens, apatrids, bipatrids, foreigners

- age and capability: minors before 14, of 14-18 years, adults, with full or limited to different degree capability

- engaged or no in the entrepreneurial activity

- Legal persons [36]

- according to the authority and act of its establishment: of public and private law

- legal nature: union of persons or property

- in the legal form of: associations (entrepreneurial and not entrepreneurial), establishments and other.

[34] Art. 137, Ibid.

[35] Classification based on the Art. 2 , 24-49 of the current Civil Code of Ukraine, adopted on 16.01.2003 № 435-IV, available at the official website of Ukrainian Parliament at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=435-15

[36] Ibid., on the bases of Articles 83-83; See also Art. 63 of the current Commercial Code of Ukraine, adopted on 16.01.2003 № 436-IV , available at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?page=2&nreg=436-15

Entrepreneurial associations in their turn are divided according to the form of ownership, number of founders, presence of foreign capital, amount of workers and income, etc.[37]

If the first classification is clear: all persons, recognized by law as such can be holders of property right, the classification of right to property according to its objects is not at all so undisputable. And the main reason is simply because debatable is definition of the object of property right itself.

Definition like "everything can be an object of property right that can be bought or sold", is criticized as a closed circular one; [38] derived from accounting – when object of property relations is everything which" appears in a balance sheet" is unacceptable, because of its chameleon nature: if you look at it from shareholder perspective, it probably will include things like "good will, know-how, trade secrets"[39] , but from creditor perspective in definition will fit only "tangible pure assets"[40] , as well as because it is specifically tailored for use in commercial sphere and is not applicable in the non-commercial areas like public health or education.[41]

So in order to define whether something is an object of the property relations, is offered case-to-case three prongs test, with three criteria being[42]:

1. Scarcity
2. Specificity
3. Publicity

[37] Art. 63 of Commercial Code of Ukraine, Ibid.

[38] Supra note 5, at 654.

[39] Ibid. at 655.

[40] Ibid. at 656.

[41] Ibid.

[42] Wolfgang Mincke. In *Property Law on the Threshold of the 21st Century*. – p. 659

Let us apply this test to the things, claimed to be objects of the property relations, of course, previously defining and describing them, and see if they really are ones:

1) Information:

When we apply Mincke test, it shows that as a rule, information is object of property relations, for

- it is scarce, but artificially made such by legal means (because invented once joke or once gained information is no longer scarce);[43]
- it can be made specific
- it has to be in majority of cases public (otherwise there will be no legal certainty regarding what is allowed and what is not and the businesses will stop out of fear to break some unknown rule);[44]

If we talk about information as object of property relations in the sphere of cyber law, it should be specific type of information – computer information. Though being extensively regulated and even over-regulated, it is not defined by the legislator. But from prospective of legal theory, "computer information is knowledge about world around us and processes in it, introduced in the form of data, which can be fixed in the electronic form."[45]

Computer information is separate from all other types of information, because it has such features as

- "unconsumeability" (meaning that from one person getting to know it, it does not disappear for the other person)
- being not material

[43] Ibid.

[44] Ibid.

[45] Supra note 20 at p. 80.

- economical (it helps save other resources)
- computerization (creation and use with help of computer technique)[46]

Besides that computer information has specific dual nature in the criminal law – it can be both tool of crime (apparatus means of computer technique like computers, peripheral devices, physical holders of machine information), and object, aim of the crime (for example machine information of user, possessor, owner; program supplies, such as system, applied, systematic programs)[47]. And because of such separation, ownership of information holder is not the same as ownership of information itself.

It's also worth to mention, that criminal law protects not computer information as such, but only the most important for society categories of it, like state, commercial secrets and personal data, leaving other kinds of computer information for regulation by softer legal means for other branches of law.

2) Digital property:

If to put it brief, digital property is intellectual property which exists in the digital computerized form. It includes electronic databases, web casting, e-books etc.

Digital property is specific and, if decided so by its owner, can become scarce and public.

3) Virtual Property:

Virtual property, like URL, e-mail account, location within a network of links, chat room or electronic bank account, is defined as type of computer code, which repeats characteristics of real world objects.[48] Being as distinct from intellectual property as ownership of the book by buyer is distinct from novelist's ownership of rights of its

[46] Orlovskij D.L., Cherednichenko O.Yu. *Computer Crimes: Concept of lectures for the Course „Informational Safety"* (2006) at p. 7

[47] Ibid. at p. 9-11.

[48] See *Virtual Property*. Joshua A.T.Fairfield. 85 B.U.L.Rev. (2005) at pp. 1053-1057

content[49]; virtual property shares with real world property three such basic characteristics as non-rivalrousness, interconnectivity and persistence, which makes possible to regulate it through common law theory of property.[50]

In spite of being widely criticized from point of view of economics, law and industry, it is worth to recognize distinct virtual property in the cyber space law, because it can allow overcome inefficient under use of on-line resources due to existing overlapping exclusion rights (anticommons) and avoid fragmentalization of property rights in cyberspace, by giving common law courts solid uniform legal ground for protection of property interest in on-line resources.[51]

Virtual property is the most public one from all three types, and it is pretty specific. However, its scarcity is debatable. For example location within network of links, which is important for websites engaged in the electronic commerce, can be taken by limited number of enterprises, and storage of e-mail is limited, but at the same time unlike natural resources, electronic resources do not have limits, and nothing prevents this enterprise to create another network of links or person to get as many e-mail addresses, as wished.

But in general now we can say that according to the criterion of object of property relations, there can be right to information, right to digital property and to virtual one.

Alternative classification of objects of property relations, and respectively property rights, which I find much more practical and easier to apply, is offered in Council of Europe Convention on Cybercrimes which is discussed and analyzed in detail in Chapter II.

[49] Ibid., p. 1095

[50] Ibid., pp.1053, 1054

[51] See ibid., at pp. 1069-1088.

C. General aquantaince with cyber crimes

In February 1999 the world woke up with news that US Ministry of Defense Skynet Satellite was subjected to military communications security breach, which has been officially characterized as enemy attacks. In the very end the threat appeared to be "a small group of hackers traced to southern England", who "managed to reprogram the control system before being discovered" and "though Scotland Yard's Computer Crimes Unit and the U.S. Air Force worked together to investigate the case, no arrests have been made."[52]

Another famous hacker's intrusion took place on the board of Apollo 13 years earlier. But back then because of this hack damaged by fuel explosion module was freed from carbon dioxide and safely landed on earth.[53]

The third story was even somewhat funny: "Early one Friday morning the CBSNews.com homepage was replaced by the Representative Kucinich's presidential campaign's logo. The page then automatically redirected to a 30-minute video called "This is the Moment," in which the candidate laid out his political philosophy. The Kucinich campaign denied any involvement with the hack, and whoever was responsible was not identified. As campaign struggled in the fall of 2003, a hacker did what he could to give it a boost" [54]

These stories, and people created them, may catch imagination and cause amazement by advancement of human brain to compete with technique. However, two of them are crimes to be punished with all severity of law.

[52] Iozzio Corinne. *The 10 Most Mysterious Cyber Crimes* , available in PC magazine at http://www.pcmag.com/article2/0,2817,2331225,00.asp, accessed 10.11.2008

[53] Segan Sasha. *The Ten Greatest Hacks of All Time* from the PC Magazine, available at http://www.pcmag.com/article2/0,2817,2330368,00.asp, accessed on 10.11.2008

[54] Supra note 51.

(Second of course is not, for system was hacked for saving people's lives).

There is no legal definition of what actually cyber crime is, but throughout the course of this research journey we will focus on individually defined crimes and their characteristics in order to be able to create own definition.

In order to give the fullest general characteristic of the cyber crimes, the most suitable beginning seems to be traditional criminalistic methodology of crime description, so we will start with personality of criminal, go on with his/her motives and aims, describe typical ways, places and tools of cyber criminals and say about the victim.[55] This information would be helpful in drawing conclusions about ways of combating cyber crimes.

If to picture typical Ukrainian cyber perpetrator, it would be professional male criminal in his 30-s. Except "profis" cyber crimes commit also so-called "challengers" and computer-dependent or ill people, but their persentage is relatively small and motivation – make fun, became little famous or cope with phobia are not as dangerous for society as of cold-blooded 79% of professionals[56] who commit cyber crimes as job and way of earning a leaving.[57] Little percentage of female cyber criminals is compensated by the fact that they appear to be greedier and their part in terms of damages is more substantial. And curious facts, helpful in breaking stereotypes about cyber criminals, are that out of 1000 cyber criminals only 7 are professional IT people – because they have high ethical standards and care about professional reputation; and that 97 % of people committing cyber crimes are

[55] Written below characteristic is my summary from the book Orlovskij D.L., Cheredmichenko O.Yu. *Computer Crimes: Concept of lectures for the Course „Informational Safety"* (2006).

[56] Ibid. at p. 11-12

[57] Ibid.

government workers (!)[58]. Now it becomes a little clearer why it's so hard to write laws which detect and prosecute cyber crimes and to enforce existing ones.

