For Law Enforcement Use Only

Brazil 9/04 Boaz Guttman Adv.

Breaking Digital Evidence in Court – Supplement 2

1. **C.C. 3047/03 State of Israel v. N. Mizrahi: 29 February 2004**

(Ruling, Justice Dr. Avi Tannenbaum, in the Jerusalem Magistrates Court): The acquittal of a person who was accused of unlawfully penetrating the internet site of an intelligence and special operations agency, after the court was convinced that his only intention was to test the security of that site.
Ruling:

2. **The law does not define the term "penetration into computer material". Nowadays, computers are linked and communicate with each other in an assortment of ways. In this kind of situation, it is not always clear what constitutes "permitted penetration", what is "audacious penetration" and what is "unlawful penetration".**

3. **It is not possible to determine conclusively that testing a website's security is always prohibited or always permitted. The legal classification of permitted or prohibited depends on the specific circumstances in which the test was performed, on the goal for which it was performed, and the intention of the person performing the test.**

4. **There is nothing unacceptable when surfers publicize insecure internet sites (particularly internet servers). When such a list is published, it acts as an incentive and a catalyst for those responsible to repair their security shortcomings. To a certain degree, surfers who test website vulnerability are acting for the public good, and if they do so with good, not harmful, intentions, they may even be thanked.**

5. **In terms of public policy, it would be unwise to allow a site-owner to state his preference that no one should test the security of his site. He should certainly not be allowed to request that anyone doing so should be deemed a criminal offender. This is because all the sites on the internet are interlinked and if one is vulnerable, then all of them are vulnerable.**

6. **If the test constitutes an initial stage for exploiting security holes and gaining access to various computers, then such a test constitutes an attempt to commit an offence. However, if the test is a totally autonomous act with no intention of causing damage, then it is acceptable and - on occasion - even welcome.**

7. **We must be cautious in applying the context of ordinary criminal laws to laws relating to the internet world. Ordinary criminal laws relate to a world grounded on clearly defined individual property, a rigid hierarchy, private interests, and actors who first and foremost look out for themselves. The internet is based on partnerships, volunteerism, trust, consensus, and resources available to and shared by all.**

8. **Taking into account all the circumstances surrounding the incident, it is clear that the accused did not commit any offence whatsoever.**

Disclaimer

This is an unofficial translation of the original judgment in Hebrew. The translation is particularly literal, in an attempt to adhere to the original Hebrew wording, even at the expense of style. Consequently, the language may read somewhat different from legal documents written originally in English.

The numbered footnotes are the judges' notes in the judgment itself. Notes marked with a star are the notes of the translator, added for the convenience of the non-Israeli reader.

Translator: Adv.Michael Prawer
e-mail: praver@netvision.net.il

Jerusalem Magistrates Court CC 003047/03

The State of Israel; ; Israeli Police – Department of Prosecutions

by Amos Cohen, Adv. Prosecutor

Vs.

Avi Mizrahi

by Omri Cabiri, Adv. Defendant

Verdict
Of the Hon. Abraham N. Tennenbaum

Introduction

1. The defendant, Mr. Avi Mizrahi (hereinafter: "the defendant") was accused of the offense of attempting to the unauthorized access of computer material, contrary to section 4 of the Computers Law, 5755 (1995) and section 34 of the Penal Law, 5377 (1977).*

Official documents in Israel refer to both the date according to the Hebrew calendar and the date according to the accepted Gregorian Calendar. The Hebrew calendar is based on the ancient tradition which counts the number of years since the creation of the world (according to the book of Genesis)

2. The factual claim, in a nutshell, is that on September 22, 2002 at about 07:25 PM, the defendant attempted to access the website of the Institution for Intelligence and Special Activities (hereinafter: "The Mossad").[1]

I have decided to acquit the defendant of all charges

3. Since this is a legal question based on a complicated technical background, I have concluded that it is impossible to avoid giving a technical explanation, albeit brief. The verdict is therefore divided into the following chapters.

- Initially, we will briefly specify the charge and the course of the litigation.

- We will then present the relatively long detailed technical background required to clarify various matters associated with the case in hand. We will try to be as brief as possible; the points requiring greater elaboration are those which will be of particular importance later on.
- We will analyze the offense of unauthorized access to a computer including the question of whether examining the security measures used in protection of websites is permitted or not.

