BILETA

14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

Balkan Hackers War in Cyberspace

Mirjana Drakulic, Ph.D.[1], Ratimir Drakulic, M.S.[2]
1 Associated Professor of Computer Law and Business Law
Faculty of Organizational Sciences, University of Belgrade
2 Assistant of Introduction to Information Systems
Faculty of Organizational Sciences, University of Belgrade

Abstract: *The activities of hackers are criminal by themselves. Their getting to the Internet gives them new dimensions and raises numerous questions of regulation, investigation, "catching", proving and punishing. However, the special situation arises when the war breaks between the hackers of different countries. That happened at the end of 1998 when the hackers from Serbia changed the site outlook of Kosovo Liberation Army and left a number of messages. The reply to this challenge came from Croatia. Its hackers got into the information system of the National Library of Serbia and blocked its work for several days. The hackers from Serbia then got into the site of the Croatian "giant' news agent "Vjesnik". All this is a special kind of terrorism, but this time in the Balkan Cyberspace. Waging of such a specific war opens a lot of dilemmas, beginning from the treatment of such activities, the legal procedure to be applied, to the question of harmonizing the activities among other countries in order to be stopped. As these activities are considered "neutral", and very often looked upon benevolently there arise, apart from legal, a lot of ethical questions. The idea of the possibilities of waging hacker war in cyberspace inspires fear and, at the same time, makes it necessary to be covered. The authors are of the opinion that these questions must be given greater attention and that national regulations that will solve this multinational and multilevel problem are to be brought into line with each other. International regulation is not to stay on the margins. To this, selfregulation should be added.*

Key words: hackers, hackers war, information war, cyberspace, law.

I FROM HAKERS TO CYBERWARRIORS

Information technology, besides its numerous advantages and its great applicability in all spheres of work and life also created different problems. The dependency on such a technology is ever growing as well as its vulnerability. A lot of problems, relations and habits have changed by its application. Practically there are no fields in which the information technology hasn't been involved, changing at least a part of them. At the same time there are fields where information technology has brought in the revolutionary changes. Art, management, surgery, trade, communication, entertainment, business, exploration, education and others are only a part of them. However, the changes weren't static, they started to breach into the activities located on the margin of legality or beyond. The computer criminal is emerging. Surprisingly fast, this specific criminal has taken an outline the sea monster of information environment. It dashed all the shores and provoked fears and dilemmas. It

opened legal and ethical gaps between known, traditional, legal principles, postulates and institutes and new regulations and demands. What was unconceivable in at the moment or space has become normal in the other, and vice versa. The best examples are hackers, which were, at the beginning, treated with friendliness and sympathy by society. In some circles they were treated almost with worship. They were talented young men, mostly students. They were often the pioneers in their professional fields. (Chandler, 1996; Spering, 1992; Levy, 1985; Rogers, 1999).

The attitude towards them is changing. The characteristics of the 80's are as follows (Drakulic, 1996):

- Unauthorized access is becoming more heterogeneous and complex;
- The first Hacker groups are being formed according to their own rules of conduct and activity
- The environment shows less adoration and generally greater concern and fear;
- The problem of determining the concept and contents of hacker activity is becoming evident;
- The problems with detection, investigation, arrest and evidence material are growing;
- The first laws are being passed which regulate this phenomenon;
- As a response, the accelerated development of protection and security systems commences;

With time, intrusions are becoming ever more sensational and strengthen the attitude to the negativity of hacking and dangerous conduct of hackers. Accordingly, Captain Midnight, Wily Hacker, Markus H.'s, HRH and many others became more and more famous, thus clouding the fame of software developers (Drakulic, Drakulic, 1995).

The beginning of the 90's is characterized by:

- Hacking definitely gains its criminal dimension;
- Hacker intrusions into the systems is becoming more organized;
- Hacker sub-culture is being jeopardized by economic and political pressures, because governments are seriously starting to fight them;
- new regulations, regarding their activities, are being passed more frequently;
- The cooperation on surveillance, detection, criminal prosecution and punishment of hackers is being internationalized and harmonized.

Therefore, the positive sign has practically completely vanished. Hackers are being transformed into individuals who abuse computer by illegal, unauthorized or "hacking" activities and conduct. It should be stated that even though their activities changed in nature, they are still one of the most complex groups of the "information family".