And if from the diversity of data try to sketch a typical American cyber criminal, it has to be noted, that "perpetrators were predominantly male (75.8%) and half resided in one of the following states: California, Florida, New York, Texas, Illinois, Pennsylvania and Georgia. The majority of reported perpetrators were from the United States. However, a significant number of perpetrators also were located in United Kingdom, Nigeria, Canada, Romania, and Italy." At the same time "males complainants lost more money than females (ratio of $1.67 to every $1.00 lost per female). This may be a function of both online purchasing differences by gender and the type of fraudulent schemes by which the individuals were victimized", with " electronic mail (e-mail) (73.6%) and web pages (32.7%)" being "the two primary mechanisms by which the fraudulent contact took place."[59]

The owners of computer systems, who are victims of cyber crimes in 4/5 of cases usually, do not report crimes because:

- do not trust in competence of police
- don't know real worth of damage or have no hope to return it
- want to preserve reputation of the organization
- are reluctant to disclose security system of organization, because information might spill

[58] Ibid. at p. 13

[59] FBI 2007 FBI 2007 Internet Crime Report, available at http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf, as accessed on 19.11.2008, p.2

- and (the best reason I've ever heard!) because in the process of investigation of other crime their own not very legal manipulations may also be discovered[60]

As cyber criminals are very creative people, there are hundreds of ways to commit crimes, in fact every cyber crime is unique in its own way, but all ways can be grouped into 5 main categories according to the goal of the crime and appear as following[61]:

1) for acquisition of computer technique: usual ways of committing crimes against property

2) for interception of information: active such as wilful intercept, character seize, message wiretapping, passive or electromagnetic interception, audio interception with or without brought-in technology, video interception and "garbage cleaning"

3) for acquiring unsanctioned access to computer devices: "catch the tail", "abordage" and "follow the fool", "emergency", "mystification", "slow choice", "storage without walls", "hole" techniques

4) for manipulations with data and leading commands of computers: change of data during entering/exit, "Trojan horse" and its "relatives", asynchronic attacks, modelling, copying of programs and integral micro schemes, methods of going through program protective means

5) combined ways

And of course, in order to have full picture, we need to give definitions as well as classification of the cyber crimes and definitions for particular ones of them. The most all-embracing seem to be two: [62]

1. According to the use of computer either as an aim or a tool

[60] Ibid. at pp.17-18

[61] Supra note 41 at pp. 19-50

[62] The following classifications starting from words "arson" and ending with "military operations" are directly quoted from T.O. Conner. *Cybercrimes: the Internet as a Crime Scene*. Accessed on 22.11.2007 at http://faculty.ncwc.edu/toconnor/315/315lect12.htm

Computer as an aim in cases of

- „Arson (targeting a computer center for damage by fire)
- Extortion (threatening to damage a computer to obtain money)
- Burglary (break-ins to steal computer parts)
- Conspiracy (people agreeing to commit an illegal act on computer)
- Espionage/Sabotage (stealing secrets or destroying competitors records)
- Forgery (issuing false documents or information via computer)
- Larceny/Theft (theft of computer parts)
- Malicious destruction of property (destroying computer hardware or software)
- Murder (tampering with computerized life-sustaining equipment)
- Receiving stolen property (accepting known stolen good or services via computer)"

Computer as a tool in cases of

- „Internet fraud (false advertising, credit card fraud, wire fraud, money laundering)
- Online child pornography; child luring (sexual exploitation; transportation for sexual activity)
- Internet sale of prescription drugs & controlled substances (smuggling; drug control laws)
- Internet sale of firearms (firearms control laws)
- Internet gambling (interstate wagering laws; lottery laws; illegal gambling businesses)
- Internet sale of alcohol (liquor trafficking)
- Online securities fraud (securities act violations)
- Software piracy & Intellectual Property theft (copyright infringement; trade secrets)
- Counterfeiting (use of computer to make duplicates or phonies)"

2.According to the insider or outsider perpetrator

Insiders usually commit

- “espionage
- theft;
- sabotage;
- and personal abuse of the organizational network,”

While outsiders are predominantly found quilty of

- „industrial espionage - theft of proprietary information or trade secrets
- terrorism - attempts to influence or disrupt U.S. policy
- national intelligence - attempts by foreign governments to steal economic, political, or military secrets
- infowarfare - cyber attacks by anyone on the nation's infrastructure to disrupt economic or military operations”

Now that we have full picture of cyber crimes and place of property on it, it is time to see how this theoretical framework is incorporated into normative system of protection of property in cyber space.

Chapter II – Normative protection of property in cyberspace

A. International framework

1. General overview of UN, OECD, EU and G 8 systems

Cyber space is borderless, and such are cyber crimes in it. So it is no wonder, that combat against cyber crimes requires close and extensive international cooperation.

This cooperation has been conducted under auspices of United Nations, Organization for Economic Co-operation and Development, the European Union, Group of Eight, and Council of Europe.

United Nations framework, embracing 192 states, among which Ukraine and United States of America, which on 24th of October 1945 both became its members[63], is naturally the most broad one, beginning with 1966 International Covenants on Civil and Political[64], Economic Social and Cultural Rights[65] and Protocols to them, containing right to property, procedural guarantees, enjoyment of scientific progress (like computers)(Art.15 (1(2) ICESCR), and going on with general instruments, as well as specific ones drafted by specific bodies of UN. As an example of first we shall name UN Convention Against Transnational Organized Crime, progressively defining property as "assets of every kind,

[63] Based on the United Nations Protocol's Blue Book "Permanent Missions to the United Nations No. 295", April 2006 Last updated with ST/SG/SER.A/295/Add.5 (3 October 2006) and on Press Release ORG/1469 of 3 July 2006; appearing on http://www.un.org/members/list.shtml, as accessed on 19.10.2008

[64] The United Nations International Covenant on Civil and Political Rights, available at http://www.hrweb.org/legal/cpr.html, accessed on 21.10.2008

[65] The United Nations International Covenant on Economic, Social and Cultural Rights, available at http://www.hrweb.org/legal/escr.html, accessed on 21.10.2008

whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets " to include virtual property and containing all instrumental aspects like criminalization of participating in organized criminal group as such, (Art.5), laundering of criminal money(Art.6),prosecution and adjudication (Art.11), seizure and confiscation (Art. 12,13, 15), jurisdiction(Art.16), extradition and transfer of sentenced (Art.17, 18), investigations procedure (Art. 19, 20), protection of witnesses and victims (Art. 24, 25), mutual assistance and technical, legal, informational, training and law enforcement cooperation (Art. 29, 18, 28, 27 respectively)[66] makes combat against international crimes coherent and coordinated.

To the second belongs work conducted by

- UNICRI (United Nations Interregional Crime and Justice Research Institute, one of the General Assembly's special research and training bodies[67]), which has mandate for facilitating judicial and law-enforcement cooperation[68], with one of its four priority working areas in emerging crimes, which includes cyber crimes[69].
- UNODC (United Nations Office on Drugs and Crime, one of the specialized offices in UN Secretariat), which not only implements the above mentioned Transnational Organized Crime Convention, but also gathers expert meetings – so far one in Italian city

[66] The United Nations Convention against Transnational Organized Crime adopted by the General Assembly Resolution 55/25 of 15 November 2000, came into force on 29 September 2003, available at http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_eng.pdf

[67] UN special bodies are located according to the UN chart available at http://www.un.org/aboutun/chart_en.pdf, accessed on 21.10.2008

[68] UNICRI's mandate as summarized from its official website http://www.unicri.it/topics/faq.php, accessed on 19.10.2008

[69] These priorities are identified for UNICRI programmes by the UN Annual Crime Prevention and Criminal Justice Commission and available also at http://www.unicri.it/topics/faq.php, accessed on 19.10.2008

of Courmayeur, on 29-30 November 2007, and anther one in Vienna on 2-3 June 2008[70] for developing action plans against identity-related crimes, directed against primarily stored in computers data. Mandate to UNODC for this specific type of activity was given by a higher UN body –

- ECOSOC (UN Economic and Social Council), by its resolutions 2004/26[71] and 2007/20[72]. In addition, ECOSOC itself among its Functional Commissions has Crime Prevention and Criminal Justice Commission (CPCJC)[73].

UN system has huge advantage of universality, but at the same time I would call it rather fragmental, targeting only quite narrow aspects of cyber crimes and barely touching question of property in its context.

Organization for Economic Co-operation and Development, in our area of interest represented by Directorate for Science, Technology and Industry,[74] in contrast to UN system is focused not on facing crimes when already committed, but on more positive side of developing different good practices and regulations in the sphere of information and communication technologies in particular, which would help to increase their economical value, and from one side serve prevention of crimes against property in cyber space, but from the other – inevitably make such crimes more attractive with increasing value of

[70] From official site of UNODC http://www.unodc.org/unodc/en/organized-crime/index.html, accessed on 20.10.2008

[71] ECOSOC Resolution 2004/26 on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at http://www.unodc.org/documents/organized-crime/ECOSOC_res_2004_26.pdf, accessed on 20.10.2008

[72] ECOSOC Resolution 2007/20 on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, available at http://www.unodc.org/documents/organized-crime/ECOSOC_resolution_2007_20.pdf, accessed on 20.10.2008

[73] Its official website is at http://www.uncjin.org/index.html, as accessed on 21.10.2008

[74] Its official website is http://www.oecd.org/department/0,3355,en_2649_33703_1_1_1_1_1,00.html

gain, and more harmful for society in terms of more and more substantial economic losses.

Starting from 1980-s OECD Council has adopted nine recommendations and five declarations related to such fields in the information, computer and communications policy as privacy in transborder information transfers, spam, cryptography, authentification and alike security matters, broadband technologies and wider access to public information, internet economy and E-Commerce.[75]

It is interesting to notice, that Council of OECD has chosen to regulate these areas only by means of non-binding instruments, from all range legal tools available (for example, conventions, agreements, decisions[76] are much stronger in legal force), which is looking especially over-precautious if to take into account, that abstaining member is exempt from application of decision or recommendation, even not talking about declaration, which it is opposing anyway.[77]

---

[75] Here I am referring to C(2008)36 Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information, C(2008)35 Recommendation of the Council on Protection of Critical Information Infrastructures, C(2007)68 Recommendation of the Council on Electronic Authentication, C(2007)67 Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, C(2006)57 Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws against Spam, C(2003)259 Recommendation of the Council on Broadband Development, C(2002)131 Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, C(97)62 Recommendation of the Council concerning Guidelines for Cryptography Policy, C(80)58 Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data; and C(2008)99 Declaration for the Future of the Internet Economy (The Seoul Declaration), C(98)177 Declaration on Authentication for Electronic Commerce, C(98)177 Declaration on Consumer Protection in the Context of Electronic Commerce, C(98)177 Declaration on the Protection of Privacy on Global Networks, C(85)139 Declaration on Transborder Data Flows available from http://webdomino1.oecd.org/horizontal/oecdacts.nsf/subject?OpenView&Start=1&Count=1000&Expand=15.1#15.1, as accessed on 21.10.2008

[76] Classification of OECD legal instruments is available at http://webdomino1.oecd.org/horizontal/oecdacts.nsf/type?openview&count=1000, as accessed on 21.10.2008

[77] Art. 6 (2) of the Convention on the Organization for Economic Co-operation and Development, available at http://www.oecd.org/document/7/0,3343,en_2649_34483_1915847_1_1_1_1,00.html, accessed on 21.10.2008

Another issue, which substantially weakens OECD system in terms of its applicability, is that it expands only to 30 member states (and unfortunate for us thing, is that Ukraine unlike US is not member of OECD).[78] And Art. 12(a) of the OECD Convention tool of "inviting" non-member states to participate in activities of organization helps little.