4. This path is indeed a long one in comparison with regular criminal verdicts, however regarding the case in hand I saw no other choice.

The charge and the course of the litigation

5. On June 19, 2003, an indictment was filed against the defendant, in which it was alleged that he attempted to access computer material without authorization. The factual assertion is that the defendant logged onto the

[1] The address of this Website is http://www.mohr.gov.il all websites that are mentioned in this verdict were last viewed on February 2, 2004.

Mossad's website and tried to access its code but failed to do so since the website was properly secured.

6. The arraignment took place on 14.9.03. followed by several sessions in which evidence was submitted, on 9.10.03, 21.10.03, and 18.12.03

7. The following documents were also submitted.

P/1 - The defendant's statement during interrogation at the police on 19.2.03.
P/2 - Documents from Bezeq and Netvision, which constitute the documents that enabled the identification of the defendant.
P/ 3 - The phone bills of the defendant's brother , Mr. Ronen Kedem, indicating the telephone line by which the connection to the Mossad website was established.
P/4 - A filtered printout of a Snort software.
P/5 - Printouts from fire-wall software which secures the Mossad website. (apparently a Linux machine)

8. The defense filed the following documents:
D/1 - A statement made by the technical director of the Tehila Project, Mr. Arik Wolf (henceforth: "Wolf" or "Tehila Expert")
D/2 - Activity report
D/3 - An expert's opinion on behalf of the defense.

9. The following witnesses testified on behalf of the prosecution:

- Attorney Hagar Rubin of the National Unit of Fraud Investigations. (hereinafter: "The policewoman" or "Rubin")
- Captain Meir Hayun, investigator of computer felonies from the National Unit of Fraud Investigations. (hereinafter: "the policeman" or "Hayun")
- Mr. Arik Wolf, deputy director of Tehila Project. (henceforth: "Wolf")

10. The following witnesses testified on behalf of the defense:
- The defendant;

- Mr. Gadi Guy (hereinafter: “defense’s expert” or “Guy”);
- The defense witness Ms. Meital Gigi, the defendant’s girlfriend (hereinafter: “Meital” or “the girlfriend”)

11. Furthermore, affidavits were filed consensually of Mr. Ofir Arkin, an expert on information security on behalf of the defense and a deposition of a Mossad employee in regard to Mr. Avi Mizrahi's application for a position with the Mossad, through its website. Both them were interrogated on their affidavits.

12. The parties submitted written briefs and the case returned to the court after receiving the defense summations and the prosecution’s response on 29.1.04.

13. As we noted, providing lengthy detailed technical background is unavoidable, but we should caution in advance that space constraints often meant that accuracy was compromised in favor of clarity.

Method of packets, protocols and ports

14. The method of packets is at the core of Internet communication. Any two computers in the net attempting to communicate do so by way of a unique protocol. Every computer connected to the Internet at any given time has an “address” consisting of four numbers between 0 and 255. Every computer that communicates with another computer does so by way of the other computer’s address. The computer sending messages divides the message into small packets. Each packet is numbered and the final address is attached to it.

15. Quite simply: .If computer A wishes to send a message to computer B, then first and foremost, A communicates to B and announces "I’m sending you a message that is made up of 30 sections". Each section is then sent separately to the final address, and attached to each label we find a “label” with the complementary details. Thus, this is a message from computer A to

computer B and the number of the packet is, let us say No. 22 out of 30 packets. Computer B receives the packets separately, arranges them into a complete package and checks if any packets were somehow lost. If a packet is missing, it sends a message to computer A, requesting the missing packet, and that packet is then re-sent.

16. The packet switching method has several advantages, which cannot be overlooked. They relate to the efficiency of the method. The path in which every packet travels is not a direct path from A to B. The packet travels through numerous computers on whichever path happens to be vacant at that time. Every computer within that range which receives the packet from A and sends it towards B, needs time to receive the packet and send it. If the packet is small, the computers can use and send a larger number of packets in the same time period and work together. An important feature of this method is that if there is a deficiency in one packet, it is not necessary to re-send the whole message. Let us compare it to a fax for example. If there is a deficiency in a fax message, the entire message has to be re-sent. In regard to packets, it is sufficient to re-send the missing packet.