The end of the 90's focused hackers in a completely new light. The development of the Internet drew them into the new "waters". They became soldiers of the special information warfare. At the same time they are the actors of internal struggles. Today they are, at least most of them, calculated, cold-blooded professionals, placing their expertise knowledge in the service of different "forces". Sometimes they are cyber terrorists, at other times common "mercenaries", and occasionally "followers" and " worshipers ". Some of them are self-taught, and some them have passed the "required" training. Whichever role they have they are dangerous and unscrupulous. Even besides spectacular intrusions into the different, and specially well guarded information systems and networks, which spread their fame, silent unauthorized, violent accesses into the data systems belonging to the domain of confidentiality bring ever growing condemn. In some cases it is completely absent or "mild" and is oriented towards describing their activity, and not towards the condemnation. This is the case when the veil of patriotism covers hacker's activity and when the reasons of the intrusion or interception are "justified". Of course the question can actually be raised - are the hackers, in the service of their own people, criminals or heroes?

II THE BALKANS CASE

The computer crime in Yugoslavia has not appeared recently. The first cases were lifted at the start of the 80's. They were the embezzlements with the misuse of Office- position and official documents' forging by using the bank computers. In the next few years the first cases of hacking were registered, but since the criminal law did not recognize unauthorized access to protected systems as a special criminal act, there are no official records, how, when and to whom it happened. The public was not informed since the hackers were trying to mask their activities. They were "assisted" by the injured and their silence. The news would appear only within professional circles, as well as sometimes in-between students, on "SEZAM" (the only BBS in Yugoslavia at that time) or in sparse computer magazines. The occurrence was not characteristic for the Yugoslav information scene, therefore it was hard to follow and analyze. Hackers were students in fact, as they said, or they were "computer fans". The intrusions were conducted more out curiosity than ill intention.

In the middle of 1996 the academic circles began to explore the Internet. Namely, that is when the basis of the academic network on the University of Belgrade was established. Having gained the routine in work with the Internet, the users started to involve into the activities which pertained to hacking. The first two cases were recorded on the two nodes of the academic computer network. The intrusions induced the crash of the network (jammed the network) since the perpetrators conducted the erasing of certain parts of the system. After the local investigation, it was established that there were bugs in the system's protection (security breaches) and that perpetrators were "kids" from 13 to 16 years of age. They connected to the net from the computers belonging to the University employees. The investigation was carried out by the staff of the damaged servers since the police had no authorization to conduct them due to the deficiencies of the Criminal Code. Silenced by "incapacity" of the state the perpetrators continued with their "work". The circle widened, and the hacks became more audacious. The hackers stepped out of the shadow and started to publicize themselves after the hacks, and sometimes they even announced the new ones. The public was neither worried nor excited and it took no sides. It had enough of other problems. Even the professional circles, information specialists and attorneys, did not, in most cases, understand the seriousness and the danger of such activities. They treated them as "mischief", prosaic reality or as "elementary" disasters. This was a new stimulation. It was a time of lone-shots.

Soon the hacker gathering started. At first to exchange the experience and to brag but soon also for joint attack on certain targets. Extremely complex political and economic situation made by the disintegration of former Yugoslavia directed them to once common living space. The broken communication is being re-established, this time through the Internet, between the bold individuals unafraid of the repression in their own countries. They helped each other in the use of certain resources of the Internet, which were inaccessible from certain countries. The picture as a whole was not so idyllic. The first confrontations grounded on the nationalistic basis were initiated. Especially evident is the confrontation between the hackers from Yugoslavia and Croatia. In the beginning it was a child's play of trickery -who broke into whose site. The weighing of powers and abilities commences. The public statements were given or messages left. Thus in July 1996 Goran Katlevic named "the king of Croatian hackers", stated that he: " broke into Yugoslavia's system on the second day of its entrance into the Internet and that it was laughingly easy." He was the first individual from the former Yugoslavia territory against whom an investigation had been initiated for mixing the sites. This skilled hacker broke into the site of the Croatian National Television (HRT) and linked it with Serbia and "Playboy". The shock that the visitors to the site experienced when they saw the texts from Serbia or the naked pictures from Playboy can only be imagined. There is no need to mention the people from the television and the government. By this act he wanted to warn on the poor protection of the sites in Croatia and the overlook of Croatian main Internet provider "Karnet" to supply certain conditions. The others left messages which were supposed to be the evidence of success and prestige. Sometimes it meant removing the opponent from the game, like the two cases of blocking the Croatian link to the Internet. The response was the alleged intrusion into the academic network in Belgrade. The investigation has shown that it was a false alarm, but that the academic network is still not taking the necessary steps to protect it. The satisfactory conclusions were not drawn from the hard experience. The interesting fact is that it motivated the hackers to unite

in finding the more effective ways of protecting the academic network. Haven't the considerations and warnings of the hackers on both sides been alike?

It was a start of hacker wars.