The **European Union** and the **Group of Eight cooperation** against cyber crimes has the same flaw in this regard: the first is regional and the second unites only the most rich and powerful countries, with the recent bright intellectual explosion in cyber technology in low developed countries, like India, with traditional high crime rate[79] means that large segment of contemporary cyber challenges goes unanswered.

But in any case something is better that nothing.

European Union, even though only for member states, has developed excellent, extensive detailed legal framework concerning different-different aspects of cyberspace, starting with on-line payment systems and standardization of electronic signatures to i2010 Strategy and *e*Europe Action Plans.[80][Existing EU legal framework is nicely summarized in Communication from the Commission of 29 June 2006 on the review of the EU Regulatory Framework for electronic communications networks and services[81], however I would not elaborate on it further, for both Ukraine and US are not subjected to it, so it will be already a little out of the scope of research for present paper.]

[78] See list of member countries at http://www.oecd.org/countrieslist/0,3351,en_33873108_33844430_1_1_1_1_1,00.html, as accessed on 21.10.2008

[79] I consider facts, that India is an example of modern cyber monster and that crime rate is usually higher in lower developed countries to be common knowledge and therefore do not give reference to it.

[80] For details see http://europa.eu/scadplus/leg/en/s21012.htm#CADREJUR, as accessed on 21.10.2008

[81] Communication from the Commission of 29 June 2006 on the review of the EU Regulatory Framework for electronic communications networks and services, available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2006&nu_doc=334, as accessed on 21.10.2008

The Group of Eight, even though having US as one of its leading participants and discussing issues of Internet and crime[82], still remains informal uninstitutionalized group, and such are all its responses to cyber crimes.

And, finally, the Council of Europe, which produced without undue flattering the most elegant, understandable and coherent contemporary document on cyber crimes – Convention on Cybercrime.[83]

Such document worth looking in depth, especially because it has been signed, ratified and entered into force for both Ukraine and US, and is therefore binding upon them.[84]

2. Focus on CoE Convention on Cybercrime

This Convention has been logical continuation and summary of all previous attempts to fight cyber crimes on international level. In its Preamble it addresses not only work, done by already mentioned UN, the OECD, the EU and the EU, but also all previous Council of Europe Conventions, Recommendations, Resolutions and Action Plans in the field[85] and

[82] See Reuters article *Factbox -The Group of Eight: what is it?* at http://www.reuters.com/article/latestCrisis/idUSB262805, accessed on 21.10.2008

[83] Little technical remark: majority of sources agree on writing "cyber crime", but here is used original way of spelling "cybercrime» as appears in Convention itself.

[84] According to the official ratification list of Council of Europe, available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, accessed on 21.10.2008, it has been signed by Ukraine 23.11.2001, and in force from 1.7.2006; and for US signed on the same date, and in force from 1.1. 2007

[85] Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology; Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997) and No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000); Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe – all mentioned in the Preamble of the before mentioned CoE Convention on Cybercrime, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, as accessed on 22.10.2008

goes forward to foresee possible interpretational problems, by offering Explanatory Report as supplement to it.[86]

Convention consists of four chapters: definitions (dream of cyber lawyer!), provisions to be taken at national level, at international level, and final provisions.

Measures, which are to be taken at national level, are divided into substantive and procedural ones.

CoC Classification of Cybercrimes and Its Critique

The substantive part offers classification of the deeds, which the state parties have to make punishable by means of their criminal law, and therefore offers classification of cyber crimes as following[87]:

1. "Offences against the confidentiality, integrity and availability of computer data and systems", where belong illegal access, illegal interception, data interference, system interference and misuse of devices.

Let's analyze each of these crimes in more detail:

Name of offence	Illegal deed	Intent	Object against which it is directed	Additional remarks
Illegal access (Art. 2 CoC)	Access to computer system (whole or part) without right	With intent; Presence of dishonest intent may be required by state-Party	Computer system - device or connected/related group of devices for performing automatic processing of data (according to the Art. 1(a) of CoC)	State may also require one computer system be connected with another, I guess, making harm caused greater

[86] This Explanatory Report is available on-line at http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm, accessed on 22.10.2008

[87] Here and below in this sub-chapter, all analyze is dedicated to the Convention on Cybercrimes, so all citations in "" and tables are made from its text, so I don't reference each word; all other references are mentioned separately

Name of offence	Illegal deed	Intent	Object against which it is directed	Additional remarks
System interference (Art. 5 CoC)	Serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	intentionally	computer data	
Misuse of the devices (Art. 6 CoC)	Without right a) making available by production, sale, procurement for use, import, distribution or alike of device or data for accessing computer system (like password or code) for committing any of above mentioned offences; b) possession of such device or data	with intent to commit any of the offences mentioned above	Device designed or adapted primarily for computer offences; password, code or other data for access to computer system	State party may apply criminal responsibility only for offences related to data, not devices.

The following definitions have some unpolished edges which can be improved, especially of illegal access and illegal interception.

First of all, definition of these crimes is circular: access is access, and interception is interception – and it is difficult to imagine how judges, majority of whom usually are in certain set in legislation respected age, which does not presuppose the same intellectual curiosity towards new technologies, as of youth, will apply these definitions; unless, resorting very frequently to technical expertises, of course. But it will increase time and expenses of criminal process.

Second – illegal access and illegal interception have only limits of intent requirement, are not limited by requirement of harm to be caused, thus raising the problem of over

broadness and punishing not guilty. For example, new paralegal is invited for work to the law firm, which has two sets of legal databases: for all workers, and for senior lawyers only. The "orientation" which bases to use is going to take place in couple of days, when the partner of the firm calls from the court hearing urgently needing some research. Poor paralegal doing his best accesses the second database, simply because it is better. Access is without right, and with clear intent. If the state party has not made the reservation about comprehensive dishonesty of intent, does it mean that when the partner of the firm wins the case, paralegal have to go to jail?

Another unclear moment is with misuse of devices. Why it is ok to misuse devices, but not data, hacker's hammer but not password? What is more damaging? Logic of Art. 6 (2) CoC remains unclear even after reading the Explanatory report, saying it was done "due to different assessments of the need to apply the offence of "Misuse of Devices" to all of the different kinds of computer offences in Articles 2 – 5".[88]

2. "Computer-related Offences"

Name of offence	Illegal deed	Intent	Object against which it is directed	Additional remarks
Computer-related forgery (Art. 7 CoC)	Input, alteration, deletion, or suppression of computer data without right	With intent to make others believe its authentic	Computer data	Party may require intent to defraud
Computer-related fraud (Art. 8 CoC)	Causing loss of property to other person by a) input, alteration, deletion or suppression of computer data; b) interference with the functioning of system	Fraudulent or dishonest intent to receive economic benefit	Computer data; computer system	

[88] Para. 78 of Explanatory Report to Convention on Cyber Crimes, available at http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm, as accessed on 22.10.2008

Current formulation of computer-related offences group, gives us grounds to think that in order to make these legal norms effective and "living", the law enforcement bodies may recourse to abuses, especially I suspect this might be true for Ukraine: no cyber criminal in sound mind would ever say he/she was committing illegal deed with "fraudulent or dishonest intent". And in fact they do not have to, under the non-self incrimination clause. Without acknowledgment of it from the side of perpetrators police hardly ever would be capable to prove intent. Without intent there will be no crime. No successful statistics of fought crimes. And this is where the stories about fingers slammed between the doors come from[89].

3. "Content-related Offences" have only one article and cover all offences like intentional offering or making available, distributing or transmitting, procuring, and possessing, related to child pornography (under which in art. 9 (2) CoC is understood "pornographic material that depicts minor, person appearing to be minor or realistic images representing a minor engaged in sexually explicit conduct"), committed with a help of computer system and using computer data. It is curious to notice that these actions have to be done "without right", suggesting that somebody may in fact have right lawfully commit all described deeds. Another curiosity lays in fact that the same deeds with adult pornography are not a crime at all.

4. "Offences related to infringements of copyright and related rights" are defined through reference to definition of copyright and related rights in national legislation with regard to existing international treaties, and should be "committed wilfully, on commercial scale

[89] No reference – it is from personal communications among Ukrainian lawyers, my colleagues

and by means of a computer system", however party decide not to subject such offences to means of criminal law.[90]

The classification, though still not very consistent in itself (because offences against computer data and systems are also computer-related and may as well involve content-related offences) still gives us good solid grounds for distinguishing **types of property, protected by the Convention.**

If to take it logically, there are only two such types of property:

1. Computer system – one or more devices for processing of computer data.

Material, tangible property, which can belong to any right holder, be it state, legal or natural person. And

2. Computer data – "representation of facts, information or concepts" in "suitable for processing in computer system form".[91]

Both computer system and computer data can be target and tool for cyber crimes. And the same crime can target both computer system and data in it simultaneously.