17. Obviously, computers must have the capacity of communicating with each other, i.e. if computer B receives a certain packet with an explanation concerning the packet's content, it must know how to read it. To answer that need, numerous different protocols have been developed, enabling every computer to know and understand the meaning of the different packets it receives. At the basis of the Internet lies a protocol called TCP/IP[2]. This protocol allows every computer to understand both the source and the nature of the packet.[3]

18. As we noted, every computer connected to the Internet at any given moment has a unique number. However, even if a computer receives a

[2] Transmission Control Protocol/ Internet Protocol

[3] For the sake of technical accuracy, there is also a protocol called UDP. It does not include a process of constructing direct connection and ascertaining that the material reached its destination and that there is no monitoring of overload or flow. In that protocol the information is simply sent. Its advantage is speed and price.

message, in numerous computers there are parallel procedures. For example, every home computer uses the Internet for surfing, as well as for sending and receiving electronic mail, occasionally downloading information by various means and so on. How does a computer know how to classify the message or packet it receives from another computer?

19. Every computer has what is referred to as *ports*, which handle different procedures. There are many such ports and the computer's operating system moves along from port to port all the time and checks if a message was sent or if there's a certain request from a certain port. A port which allows activity is called an "open" port.[4]

20. In order to facilitate the writing of new programs and cooperation between computers, these ports have numbers, agreed upon in advance. Port 80, for example, serves the various browsers for the purpose of surfing the Internet, port 25 is allocated for sending electronic mail, port 110 to receiving electronic mail and so on.

Names, numbers, allocations and surfing the Internet

21. As we explained, each computer connected to the Internet has a unique number. However, the public is utterly unfamiliar with these numbers, though it is familiar with names of websites. For example, the courts' website is www.court.gov.il. Where has the number gone?

22. The answer is that at the early stages of the development of the Internet, it transpired that it was much easier to remember names than four random numbers. For that need, there are "name servers." (Here, like in any other place, a server refers to computer that provides service.)[5] When we type the name of the desired website , there are name servers to whom our computer

[4] For clarification, we have given a somewhat simplistic definition. Actually there are ports known to all (and access to them should be monitored), there are registered ports and there are dynamic ports. Details about them can be found online at: http://www.iana.org/port-numbers

[5] Those are called DNS – Domain Name System

sends the name of the website and they return the number. Thus, there is a quasi "translation" of known names into numbers. For example, the number of the Mossad's website is 147.237.72.43 and the court's site is 10.1.1.48.

23. A body known as ICANN is charged with the allocation of unique numbers and names of every computer.[6] It should be noted that these numbers are not always permanent. For example, each Internet provider receives an inventory of numbers. When one of the subscribers connects to the provider, he receives one of the numbers allocated to the Internet provider, on a temporary basis, and that number serves him for the duration of the surfing session. When the subscriber disconnects, that number becomes free and another subscriber who connected through the provider will receive the available number. Unlike home users, servers have a permanent address. This is because many people have resort to these servers and a permanent address saves tremendous resources.

24. We will now briefly explain what happens when we surf in a certain website. Our computer sends a message to the computer that contains the website (called an Internet server or a website server). Using the familiar protocol sent from the website, our computer requests the website server to send it information. The information, also sent in form of packets, is operated by the browser and this enables us to view the website. In other words, there is no physical "place" or "site" to which we enter. What we have is the interaction between our computer and the website server, which sends the material we request.

<u>The theoretical principles of the Internet</u>

25. It should be clear from the foregoing that for the Internet to work, many agreements are needed. However, the theoreticians of the Internet in its early stages had even broader demands. Their vision of the Internet was that it would be the "mother of all computer networks" in the world. A network

[6] Internet Corporation for Assigned Names and Numbers – an international body which operates for no profit. Its Internet address is http://www.icann.org

to which every computer, or, to be more precise, every computer network would be able to log on to (hereinafter, we will refer to a computer or a network, although in most cases networks are those that are connected to the Internet.)

26. The founders of the Internet wished to set a few principal rules.

27. First, every network connected to the Internet would be able to connect to the Internet and any other network without the need to change anything in it, i.e., every computer network in the world, or any large computer for that matter, would be able to connect through the Internet.

28. Secondly, the transfer of information in the Internet should be based on maximal efficiency. If a certain packet does not reach its final destination, the source is informed shortly thereafter, and a new packet is sent.