Further on the situation gets new dimensions, the consequences being the political events on the territory of Yugoslavia, particularly Serbia. The conflict turns to the sites related to Kosovo. In October 1998 the presentation of the Kosovo's Albanians paper "Glas Kosova" ("The Voice of Kosovo") was modified. It was the time of great uncertainty in Serbia-Will there be bombing or not? The threat of military intervention raised spirits not only in Yugoslavia. Many foreign sites had their versions about the future developments. Even the Federal Government have placed links on their site leading to the pages, which presented the atrocities done by Albanian terrorists. Special sites belonging to Yugoslavs worldwide were opened in order to present the news to foreign communities. At the same time several widely recognized information agencies (BBC, SKY, and CNN) enabled a vote on the issue whether NATO should bomb Yugoslavia. The voting as a rule lasted for a day and showed that the majority of them were for the bombing. The exception was BBC, enabling the vote for several days. In the beginning there were more visitors who thought that NATO should bomb Yugoslavia. In time, the situation changed. At the end of the voting period 67% of the voters were against the bombing and 33% for. Namely, in such a tense situation it appeared that doing anything is completely normal. One of such "anything activities" was a hacker's intrusion into site of the paper in Albanian. During the "visit" the Serbia coat of arms was placed on the front page together with several "adequate" messages. The messages were written in Serbian and English. One of the messages was: " Welcome to the site of the greatest World liars and murderers", while the second: "Brothers Shiptars this coat of arms will remain on your flag as long as you exist." (Shiptar is an old Serbian name for Albanians from Yugoslavia). The messages were on the site for several hours. Afterwards they disappeared together with the complete presentation. After a certain amount of time the address was signed out as well. The presentation was returned in the same form as it was before the intrusion after the situation had calmed down. It is doubtful whether the news is true about the reward, which has supposedly been offered to the one who locates the guilty party.

This event had been preceded by the intrusion into the official site of the Kosovo information center. The hacker war was declared within Yugoslavia as well. These intrusions are assigned to the group that named itself "The Black Hand" alluding to the namesake organization which overthrew the Dynasty in Serbia in the first years of the 20th century. This organization, due to its activity and secrecy, is considered the first terrorist organization in Serbia, regardless of their self-claimed patriotism. It actively supported the liberating strife of the Serbs on the whole territory of the Balkans and especially in the Austro-Hungarian Monarchy. As an aftermath of their activity, some historians assign the attempt on life of Prince Ferdinand and his wife by "Mlada Bosna" (Young Bosnia) organization. The group of hackers wanted to inherit such a reputation regarding themselves as patriots and liberators. There even existed explanations that by such activities the span of life of this organization has been prolonged and that it is a rare one which has "stood the test of time for over a century".

"The Black Hand" continued its activity. By the end of the October 1998 it raided the site of the Croatian news agency "Vjesnik" and left there a message: " The Black Hand wants to change the false image which orbits the planet that the Serbs are villains." Further they stated that they do not mean war and that they mean no evil. "Vjesnik" immediately reported that the members of the "Black Hand" were discovered and where and how they approached the site. At the same time, claiming that it was done from the computers of two faculties they pointed to Serbian academic network claiming that hackers still travel and act from within it. Mini investigation carried out on the named faculties showed that the news "Vjesnik" had placed about the location of the perpetrators is incorrect. The more their activities were frequent and remarkable the more questions were raised about their identity. The journalists of the Belgrade magazine "Svet Kompjutera" ("The World of Computers"), after the extensive search and by contacting numerous individuals able to bring them

in contact with "The Black Hand", finally succeeded to actually make contact. In one of the Chat-Rooms they chatted with the two of its members and they discovered more about the presentations that were "rearranged" as well as more about the reasons why they had done it. Thus, their main motif was to stand out in the electronic defense of Yugoslavia's interests. Nevertheless, it still remained unknown who they are. Different stories are circling in Serbian hacker underground. According to one of them, this group is not dangerous and has a role of "row-maker" and after their performance the second group, which is dangerous, steps in. Their mysterious members are skilled at changing images, words, letters in the attacked presentation giving it the new meaning and shooting at the other side of coin. Others are close to the view that this group exists but is followed by numerous satellites of less skilled imitators determined to get attention by the public or acquire the "pass" to join the group. And of course, there's the third party that negates the existence of the group.

No matter how true is the assumption, the public was not completely indolent this time. The climate of tacit approval was felt and the idea of the patriotism rather than criminal was borne. The newspaper columns began being filled up by the statements of the "actors". The professional public still mainly ignored this, and was not drawn into the "daily politics".

By these actions, the opportunities were created for the information war to continue.