On the one hand, such modest representation of types of property protected in the cyberspace by this convention, including only undisputable ones (computer system and computer data, which in theories of property law discussed in Chapter I correspond to regular tangible property, digital property and information – with two latter falling under computer data), narrows the scope of protection, by not embracing novel concept of virtual property. But on the other hand, with full regard and understanding of the compromise mechanism on which all international law functions, we can not blame drafters of conventions for this omission, because such futuristic approach would probably

[90] Art. 10(1), (3) of Convention on Cybercrime, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, as accessed on 22.10.2008

[91] Ibid., Art. 1

be not supported by all states-potential signatories. And besides that, Parties to Convention are by reference in Art. 14 (2) (b) of CoC welcome to extend national criminal law protection to other types of property as well.

Flexible system of reservations foreseen for the States-parties, as well as possibility of taking criminally responsible not only physical, but legal person[92], are among two another interesting particularities of discussed document.

However, the biggest problems in protection of property in cyberspace arise not in material aspects, but in procedural ones.

Procedural and related norms

One of the most problematic areas in fighting cyber crimes is preservation of proofs, because specifics of this crimes lies in the fact, that all material prints of them are very quickly perishable.

Foreseen measures include:

1) Orders for expedited preservation of computer data (interim measure aimed at keeping data which is perishable regardless of number of service providers involved) – Art. 16

2) Production order (which helps identifying subscriber's information about services receiver) – Art. 18

3) Orders for search, seizure, real-time collection and interception of computer data – Art. Art. 19, 20, 21

[92] Foreseen also in Art. 10 of the UN Convention on Transnational Organized Crime, available at http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_eng.pdf, accessed 20.10.2008

As jurisdiction in cases of cyber crimes is often definable with great difficulties (are applicable principles of both personal and territorial jurisdiction, and conflict of jurisdictions is to be determined by consultation of States involved – Art. 22), all these and similar investigative measures are to be carried out in very close international cooperation of the states, which is based on four types of legal instruments: international instruments for criminal cooperation, reciprocal agreements, domestic ones, and these Convention, which as specific legal document particularly targeting these type of cyber crimes is used for gap filling even in cases of absence of international instruments and reciprocal agreements, that is mutual treaties about cooperation and assistance especially for extradition, in order to still allow it to happen.[93] But it has to fall in line with minimal penalty and dual criminality requirements (that person is extradited to state which has lesser penalty and that the deed shall be regarded as crime in both states)[94].

Other principles, under which States carry out cooperation in criminal matters, are confidentiality, volunteerism and proportionality.

First is applied in most cases only to the investigative stage, where in order not to jeopardize criminal investigation, all exchange of information between states and this information as such has to be kept strictly confidential.[95] On the other stages of process, where public interest in crime being punished may outweigh such requirement, it might be made more open to public.

Two other principles are not so specific. Volunteerism means that States voluntarily, without any long and complicated procedure of request for information by other State can

[93] Art. 23, Art. 24 (3) of the Convention on Cybercrimes, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, as accessed on 22.10.2008

[94] Art.24 (b), Art. 29 (4), Ibid.

[95] Art. 27 (3) Ibid.

forward information they found relevant and interesting for that other State just by their free will, but may subject it to certain conditions, as stated in Art. 26.

Principle of proportionality is the most general one. It also is closely related with principle of balance referred to in the Para. 10 of the Preamble and means that as each and every criminal investigation in order to disclose crime, has to access certain personal data, the due balance between interests of investigation and privacy has to be kept.

Now, when we have determined international standards for protection of property in cyber space, let us see how they are implemented and used on national level.

B. National Framework

1. Ukraine

History of Ukrainian cyber crimes has started in 1997.[96] Before that we either lived in the times, which were cyber crimes –free, or, most probably, in times when did not exist statistics of crimes called "cyber".

Now we do. And though this statistic nowadays still operates with modest numbers – 53 in 2004, 62 in 2005, there is a growing negative trend of unsuccessful investigations, when only half of those reported cases are solved, with solved not meaning remedied and punished.[97]

In the ocean of cyber crimes Ukraine is only a small drop, which probably could have been dried with its own forces being it regular crimes. But the cyber crimes are borderless, and only one tiny weak link in world cyber security system can easily destroy the whole chain, making it useless.

[96] Azarov D.S., *Crimes in the Sphere of Computer Information (Criminal-Law Research)* (2007), p.10

[97] Ibid. p.13

Constitution of Ukraine proclaims, that legal regime of property as well as "deeds, which are crimes" and responsibility for them, judicial system, procedure and expertise, organization of prosecution and punishment can be determined exclusively and only by the laws of Ukraine.[98]

This requirement is fruit of understanding of huge responsibility embodied in regulation of these spheres and their crucial role for society. Therefore, it is only the Supreme Council of Ukraine, collegial wisdom of 450 deputies, who have right to regulate this matters.

One of the first laws of independent Ukraine was Law on property.[99]

Then in 2001 finally we adopted not Soviet (translated from Russian legislation "copy-paste") type, but first real Ukrainian Criminal Code,[100] and in 2003 almost simultaneously – Civil and Commercial Codes which elaborated on right to property.

Besides them was adopted package of laws, related to certain specific aspects of cyber space and its protection: on information and on scientific-technical information, on protection of information in informational-automatized systems, on all types of connection, on telecommunications, on state secret, on basics of national security, electronic digital signature, electronic documents and electronic flow of documents. [101]

---

[98] Art. 92 (1) (7), (14) and (22) of the Constitution of Ukraine, available from parliamentary website http:// zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=254%EA%2F96-%E2%F0, accessed on 09.11.2008

[99] Law of Ukraine of 07.02.1991 № 697-XII On Property, available from parliamentary website at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=697-12 , accessed on 09.11.2008 – acted until 2007, when was cancelled because of incompatibility with new Civil Code 2003 which appeared in practical application

[100] In Ukrainian legislative tradition Code is unified into one piece of legislation collection of laws on the matter

[101] Law of Ukraine of 02.10.1992 № 2657-XII On Information, Law of Ukraine of 25.06.1993 № 3322-XII On Scientific-Technical Information, Law of Ukraine of 05.07.1994 № 80/94-BP On Protection of the Information in the Informational-Automatized Systems, Law of Ukraine of 16.05.1995 On Connection of Ukraine, Law of Ukraine of 18.11.2003 № 1280-IV On Telecommunications, Law of Ukraine as of 21.09.1999 № 1079-XIV On State Secret, Law of Ukraine of 19.06.2003 № 964-IV About Basics of National Security of Ukraine, Law of Ukraine of 22.05.2003 № 852-IV On Electronic Digital Signature, Law of Ukraine of 22.05.2003 № 851-IV On Electronic Documents and Electronic Flow of Documents – all checked on 15.11.2008 and accessible from website of Ukrainian parliament www.rada.gov.ua in their official version

All criminal procedural matters are regulated by Criminal-Procedural Code of Ukraine.[102]

And the last, but not in any way least - Law of Ukraine of 07.09.2005 № 2824-IV On the Ratification of the Convention on Cybercrime.[103] From this moment it has become with accordance of provision of Art. 9 (1) of Constitution part of national legislation of Ukraine. And in conditions of equality of all forms of law it has supremacy as the latest and the most specific law, according to which have been changed all previous ones. This is why we have dedicated to it so much attention in previous chapter.

Regarding the substantial requirements of the Convention, Ukraine has fully incorporated them in our legal system, with only two reservations[104]:

- Art. 6 CoC[105] (misuse of devices) reservation: production, sale, procurement for use or otherwise making available, when it concerns device main purpose of which is commission of offences (like harmful computer programmes) is not a crime; the same as production and procurement for use of password, code or alike data for access to part or all computer system (named in part 1 a. ii) is also not regarded as crime.

If first part of this reservation, though seemingly illogical, but is falling under reservational limit of Art. 6 (3) of CoC, second part is questionable from the side of interpretation, because Art.6(3) states, that reservation shall not concern "the sale, distribution or otherwise making available of the items referred to in paragraph 1 a. ii". So

---

[102] Criminal-Procedural Code of Ukraine – Law of Ukraine of 28.12.1960 № 1002-05 available at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1002-05, accessed on 15.11.2008

[103] Law of Ukraine of 07.09.2005 № 2824-IV On the Ratification of the Convention on Cybercrime, available at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2824-15, accessed on 15.11.2008

[104] Supra note 99.

[105] Here and below Convention on Cybercrime, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, as accessed on 22.10.2008

it is a question of whether we treat production and procurement for use as way of "making available". The answer of Ukrainian legislator and international delegations with whom it agreed on this reservation was no, it is not.

However, in the very end in the Criminal Code appeared art. 361-1, aimed at protection against interference without right to computer system. And it can be reasonably implied, that in order to interfere, we need to access first.[106]

But I still would suggest that this norm needs to be clarified and modified, because in its current wording it gives cyber criminals free tools for hacking computer systems, and it substantially weakens protection of property in relation to cyber crimes.

- Art. 9 reservation says that procurement and possession of child pornography with means of computer system and data-storage is not a crime.

From the side of formal requirements, Art. 9 (4) allows such reservations. However, my intellectual curiosity still asks the question: » why?" In precise case with Ukrainian reservation, I may try to explain it because in structure of cyber crimes in Ukraine number of content-related cyber-offences is very small, and legislation in relation to them vague, so this reservation was done for benefit of the doubt, thinking that its better to let few possibly offenders free then to punish them and undermine belief in justice.

But on international plane, what justifies existence of this reservation? Looking into explanatory report to it[107] still does not give the answer.