29. Thirdly, "black boxes" would be the primary tool for a connection between networks. These black boxes would receive information and transfer it on to the requested address without "touching" the information and without knowing its content. In other words, if computer A sends a message to computer B through a network of computers, no computer on the way would bother to read the message. This mediating computer will receive the message, check where it should be sent on to, and will send it on without dealing it with it too much. By the way, these black boxes subsequently became gateway routers.

30. Fourthly, and perhaps most importantly, the principle was that there would be no central control or method of controlling the Internet in any way, i.e. networks can connect to each other without anyone being able to control the final outcome.[7]

[7] About these principles and the history of the Internet, see http://www.isoc.org/Internet/history/brief.shtml

31. It should be noted, that these principles require a broad consent among all networks, computers and users. However, once this consent was established, the Internet became stabilized and almost immune to damage.

Security holes, fire walls and security software

32. A prominent matter not considered by the Internet founders was the question of security. The Internet was constructed and maintained based on the idea of scientists who were unconcerned with its commercial uses. They regarded the Internet as a common resource for the entire public and built the its components accordingly. Considerations of security, safety and possibilities of abuse were not the primary considerations of those engineers and computer experts. This becomes apparent when we see a few of the deficiencies and problems that can be caused by users, some of which we will explain in view of their relevance to our case.

33. As we have said, every computer receives packets and composes them into complete messages. However, what happens when a computer receives packets at a rate in which it cannot handle? Of course, every computer has a buffer in which it can store the packets awaiting treatment. But, what happens when the accumulated packets exceed the volume of the buffer? If, for example, a computer can treat 4000 packets per second, what happens when 20,000 packets per second are sent? The answer is that in this case the packets will be lost without treatment and will disappear. Theoretically, of course, the sending computer should receive a message to send the necessary packet again but if an overload occurs, that packet too will remain untreated. This principle is the basis for one of the best known forms of attacks on the Internet, called DOS (Denial of service).[8]

34. An Internet website server cannot serve more than a limited amount of users. If, for example, 100,000 users try simultaneously to connect to the

[8] This is not the place to explain the technical background however, sometimes an attack on a computer by an overflow of information (buffer overflow) is just a first step in taking control over the computer.

[Israeli] courts' website, it is reasonable to assume that most of them will not be able to connect at all. Let us observe what happens. We will assume that an Internet server can receive 4,000 requests at any given time. If at a particular moment it receives 100,000 requests, then 96,000 of them will not receive any service. Moreover, even if those 96,000 were to stand in “line” to get service, then too they will not receive any service. This is because all browsers and surfing software are programmed to wait a certain period of time and if they don’t receive the service, they return to the sending computer and announce that the action failed.

35. Returning to the point made in regard to attacks on a computer. A person intent on attacking a certain website need only send a larger number of service requests than the website can provide. One method of sending a huge number of service request is to take control of computers and program them to simultaneously send service requests to the server they wish to “topple.”

36. Of course, against any attack there is a defense and vice versa. The large servers are programmed so that when receiving an unreasonable amount of requests from a certain address, they can automatically block that address and ignore all packets arriving from it.

37. However, naturally there are many “security gaps”. As noted above, the Internet comprises numerous different servers, different networks, different applications different software, etc. A security gap/deficiency for our purposes is a situation in which a person intent on causing damage can exploit an opportunity to inflict damage on different computers. Such damages are found in almost any computer system. However, a gap that can be exploited in a Linux system cannot necessarily be exploited on a Windows system. Damage caused to one mail program will not cause damage to other mail programs and so on. In any case, there are a huge number of such security gaps. In Windows alone (in all its versions), 119 security gaps were found in 2003 alone.

Fire walls and active and passive security check programs

38. In order to avoid attacks and exploitation of security gaps, various means were developed. The primary ones are the fire walls and programs for security checks. The program called "Fire Wall" is a security program installed between the secured network and the Internet. The role of the wall is to monitor the incoming packets and refuse to receive other packets, all in accordance with the policy of the security manager of the network. This protection is somewhat aggressive, and not necessarily sophisticated. A network manager can, for example, decide that his network will not receive any electronic mails. The way to do so is simple. Every packet directed to port 110 will simply not be received. The network will remove it and ignore it.