The war spread to other parts of the country and aimed at other opponents. An interesting case was that of a "flying hacker" that made a mess in one of the cities of Republika Srpska and drew the forces of UNPROFOR out of their minds. Namely, the members of the peacekeeping forces used in their field-situation reports the system based on colors. The green meant - normal situation, the orange - battle readiness and the red- alert. The hacker broke passwords and codes and left only the red color. In several cases it caused the road and street blocking. "The Peacemakers" relaxed only when hacker left the cyberspace of Serbian enclave.

The case that occurred in Croatia, even though it did not originate from the hacker's arsenal, is extremely picturesque. It points out that in this war there are no situations, which will not be used to damage the other side. In January 1996 two PC's and two laptops disappeared from the UN mission in Zagreb. The representative of the mission stated that together with the computers the newest translations statements data of Serbian civilian's referring to the larceny and destruction of Serbian houses in Croatia disappeared, too. The data about the forceful exile of the Serbs by Croatian soldiers, especially from the operation "Storm," were also there. Representative of the UN had been gathering the data for four years. By such a disappearance the evidence on which the actions at the Hag court could be taken vanished.

Even though they were present on the Internet for a short period of time the Yugoslav hackers had used their presence to enter every form of warfare. The Balkans area has always been extremely suitable for warfare, even for the specific one. On the other side, the forms of such a warfare and mutual struggle still hasn't been taken seriously enough let alone explored. It leaves numerous questions unanswered.

III HOW TO GO ON - THE EFFICIENCY AND INEFFICIENCY OF YUGOSLAV LAW?

Yugoslavia has been on the margins of the events of Information technology scene for a long time. Yugoslavia straggled behind in legal regulation of the problem and with the cases related to the application of information technology. In the first half of 1998 by passing the law related to the protection of personal data (*Personal Data Protection Act*), the law related to the topography of integrated circuits (*Topographies of Integrated Circuits protection Act*) and the law related to copyright and related rights (*Copyright and Related Rights Act*) a significant shift had been made. These acts should be followed by the end of the year by The *Telecommunication Act* and by

Criminal Code. Both the laws are in draft (Drakulic, Drakulic, 1999).

The *Criminal Code* will be of special importance for the hacker activity. In June 1998 the Workgroup outlined the draft. According to this version of the Draft a special chapter related to computer crime was provided for. Specifically, the chapter XXXIII is dedicated to **Criminal conduct against the systems for electronic data processing (**the title is covered by the spirit of other groups of criminal activities). This will place Yugoslavia among the countries which included this form of crime in their National Legislature. By such steps the recommendations of the Computer Criminality Resolution of the VII Congress of OUN, XV International Congress for the Criminal Law, Recommendations of the European Union for Criminality related to computers and Recommendations related to realizing the problems in the criminal procedural law related to information technology, as well as other international documents, were accepted. This will probably initiate the permanent tracking and analysis of these specific criminal activities, enabling the novation of the regulations.

In the special chapter, five criminal activities were provided for: 1) the damaging of the computer data and programs 2) computer sabotage 3) computer fraud 4) the interference with the operation of the systems and interference with the networks for electronic data processing 5) unauthorized access to protected systems and networks for electronic data processing. A minimum has been adopted, defined by International Acts.

In later versions the articles were reformulated, both the titles and the contents. The Article 138, The meaning of terms in this Code, has now incorporated the terms: computer data, computer network, computer virus. The concept of document was extended to include computer data, while the form in which an official paper can exist is treated as a document, a letter. The shipment and the document can be in electronic (digital) form. By such definitions the possibilities were created to extend some criminal activities (such as theft, felony, burglary and robbery) with computer modalities.

The title of chapter XXXIII was renamed to **Criminal activities against the security of the computer data.** The terms of the former five activities were reformulated with adequate changes to the contents as well, while three other criminal activities were added. Therefore the following activities are presented in this version of the Draft:

1. Unauthorized use of the computer and computer network;
2. Damage to the computer data and programs;
3. Computer sabotage;
4. Computer fraud;
5. Interference with the operation of the computer data processing and computer network;
6. Unauthorized access to protected computer and computer network;
7. Design of and infecting with computer viruses
8. Prevention or restriction of access to computer network;

In defining the sentence, the spirit of the Code, the character of the activity together with its consequences are being registered. The sentence ranges from fines to three month's imprisonment, as minimum, to 12 year-maximum sentence. In case that the activity is represented by a concommitent criminal activities the imprisonment sentences can be even more strict. The computers and the rest of the equipment used for the conduct of the criminal activity can be confiscated in case they are the property of the perpetrator. If not, they can be confiscated for general security reasons or on moral grounds in case it does not interfere with the rights of the third party to claim the remedy for the damage done by the perpetrator. The obligatory confiscation of the equipment can be regulated on a special basis, the case being criminal activities of the damage made to the computer data and programs and for the design of and infecting with computer viruses.