Criminal Code of Ukraine contains Chapter XVI, which is named "Crimes in the sphere of use of electronic-counting machines (computers), systems and computer nets

[106] Criminal code of Ukraine, adopted on 05.04.2001 (valid from 01.09.2001) № 2341-III, available on the official website of Ukrainian Parliament at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14, accessed on 09.11.2008

[107] Explanatory Report to Convention on Cybercrimes
is available on-line at http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm, accessed on 22.10.2008

and nets of electro connection". [108] As by legal tradition of Ukrainian legislator Chapters in Criminal Code have to be named according to the object, it protects, such name has received strong criticism from at least two points of view: first of all, because computer is the same object of property relations as the rest and use of it is the same element of right to property, debatable is justification for putting it in the separate chapter; second- because in this chapter legislator without grounds united in one chapter two different legal relations: in the sphere of computer information and in the sphere of telecommunications (used as synonym for electro connection and containing teletype, telegraph, telephone, mobile or cell, radio and TV connection).[109] It is also argued, that because of this duality, under title of Chapter XVI are protected only those legal relations, where these two connect: only when computer information is transmitted through channels of telecommunications, because other crimes against telecommunications – like damage of telecommunications' lines (Art. 360) are situated in other Chapters.[110]

Though these regulation may work (because for example access to Internet, one of the most important nets in cyber space, if to put aside Fi-Wi means, is acquired through modem and telephone), it is the case where trying to be all-embracing, leads to over breadth jeopardizing effectivity, and these spheres would be much easier and efficiently protected, if the legislator would separate this "Siamese twins".

Having said that, it is time to look at six crimes contained in this Chapter XVI in depth:

[108] Here and below I give my translation of wording of the Criminal code of Ukraine, adopted on 05.04.2001 (valid from 01.09.2001) № 2341-III, available on the official website of Ukrainian Parliament at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14, accessed on 09.11.2008

[109] From class notes, recorded during the lecture on computer crimes conducted in National University of "Kyiv-Mohyla Academy" (Kiev, Ukraine) by Prof. Azarov D.S.

[110] Ibid.

Art. 361 "Interference in the work of computers, automatized systems, computer nets or nets of electro connection" is a deed, which in order to be punishable shall lead to "spill, loss, forfeit, blockage of information or violation of established order of its rooting" [111]

Art. 361-1 focuses on **"**creation for use, distribution or sale of harmful of program or technical means, their distribution or sale" [112], designed for such interference.

Art. 361-2 - on "sale and distribution of information with limited access through computers, automatized systems, computer nets or storage devices"[113] of such information.

Art. 362 targets **"**change, destroy or blockage of information, which is being processed or is being saved" committed by the person, who has right to access it.

Art. 363 speaks on "violation of rules of exploitation or order or rules of protection of information, which led to substantive damage, committed by person, who is responsible" for operating these "computers, automatized systems, computer nets or nets of electro connection"

and Art. 363-1 prohibits spam ("intentional mass distribution of messages of electro connection, committed without prior consent of addressees") which has led to transgression or stoppage of work of the abovementioned objects.

As we can see, these crimes deal with several types of property objects:

- computers
- automatized systems
- computer nets
- nets of electro communication
- computer storage devices

[111] Supra note 104.

[112] Here and all the way down while making adopted translation of articles Ibid.

- harmful program means
- harmful technical means
- information: which is transmitted with the means of electro connection, is being processed in computers, computer nets or automatized systems; information with limited access.

It is clear, that the last type of property – though immaterial, is key to all of the above, because "who owns information, owns the world"[114]. It is information and its flow, which makes all these material things it exists in so precious, vulnerable and urgently in need of protection. Under **computer information** we understand "knowledge about outer word and processed, which are happening in it, presented in the form of data, which can be fixed in electronic form (but not always is fixed – for example during transmission it is already not in one place but yet not in another)".[115] Such understanding corresponds to definition of "computer data" in Art. 1 of the Convention.[116]

Information with limited access can exist in two forms – as confidential information or as secret information. Definition of confidential information is of excluding type – there is a list of things in law,[117] which can not be kept confidential, like standard of living of population or epidemics, and all other ones physical or legal persons, state, can themselves decide how to keep and disclose, if the right of public to know does not overwhelm their right to hide. Secret information is information, evaluated by the state expert in questions of secret, which because of its character and possibility to harm

[114] These words have been in different times attributed to Francis Beckon, Winston Churchill and Mr. Rothschild http://otvety.google.ru/otvety/thread?tid=7be7643fe2c88011

[115] There is no legislative definition of computer information, and the one quoted was invented by my Professor of Criminal Law – Azarov D.S.

[116] Convention on Cybercrime, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, as accessed on 22.10.2008

[117] Law of Ukraine of 02.10.1992 № 2657-XII On Information, available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12, accessed on 15.11.2008, Art. 30

national security of Ukraine if disclosed, and was included in the List of State Secrets under certain category and level of access.[118]

Harmful program means are "soft" and technical means "hard" tools of committing cyber crimes, with examples of first being viruses like "I love you" or "Trojan horse", and second – ultra-sensible sound catcher, which allows to record and differentiate sound of each key on the keyboard and intercept information being inputted in this moment.

Computer storage devices like USB sticks, CD and DVD discs, hard and floppy disks, are not separate object of protection, however, if we take into account, that their value all the time increases, especially USB drives and hard discs that now can be bought separately in a form of little case containing 300 additional GB of computer memory, simple example of which costs around 613 US dollars.[119] When is harmed external storage device like that, this is way of harming computer information on it.

For now the question can be solved if to reflect damage to storage devices while counting total damage done by crime, and be punished more severe if it is greater. And for redress, the victim of the crime can claim this sum also in damages to be compensated in civil suit in criminal case.[120]

Computers, their nets, automatized systems and nets of electro connection are expressly mentioned among property objects which can be damaged in process of commission of cyber crimes.

[118] Law of Ukraine as of 21.09.1999 № 1079-XIV On State Secret, available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1079-14, accessed on 15.11.2008, Art. 1

[119] Prices is indicated according to the price-list of computer store at http://www.knsneva.ru/vcd-20645-1-268745/GoodsInfo.html

[120] Art. Art 248, 253, 255, 261, 264, 268, 272, and so on, Criminal-Procedural Code of Ukraine – Law of Ukraine of 28.12.1960 № 1002-05 available at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1002-05, accessed on 15.11.2008.

Under computer we understand electronic-counting device, as these two terms are used in all articles of this Chapter of Criminal Code as synonymic.[121]

Terms computer nets is used in Ukrainian legislation meaning two or more connected together computers. It is a little different than in Art. 1 (a) of the Convention[122], where it says that even one device can be computer system. But I honestly can not imagine it, because "system" means connection of elements,[123] and one standing alone element can not be regarded as a "system".

Automatized systems and nets of electro connection, as we have already mentioned above, appear in this articles only because legislator mixed together two types of legal relationships, and touch computer crimes in rare cases when they are committed through such systems or with means of electro connection like telephone/modem.

This approach is not the only difference between Ukrainian and international approaches. Ukrainian Criminal Code is different from international standard set in the Convention on cyber crimes in several ways, both in criminal judicial technique and substance.

First of all, if Convention has so-called material structure of crimes – criminal is deed itself, while Ukrainian has also material structure of crimes – for deed to be treated by state as a crime, needs to be also harmful consequence. It makes proving that something is a crime more difficult and number of crimes lesser.

Then, Ukrainian legislature foresees so-called qualified structure of crimes - all articles, except Art. 363 says, that those deeds committed for the second time, with prior

[121] Criminal Code of Ukraine adopted on 05.04.2001 (valid from 01.09.2001) № 2341-III, available on the official website of Ukrainian Parliament at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14, accessed on 09.11.2008, Art. Art. 361, 361-2, 362, 363, 363-1.

[122] Supra note 115.

[123] From Wikipedia at http://en.wikipedia.org/wiki/System, as accessed on 19.11.2008 : "system (from Latin *systēma*, in turn from Greek *σύστημα* systēma) is a set of interacting or interdependent entities, real or abstract, forming an integrated whole."

conspiracy of group of persons, or causing significant damage (100 or more times higher than minimum salary) have to be punished more severely.

Next, Art. 11 of the Convention [124] requires criminalization of "attempt of aiding or abetting". Ukrainian criminal law always takes into account role the perpetrator played in the crime,[125] however, if to take into account that this Article of Convention does not indicate because of which circumstances the crime has been left unfinished and remained only "attempt" (was it brilliant work of police in preventing crimes or wilful decision of to-be perpetrators not to finish the crime), this article creates danger that person, which realized wrongfulness of own act and decided to stop, will be punished anyways. Therefore, even though Ukraine has not made specific Article 11 CoC reservation in this regard, this provision was not mirrored in national Criminal Code as contrary to national legal system and principles of criminal law.[126]

And the last, but not least difference is substantial one.

Ukrainian legislation directly foresees spam, not explicitly mentioned in the CoC, at the same time protection against child pornography, and of intellectual property rights is done by means of other norms of the Criminal Code, without taking into account their specificity when committed on-line, the same as computer-related fraud (Art. 190 (3) of Criminal Code of Ukraine), placed in the Chapter VI about general crimes against property, and Art. 200 financial crimes, which can be done with computer means in the Chapter VII about crimes in the sphere of commercial activity.

Neither Convention, nor Ukrainian legislation defines cyber crimes, at the same time Convention places under this title broader spectrum of crimes.

[124] Also Supra note 115.

[125] Supra note 120, Art. Art. 26-30

[126] Ibid. Art. Art. 13-17

Another very interesting paradox of Ukrainian legislative technique, comprehensively needed to be mentioned here, is that on one side, as we have already said above, signed and ratified Convention by itself becomes part of national legislation, and it is incorporated in national legal system by law. On the other side, Criminal Code is also a law. Therefore we have two laws on the same matter, which are different.

There is no publicly available data on practice of this conflict resolution, but by general rule the latest shall prevail, and the latest was law incorporating Convention. However, I firmly believe, that Criminal Code needs to be one more time amended to make the system of anti-cyber crimes protection coherent.

To be objective, we must admit that there has been at least three attempts at the level of legislative proposals to do so, but all of them so far unsuccessful. [127]

Regarding the procedural law, the Criminal Procedural Code has been not in any way modified to meet specific needs of combating cyber crimes. But hopefully, new Criminal Procedural Code, which is planned on the level of talks in legislature for long ago (because the old one is 48 years old already and quite outdated), will take care of it.

As for now, the procedural provisions are introduced only in Law on ratification of Convention, saying, that mutual assistance in criminal procedural matters regarding the cyber crimes is to be carried out either through Ministry of Justice if the assistance is sought by the judge, or through the General Prosecution Office of Ukraine if it is sought by prosecutor or similar law-enforcing authority.[128] Therefore, there is no specific institutional structure for combating cyber crimes, and it is only organs of general

[127] Legislative proposals № 908-IV from 05.06.2003, № 3039 from 30.01.2003 and № 3039-1 from 20.02.2003, analyzed in Azarov D.S., *Crimes in the Sphere of Computer Information (Criminal-Law Research)* (2007), at pp. 239-249

[128] Ibid. 99

competence without specialization, that need to face the difficulties of combating cyber crimes.

In all these intertwined and overcomplicated system of anti-cyber crime laws, surprisingly enough exists good old elegant **solution**. Universal remedy for property losses for victims of cyber crimes – civil suit in criminal matters.[129]

What is it? **Civil suit in criminal matters** is way of compensating damage to property, injured or destroyed by crime, implementation of which begins after decision of the court gains its legal force.

It has mixed legal nature, because incorporates both norms of civil and criminal law, uniting their strength and weaknesses: it saves a lot of time and resources, because is based on established in criminal case fact of crime and sum of damage, done by it; claim can be made in every documentary form and is except from state tax. It is easy to apply, and the investigator has duty to inform person about such right. And possible amount of compensation is highered by the fact that it can be secured through preliminary measures, applicable right after person discovered violation of his/her property rights', and finding of perpetrator's property is done by the best means of criminal police. However, the weak side is that period of submitting this claim is limited – only before the beginning of court investigation in criminal matter, and if party misses this moment, and then it can receive compensation only in regular civil damage suit.

Damage according to it is compensated either by perpetrator (in most cases), or by responsible for him persons (if it is a minor below 14 – parents or legal guardians, from 14 to 18 perpetrator pays compensation him/herself, but in case he/she lacks money, the costs also bear parents/legal guardians), if perpetrator has not been identified – the state. If

[129] Paragraphs on civil suit in criminal matters are based on my research done for the Criminal Procedural Law, with all laws, court practice and literature I read for it indicated in list of literature and normative sources

perpetrator pays voluntarily, it usually reduces the final penalty and in some cases can even prevent further punishment.

This compensation has personal character – coming from guilty deed of one person to another one, suffering personal loss from it. The actual sum of compensation depends on actual financial possibilities of the perpetrator, and they can hide their real income. But the good thing is that it can not be hidden forever – as this suit almost does not have statute of limitations and civil suit in criminal case decision is executed even if perpetrator is granted pardon or falls under amnesty.

Thus we can state, that in spite of little shortcomings civil suit in criminal cases remains in Ukraine so far the best (in comparison to another alternative - regular civil suit for damage compensation, which is longer and costlier) and the most efficient way to remedy property damage, done by crimes, and cyber crimes in particular.

2. United States

Amount of cyber crimes regularly committed in US is counted on the much bigger scale, than in Ukraine and is assessed in hundreds of thousands a year.[130] But statistical data of Ukraine and US can not be directly comparable, because of natural – much bigger population and geographical area, technocratic – majority of root servers have been situated on the territory of US due to their technical advancement, and legal factors - there are more deeds defined as crimes in United States than in Ukrainian laws.

However, the fact that United States had encountered cyber crimes earlier and at a larger scale, gives us presupposition, that they have also developed response to them at a larger scale.

[130] FBI 2007 Internet Crime Report, available at http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf, as accessed on 19.11.2008

And this supposition is right.

United States of America have not only net of both federal and state laws and precedents about their application to stand against cyber crimes, but have developed elaborate institutional structure for facing cyber crimes and anti-cyber crimes' national strategy.[131]

National Strategy to Secure Cyberspace contains three main objectives: to prevent attacks, to minimize vulnerability and to decrease losses.

In achieving these objectives, the key factor is public and private cooperation, in which private sector takes the lead, and government interferes only in the most acute cases, need of national coordination or regarding questions, nature of which allows it to be solved only by government (like national security).

In order to structuralize directions of actions, have been identified five national priorities: to create system of responses, to launch program for reduction of vulnerability, to start training and enhance international cooperation and for the beginning to secure governmental cyberspace.

On implementing these priorities currently are working four governmental institutions. In line with aim of effective response works Computer Emergency Readiness Team of Department of Homeland Security.[132] FBI targets those crimes, which can not handle private sector, and issues FBI Best Practices to Prevent Internet Crime[133]. US Secret Service under Congress auspices works with financial cyber crimes, costing national

[131] National Strategy to Secure Cyberspace, developed by US Department of Homeland Security in February 2003, available at http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf, as accessed on 19.11.2008.
Below goes my summary of it.

[132] US Department of Homeland Security Computer Emergency Readiness Team webpage http://www.us-cert.gov, accessed on 19.11.2008

[133] Supra note 128, starting at p. 17

economy the most dramatic losses.[134] And US Department of Justice provides help to fighters against cyber crimes of all levels by providing them with legal resources in Computer Crimes and Intellectual Property Section.[135]

Among federal legislation, [136] which as opposite to state-level one regulates those cyber crimes, where

- computer information harmed has international or state military security aspects
- injured computer belongs to federal entity
- crime is connected with financial body
- for commitment of it are used interstate or international communications or actors[137],

or, to put it brief, - where crime endangers values, entrusted to protection of federal government, we can group two categories of laws.[138]

The first – directly aimed at cyber crimes, such as articles 1029, 1030, 1362, 2510, 2701, 3121 of Title 18 of the United States Code, which deals with computer fraud, access devices, lines, stations and systems of communication and interceptions in it and operation with this information, such as storage, recording, routing, addressing and signaling. [139]

---

[134] US Secret Service webpage http://www.ustreas.gov/usss/whoweare.shtml, accessed on 19.11.2008

[135] US Department of Justice Cyber crimes Section webpage http://www.cybercrime.gov, accessed on 19.11.2008

[136] Here we will analyze and discuss only federal legislation. First of all, because almost each of 50 states has own anti-cyber crimes laws which are very similar to federal and it will be physically impossible to embrace them all, second for the clarity of comparison, for Ukraine has single all-state level cyber legislation

[137] Supra note 125, p. 225

[138] Ibid. for idea of division of legislation into two such categories

[139] 18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices , 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers , 18 U.S.C. § 1362. Communication Lines, Stations, or Systems , 18 U.S.C. § 2510 et seq. Wire and Electronic Communications Interception and Interception of Oral Communications , 18 U.S.C. § 2701 et seq. Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. § 3121 et seq. Recording of Dialing,

And second big group – legislation which helps tackling cyber crimes through related crime areas: arson, if it destroys computers and computer devices; fraud with credit cards, when committed on-line; unlawful operations with military information, if carried out with computer means; falsification of official data with computer means; fraud with communication means, including postal services delivered on-line; purposeful causing of damage, to military objects in particular; [140]

Apart from the said Titles of the US Code aspects of computer-related crimes can be found in such recent legislature as Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act (PROTECT Act) regarding the content-related cyber crimes;[141] Homeland Security Act 2002, especially Sec. 225,[142] and USA Patriot Act 2001[143] regarding national security related aspects of cyber crimes; as well as great body of case law, explaining peculiarities and specifics of application of cyber law norms,

---

Routing, Addressing, and Signaling Information, available at US Department of Justice official database at http://www.cybercrime.gov/cclaws.html, as accessed on 27.11.2008

[140] 15 U.S.C. § 81. Arson on Special Marine or Territorial Jurisdiction, 15 U.S.C. § 1644 18 U.S.C. § 793. Gathering, Transmitting or Losing Defence Information, 18 U.S.C. § 794. Gathering or Delivering Defence Information to Aid Foreign Government, 18 U.S.C. § 1001. Fraud and False Statements, 18 U.S.C. § 1341. Frauds and Swindles, 18 U.S.C. § 1343. Fraud by Wire, Radio, or Television, 18 U.S.C. § 1361. Government Property or Contracts, 18 U.S.C. § 2071. Concealment, Removal, or Mutilation Generally, 18 U.S.C. § 2155. Destruction of National-defence Materials, National-defence Premises, or National-defence Utilities, 18 U.S.C. § 2314. Transportation of Stolen Goods, Securities, Moneys, Fraudulent State Tax Stamps, or Articles Used in Counterfeiting, 18 U.S.C. § 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications, as available from http://uscode.house.gov/search/criteria.shtml, accessed on 27.11.2008

[141] Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act (PROTECT Act), available from http://www.cybercrime.gov/cclaws.html#recent, accessed on 21.11.2008

[142] Homeland Security Act 2002, Sec. 225 (called Cyber Security Enhancement Act), available at http://www.cybercrime.gov/homeland_CSEA.htm, as accessed on 21.11.2008

[143] US Patriot Act 2001, available at http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:%5D, as accessed on 21.11.2008

among landmark cases being *Intel Corp. v. Hamidi*[144] about spam being not violation of trespass against such cyber property as e-mail computer system, *Guest v. Leis*[145] about immunity of government official's computers against seizure, *Dowling v. United States*[146] US Supreme court case, where it has been found that "[the infringer] does not assume physical control over the copyright, nor does he wholly deprive the owner of its use" and therefore shall not be punished, after which MIT student promoting free software and computer games charged with computer wire fraud statute in *U.S. v. Lamacchia*[147] has been set free.