By the stipulated regulations the new basis for a special form of a protection is being created which

by its nature is extremely strict - criminal. When the Criminal Code is passed it will enable the punishment of the perpetrators of hacker activities. The regulations related to damage of computer data and programs, interference with the computer and network operation and/or unauthorized access to protected computer and computer network could be enforced. The slightest sentence that could be decided upon will be fine (for damages to computer data and programs), while the hardest could be up to five years of imprisonment (for unauthorized access to the computer and network). In case the group or any other union is organized with the aim to conduct criminal activities or if the agreement is made on the execution of the criminal activity it will be sentenced by appropriate sentence. The organizer will be sentenced with imprisonment from three years to lifetime , while the accessory from 6 months to five years. The agreement for the conduct of the criminal activity will be punishable as well. Therefore, the activities of hacker groups such as "The Black Hand" will also be punishable.

The activities of Croatian hackers could be punishable as well if their extradiction is demanded, under the terms of reciprocity. The same principle applies for the Serbian hackers in Croatia according to their Criminal Code. This is hard to imagine because of the antagonism formed by the disintegration of former Yugoslavia.

The situation is much more complex when the site developers are in question, especially for the sites such as the site of Kosovo Liberation Army. The question is being raised whether the content of such a site can be treated as illegal and harmful? If the answer is affirmative then the list of problems is extended by all other problems related to regulation and prevention of presentations with such contents.

However, the activities such as Cyber terrorism or provoking the global information war are not provided for by the Draft of the Criminal Code since it was thought that it is necessary to wait for the solutions and experiences of other countries.

In order to make these regulations efficient it is necessary to provide for the special regulations and principles which will be built into Procedural criminal law, namely in the Criminal Law Act. The law awaits change and recommendations to be included from respective international acts, as well as the solutions from computer developed countries which have already regulated these issues.

What the Yugoslav legal infrastructure is missing are the activities related to self-regulation, as well as the readiness of the police to discover, prosecute and apprehend the perpetrators of criminal activities belonging to the domain of "classical" computer crime, not to mention the crimes related to computer networks. The situation is none the better in the Judiciary. The lack of respective associations (professional and interest), non-governmental organizations and institutions with the aim to track and prevent the occurrences of these activities in question is evident. Disordered organization and inefficiency in terms of protection are also the distinguishing marks of the Yugoslav cyberspace. This can be interpreted as a consequence of Yugoslav absence in terms of isolation from the international scene, but also as a sign of turning towards the national self-proof that it is not straggling behind in the whole shebang.

IV CONCLUSIONS

The appearance of the "Black Hand" group on the Yugoslav hacker scene marked the turning point. The hackers are not isolated individuals anymore and they have grown into organized groups with the aim of "defending the national interest". The fact of the constant danger of international military intervention should not be neglected which can be an additional stimulation to Yugoslav hackers for a still better organization and efficiency. It might be the reason for the mobilization and national

homogenization and it is probable that the hackers from abroad would join in. Isn't the current Balkan situation favorable for the appearance of virtual soldiers, with new weapons and abilities, not directly present on the battlefield?

The question is being raised what will happen to these groups after the situation calms down? Will they cease to exist or will they disappear or they will change the object of the activity? Such objects can be numerous, especially, in the field of electronic economic espionage, which was not yet encountered in Yugoslavia. Maybe it will be a part of the defense of the national interests, that is understandable and not justifiable, due to the economic drop out and difficulties Yugoslavia encountered in the last decade.

REFERENCE

1. Chandler A., The changing definition and image of hackers in popular discourse, International Journal of the Sociology of Law, no. 24/96.

2. Drakulic M., Drakulic R., Hakerska etika u kontekstu profesionalne etike informaticara (The Code of Hackers Ethic in the Context of the Computer Professional Ethic Code), Igalo, Institut "Mihajlo Pupin", 1995.

3. Drakulic M., Osnovi Kompjuterskog prava (Fundamentals of Computer Law), Beograd, DOPIS, 1996.

4. Drakulic R., Drakulic M., Kompjuteri i kriminal (Computers and Crime), Zabljak, Elektrotehnicki fakultet u Beogradu i Elektrotehnicki fakultet u Podgorici, 1999.

5. Levy S., Hackers, New York, Dell, 1995.

6. Sterling B., The Hacker crackdown: Law and disorder on the electronic frontier, Toronto, Bantam Books, 1992.