Even these few mentioned above cases show, that in spite of very extensive regulation, which not only meets all international standards set in Council of Europe Convention on Cybercrimes, but even exceeds them, American cyber law protects only that property, which can have some material form and therefore material damage – computers, computer systems, computer programs, which can be written down, and information which potentially can be stored on some device; but virtual property objects like e-mail, are often unprotected because judges are reluctant to call crime something over which perpetrator does not have "physical control".[148]

Another law-enforcement issue is that due to this dual way to combat cyber crimes by both specific anti-cyber crime norms and computer-related general norms, exists danger of

[144] *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1347-48 (Cal. 2003)
Also available at http://cyber.law.harvard.edu/openlaw/intelvhamidi/cases.html, as accessed on 12.11.2008

[145] *Guest v. Leis* Nos. 99-4115, 99-4176 (6th Cir. July 2, 2001), available from http://www.findlaw.com/01topics/10cyberspace/computercrimes/gov_laws.html, as accessed on 12.11.2008

[146] *Dowling v. United States* 473 U.S. 207 (1985) at p. 217.
Also accessible at http://cyber.law.harvard.edu/cyberlaw2005/Dowling_v._United_States, as accessed on 21.11.2008

[147] *U.S. v. Lamacchia* No.94-10092RGS (United States District Court, District Court of Massachusetts, 7th of April 1994), available at http://www.loundy.com/CASES/US_v_LaMacchia.html, as accessed on 12.11.2008

[148] Supra note 144.

qualifying the same deed two times. To avoid it, we need to apply general principle of law, giving priority to particular law before general.[149] And in order to help judges with this question by US Sentencing Commission has developed sentencing guidelines, in which among other it advices to increase level of crime in exact correlation with damage done to property, and places cyber crimes among economic crimes. [150]

However, such legal tool as bigger sentence has more ideological than practical effect for protection of property in cyber space, when it shows all potential perpetrators that the bigger property damage, the more years in prison they will serve. And this legal remedy works more for perspective of crime prevention or at least damage-lessening.

And practical tool for remedying damage, done by cyber crime, as any other property and non-property crime, exists so called "civil suit in criminal matters". While this name may be put without parenthesis in Ukrainian legal system, where it represents something in the middle between civil and criminal law, and is civil damage suit based on material civil law, but conducted according to criminal procedural norms, together with criminal investigation, in US it is normal civil suit, carried on civil procedural norms not together with, but after criminal case is over, only link it has with criminal maters is use of criminal findings and fact that damage was done by crime.[151]

In spite of both countries' systems working quite good, with Ukrainian being a little more effective, because it is not initiative of crime victim to sue for compensation, but obligation to offer such opportunity by state officials investigating cyber crime, and its greater time and cost economy, both examples of civil remedy scheme have flaw in logic:

[149] I consider this principle common knowledge and therefore do not give reference.

[150] U.S. Sentencing Guidelines that Relate to Computer Intrusions , available at http://www.cybercrime.gov/2B1.1Full.htm, accessed on 21.11.2008

[151] On the basis of materials placed by US Department of Justice Office for Victims of Crime and US National Crime Victim Bar Association at http://www.ovc.gov/help/welcome.html and http://www.victimbar.org/vb/main.aspx?dbID=DB_ProviderInfo725, as accessed on 27.11.2008

because of legal technicality, difference in standards of proof in civil and criminal cases, it happens that not guilty in crime are guilty in civil case, or it can go that far that victim of the crime receives compensation from the seizure of the book about this crime, written by the accused.[152]

[152] As has happened in the O.J. Simpson trial, from the trial materials at http://www.law.umkc.edu/faculty/projects/ftrials/Simpson/Simpsonaccount.htm, accessed on 21.11.2008

Conclusions, challenges and perspectives

This work has been an attempt to study cyber crimes, define them, identify weak spots in legislation allowing them to exist, and foresee effective legislative responses to cyber crime challenges, allowing to secure property in cyber space.

Using triple comparative method: comparing theoretical and practical approaches; international and national systems, and two (American and Ukrainian) national systems of cyber crime regulations among themselves, I have come to conclusions, that:

1. Existing legal approaches understand cyber crimes broadly, as crimes in which computer and computer-related objects are either objects or tools of crime. Such theoretical definition will serve for the purpose of law-drafting, however its normative fixation is unnecessary in view of dynamic nature of cyber crimes, non-stopping need for amendment of which will preclude prosecution of freshly emerging cyber crimes.

2. Number of cyber crimes will raise faster than number of legislative responses to them, but be compensated by the scientific and technical progress, twilight side of which they are. And as the law, the same as politics is only art of possible,[153] we can soften this situation by improving protection of right to property, which is one of the most fundamental and valuable rights being injured in the cyber space, by interchanging and implementing advantages of existing national systems.

3. Currently in the world exists two layer structure of combating cyber crimes: international, leaded by the Council of Europe, and national ones. International system faces transborder challenges of cyber crimes. National ones take into account national paradigms of property and specifics of criminal law related to them. Because of these specifics substantial norms of law clearly are limited by domestic use and can not be imported in other legal systems beyond the level of minimal compromise, reached in the

[153] Words "Politics is art of possible" belong to Thomas Mann

Council of Europe Convention on Cybercrimes, which was incorporated in both US and Ukrainian national legal systems.

4. However, procedural norms and organizational strategies can. And such implementation can be very fruitful:

Ukrainian system of protecting property in cyber space would greatly benefit from adopting American approach of creating specialized (as opposing to currently acting general) governmental bodies, which would have narrower, but much higher competence in the matter.

American system would save huge amounts of time and money, if civil suit for compensation of committed by crime damages, would be as now in Ukraine incorporated in the criminal procedure and lead by state officers on behalf of victims of crime and not by victims alone. Such model would strengthen trust of citizens in their government and create responsible citizenship.

And both systems would be ready to face future cyber crime challenges if would foresee in legislation protection not only of material, digital (intellectual) property and computer information, but of virtual property as well.

Bibliography

A. Books

Azarov D.S., *Criminal Responsibility for the Crimes in the Sphere of Computer Information (autoreferat for dissertation for Candidate in Juris Doctor)* (2003).

Azarov D.S., *Crimes in the Sphere of Computer Information (Criminal-Law Research)* (2007).

Banning, Theo R.G. van, *The Human Right to Property* (2002).

Basylevych V.D., *Intellectual property* (2006), pp.78-140.

Bick Jonathan, *101 Things You Need to Know About Internet Law* (2000).

Biegel Stuart, *Beyond Our Control? Confronting the Limits of Our legal System in the Age of Cyberspace* (2001).

Belovas, Ulla, Legal *Aspects of Internet Banking (*2003).

Bojko, A.M. *Criminal law obligation of compensation of caused by crime damage.(Autoreferat for Candidat in Juris Doctor)* (1995).

Brinson, J.D., Dara-Abrams B.,Dara-Abrams D., Masels J., McDunn R., White B., *Analyzing E-Commerce and Internet Law* (2001).

Cavazos, Edward A., Morin Gavino, *Cyberspace and the Law: Your Rights and Duties in the On-line World* (1994).

Clifford, R., *Cyber crime: The Investigation, Prosecution and Defence of a Computer-Related Crime*. (2001).

Karchevs'kyj M.V., *Crimes in the Sphere of Computer Technique Use* (2006).

Klymenko O.Ya. *Civil suit as one of the forms of providing of compensation for damage caused by crime by investigator.(Autoreferat for Candidat in Juris Doctor)* (2003).

Koblikov A.S.(Ed.) *Criminal process* (2000), pp. 121-127.

Kovalenko Ye.G., Maliarenko V.T. (Ed.) *Criminal Process of Ukraine* (2006), pp. 159-190.

Krykunov O.V. *Civil suit for compensation of moral harm in Criminal process of Ukraine.(Autoreferat for Candidat in Juris Doctor)* (2002).

Lessig, L., *Code and Other Laws of Cyberspace* (1999).

Maanen, van E. / Walt A.E.van der (ed.), *Property Law on the Threshold of the 21st Century* (1996).

Organization for economic co-operation and development, *10 Computer-related crimes: analysis of Legal Policy* (1986).

Orlovskij D.L., Cheredmichenko O.Yu. *Computer Crimes: Conspect of lectures for the Course „Informational Safety"* (2006).

Power, R., *Tangled Web: Tales of Digital Crime from the Shadows of CyberSpace* (2000).

Rose, L., *Net law: Your rights in an online world* (1995).

Tertyshnik V.M. *Kryminal-procedural Law of Ukraine* (2003), pp. 370-378.

Tertyshnik V.M. *Scientific-practical Commentary to Criminal-procedural Law of Ukraine* (2003).

Todorovska, Mirjana, Protection *of the Intellectual Property on the Internet* (2003).

Wall, David (ed.), *Crime and the Internet* (2001).

B. Articles

Adam Mossoff, *What is Property? Putting the Pieces Back Together*, 45 Ariz. L. Rev. 371, 376 (2003)

Corinne Iozzio . *The 10 Most Mysterious Cyber Crimes* , available in PC magazine at http://www.pcmag.com/article2/0,2817,2331225,00.asp, accessed 10.11.2008

Harold Smith Reeves, Comment, *Property in Cyberspace*, 63 U. Chi. L. Rev. 761, 776 (1996).

Jane K. Winn, *Electronic Chattel Paper Under Revised Article 9: Updating the Concept of Embodied Rights for Electronic Commerce*, 74 Chi.-Kent L. Rev. 1055, 1061-62 (1999).

Joshua A.T. Fairfield, *Virtual Property*, 85 B.U.L.Rev. 1047 (2005).

Kenton K. Yee, *Location.Location.Location: Internet Addresses as Evolving Property*, 6 S. Cal. Interdisc. L.J. 201, 203-10 (1997).

Patricia Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. Rev. 2164, 2170 (2004).

Richard Epstein, *Cybertrespass*, 70 U. Chi. L. Rev. 73, 76 (2003).

Sasha Segan. *The Ten Greatest Hacks of All Time* from the PC Magazine, available at http://www.pcmag.com/article2/0,2817,2330368,00.asp, accessed on 10.11.2008

T.O. Conner. *Cybercrimes: the Internet as a Crime Scene*. Accessed on 22.11.2007 at http://faculty.ncwc.edu/toconnor/315/315lect12.htm

C. Normative sources

International framework [according to drafting body, in order of appearance in the text]

UN

The United Nations International Covenant on Civil and Political Rights, available at http://www.hrweb.org/legal/cpr.html, accessed on 21.10.2008

The United Nations International Covenant on Economic, Social and Cultural Rights, available at http://www.hrweb.org/legal/escr.html, accessed on 21.10.2008

The United Nations Convention against Transnational Organized Crime adopted by the General Assembly Resolution 55/25 of 15 November 2000, came into force on 29 September 2003, available at http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_eng.pdf, accessed on 20.10.2008

ECOSOC Resolution 2004/26 on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at http://www.unodc.org/documents/organized-crime/ECOSOC_res_2004_26.pdf, accessed on 20.10.2008

ECOSOC Resolution 2007/20 on International cooperation in the prevention, investigation,

prosecution and punishment of economic fraud and identity-related crime, available at http://www.unodc.org/documents/organized-crime/ECOSOC_resolution_2007_20.pdf, accessed on 20.10.2008

OECD

Council of Organization of Economic Co-operation and Development in Europe Recommendations:

C (2008)36 Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information,
C (2008)35 Recommendation of the Council on Protection of Critical Information Infrastructures, C (2007)68 Recommendation of the Council on Electronic Authentication,
C (2007)67 Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy,
C (2006)57 Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws against Spam,
C (2003)259 Recommendation of the Council on Broadband Development,
C (2002)131 Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security,
C (97)62 Recommendation of the Council concerning Guidelines for Cryptography Policy,
C (80)58 Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data;

and Declarations

C (2008)99 Declaration for the Future of the Internet Economy (The Seoul Declaration),
C (98)177 Declaration on Authentication for Electronic Commerce,
C (98)177 Declaration on Consumer Protection in the Context of Electronic Commerce,
C (98)177 Declaration on the Protection of Privacy on Global Networks,
C (85)139 Declaration on Transborder Data Flows

all available from http://webdomino1.oecd.org/horizontal/oecdacts.nsf/subject?OpenView&Start=1&Count=1000&Expand=15.1#15.1, as accessed on 21.10.2008

Convention on the Organization for Economic Co-operation and Development, available at http://www.oecd.org/document/7/0,3343,en_2649_34483_1915847_1_1_1_1,00.html, accessed on 21.10.2008

EU

Communication from the European Union Commission of 29 June 2006 on the review of the EU Regulatory Framework for electronic communications networks and services, available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2006&nu_doc=334, as accessed on 21.10.2008

CoE

Convention on Cybercrime, available at
http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, as accessed on 22.10.2008

Explanatory Report to it
is available on-line at http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm,
accessed on 22.10.2008

Committee of Ministers Recommendations:

No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications,
No. R (88) 2 on piracy in the field of copyright and neighboring rights,
No. R (87) 15 regulating the use of personal data in the police sector,
No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes,
No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Resolutions:

No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997) and No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000);

Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe –

available from http://www.coe.int/t/cm/documentIndex_en.asp, as accessed on 22.10.2008

Ukraine

Constitution of Ukraine, available from parliamentary website
http:// zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=254%EA%2F96-%E2%F0,
accessed on 09.11.2008

Civil Code of Ukraine, available on-line at the official website of Ukrainian Parliament at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=435-15, as accessed on 09.11.2008

Commercial Code of Ukraine, available from the website of Ukrainian Parliament at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?page=2&nreg=436-15, accessed on 09.11.2008

Criminal Code of Ukraine adopted on 05.04.2001 (valid from 01.09.2001) № 2341-III, available on the official website of Ukrainian Parliament at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14, accessed on 09.11.2008

Criminal-Procedural Code of Ukraine – Law of Ukraine of 28.12.1960 № 1002-05 available at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1002-05, accessed on 15.11.2008

Law of Ukraine of 07.02.1991 № 697-XII On Property, available from parliamentary website at http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=697-12, accessed on 09.11.2008 [acted until 2007]

Law of Ukraine of 02.10.1992 № 2657-XII On Information, available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12, accessed on 15.11.2008

Law of Ukraine of 25.06.1993 № 3322-XII On Scientific-Technical Information, available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3322-12, accessed on 15.11.2008

Law of Ukraine of 05.07.1994 № 80/94-BP On Protection of the Information in the Informational-Automatized Systems, available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80%2F94-%E2%F0, accessed on 15.11.2008

Law of Ukraine of 16.05.1995 On Connection of Ukraine № 165/95-BP, available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=160%2F95-%E2%F0, accessed on 15.11.2008 [acted until 2003]

Law of Ukraine of 18.11.2003 № 1280-IV On Telecommunications, available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1280-15, accessed on 15.11.2008

Law of Ukraine as of 21.09.1999 № 1079-XIV On State Secret, available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1079-14, accessed on 15.11.2008

Law of Ukraine of 19.06.2003 № 964-IV About Basics of National Security of Ukraine, available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15, accessed on 15.11.2008

Law of Ukraine of 22.05.2003 № 852-IV On Electronic Digital Signature, available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=852-15, accessed on 15.11.2008

Law of Ukraine of 22.05.2003 № 851-IV On Electronic Documents and Electronic Flow of Documents, available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=851-15, accessed on 15.11.2008

Law of Ukraine of 07.09.2005 № 2824-IV On the Ratification of the Convention on Cybercrime, available at
http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2824-15, accessed on 15.11.2008

Law of Ukraine of 21.04.1999 № 606-XIV On Executive Procedure [Procedure of Execution of Court Decisions], available at http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=606-14,
accessed on 24.11.2008

Ruling of the Supreme Court of Ukraine "About Court Practice in Cases of Compensation of Moral (immaterial) Damage" from 31.03.1995 № 4

Ruling of the Supreme Court of Ukraine "About Practice of the Courts in Viewing Civil Cases with Claims for Damage Compensation" from 27.03.1992 № 6

Ruling of the Supreme Court of Ukraine "About Practice of the Courts of Ukraine in Using Legislation about Compensation of Material Damage Caused by Crime and Recovery of Unlawfully Acquired Property" from 31.03.1978 № 3 with subsequent changes

United States

Constitution of the United States of America

United States Code

15 U.S.C. § 81. Arson on Special Marine or Territorial Jurisdiction

15 U.S.C. § 1644 18 U.S.C. § 793. Gathering, Transmitting or Losing Defence Information

18 U.S.C. § 794. Gathering or Delivering Defence Information to Aid Foreign Government

18 U.S.C. § 1001. Fraud and False Statements

18 U.S.C. § 1341. Frauds and Swindles

18 U.S.C. § 1343. Fraud by Wire, Radio, or Television

18 U.S.C. § 1361. Government Property or Contracts

18 U.S.C. § 2071. Concealment, Removal, or Mutilation Generally

18 U.S.C. § 2155. Destruction of National-defence Materials, National-defence Premises, or National-defence Utilities

18 U.S.C. § 2314. Transportation of Stolen Goods, Securities, Moneys, Fraudulent State Tax Stamps, or Articles Used in Counterfeiting

18 U.S.C. § 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications,

as available from http://uscode.house.gov/search/criteria.shtml, accessed on 27.11.2008

18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices ,

18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers ,

18 U.S.C. § 1362. Communication Lines, Stations, or Systems ,

18 U.S.C. § 2510 et seq. Wire and Electronic Communications Interception and Interception of Oral Communications ,

18 U.S.C. § 2701 et seq. Stored Wire and Electronic Communications and Transactional Records Access,

18 U.S.C. § 3121 et seq. Recording of Dialing, Routing, Addressing, and Signaling Information,

all available at US Department of Justice official database at http://www.cybercrime.gov/cclaws.html, as accessed on 27.11.2008

Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act (PROTECT Act), available from http://www.cybercrime.gov/cclaws.html#recent, accessed on 21.11.2008

Homeland Security Act 2002, Sec. 225 (called Cyber Security Enhancement Act), available at http://www.cybercrime.gov/homeland_CSEA.htm, as accessed on 21.11.2008

Homeland Security Act 2002, Sec. 225 (called Cyber Security Enhancement Act), available at http://www.cybercrime.gov/homeland_CSEA.htm, as accessed on 21.11.2008

US Patriot Act 2001, available at http://thomas.loc.gov/cgibin/bdquery/z?d107:HR03162:%5D, as accessed on 21.11.2008

U.S. Sentencing Guidelines that Relate to Computer Intrusions , available at http://www.cybercrime.gov/2B1.1Full.htm, accessed on 21.11.2008

National Strategy to Secure Cyberspace, developed by US Department of Homeland Security in February 2003, available at http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf, as accessed on 19.11.2008

FBI 2007 Internet Crime Report, available at http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf, as accessed on 19.11.2008

Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1347-48 (Cal. 2003)

Also available at http://cyber.law.harvard.edu/openlaw/intelvhamidi/cases.html, as accessed on 12.11.2008

Guest v. Leis Nos. 99-4115, 99-4176 (6th Cir. July 2, 2001), available from http://www.findlaw.com/01topics/10cyberspace/computercrimes/gov_laws.html, as accessed on 12.11.2008

Dowling v. United States 473 U.S. 207 (1985).
Also accessible at http://cyber.law.harvard.edu/cyberlaw2005/Dowling_v._United_States, as accessed on 21.11.2008

U.S. v. Lamacchia No.94-10092RGS (United States District Court, District Court of Massachusetts, 7th of April 1994), available at http://www.loundy.com/CASES/US_v_LaMacchia.html, as accessed on 12.11.2008

D. Main websites

www.rada.gov.ua homepage of Ukrainian Parliament (Verkhovna Rada), where are placed the most updated official versions of all Ukrainian legislation for public access

http://www.cybercrime.gov homepage of US Department of Justice Computer Crimes and Intellectual Property Section with links to cases and legal resources on cyber crimes in US

http://www.us-cert.gov homepage of US Department of Homeland Security Computer Emergency Readiness Team

http://www.fbi.gov/cyberinvest/cyberhome.htm FBI cyber investigations webpage