39. However, fire-walls are not sufficient since there may also be "legitimate" packets that succeed in penetrating the portion the network and inflicting damage. A number of programs handle this. Those programs try to identify patterns in the behavior of the packets and the computers (to be more precise, the addresses) that send requests to the network. These installments are usually passive programs, which operate in the background, and their role is to warn those responsible for the security of the possibility of an attack, or of "suspicious activity" in the network.

40. The most well known monitoring program is Snort software, which is a freebie software with an open code. i.e. the community of programmers the world over provide each other free assistance in order to develop it and solve problems in it.[9]

41. The Snort software is programmed to identify attacks or unauthorized accesses, as opposed to a fire-wall, which is intended to block such attacks. The emphasis in Snort software is on identification and not blockage. There are those who install it outside the network before the fire wall in order to identify attacks in their early stages, including unsuccessful ones; others

[9] The Snort can be found at: http://www.snort.org

install it after the fire wall in case of a breaking into the network.[10] The meticulous ones place it both before and after the various genres of fire wall.

42. In addition to fire walls and passive programs there are also active programs that examine various security failures. How does a website owner know if his website is secured? Theoretically, the answer is simple. He must examine the current list of known security failures, looking for every particular gap, and every kind of failure, in order to ascertain whether that particular failure is present in the computer. If a failure is found then a method of treatment must be decided upon, but the initial stage is to check all those possibilities.[11]

43. The problem is that security gaps are dynamic and changing. Any self-respecting company that finds a failure in its products immediately sends a correction to its clients. For example, Microsoft regularly places security patches on its website to repair gaps that were discovered. Moreover, there are numerous programs, different computers, rare operating systems, etc. A single program encompassing all of the failures discovered is unpractical.

44. Actually, there are freebie programs and commercial programs. Usually, commercial programs are more efficient than the freebies. It should be noted, that in order for a security checking program to be effective, it must be updated regularly; to be more precise, it should be updated daily and sometimes even more than once a day. It needs to add details, delete details, and check various operating systems on different platforms and so on. Such task of updating is usually difficult. As of today, there are no such freebie programs, except a program called Nesus, which is also updated often by a community of programmers who do free of charge.

---

[10] Another benefit of placing the Snort after a fire wall is identifying illegitimate patterns of legal users in the Internet. In other words, it is possible to follow inappropriate behavior of legal users.

[11] Security check programs need to check which services are performed by the server, and then check if that server can be manipulated by a security hole. To do that, they check which ports in the computer are “open”, in order to identify which services are preformed by the server because the ports relevant to those services would be “open”. Therefore they usually start by checking the ports in a procedure called port scanning. The American law often relates to port scanning.

45. On the other hand, there are expensive commercial programs that perform these kinds of checks, costing tens of thousands of dollars. The accepted view is that these programs are superior in regard in terms of both security and checking. In other words, they check failures up to the stage of the last key stroke (i.e. they are capable of examining every possible kind of damage, should the checker wish to do so]. Despite the high prices there are websites such as commercial websites or banks websites for which such expense are both economically worthwhile and essential.

46. It should be remembered that both commercial programs and freebies are just programs for security failures checks. To exploit a failure in order to initiate an attack on a website, far more comprehensive knowledge is required. By way of metaphor (admittedly, not a very successful one), the fact that anyone can see through a car window whether or nor there's a car alarm installed, is not sufficient to enable breaking into the car since one must know how to break the lock and start the car without a key.

47. Let us give one example relevant to the case in hand. As we explained, in every computer there are numerous ports, which are identified by programs and procedures in the computer. However, how will a computer react if it receives a packet addressed to a non-existent port? Usually this is port 0 which does not have a role and does not exist. It's possible that the system would simply ignore it completely, but it is also possible that the system would spend time considering what to do with it. There have been systems that spent a great deal of time considering what to do with such a packet, time that increases as the amount of packets grows. As such, if it takes the computer half a second to consider how to handle the first packet that was sent to the wrong address, then when 100 packets are sent it would take not (100x0.5 second|) but (100x1 second), i.e. the more packets sent to a non-existing port, the more it confuses the system, until it collapses.

48. Theoretically, there is a security failure here, but practically this is just the first stage towards the exploitation of such a failure. Because, even if one

knows that it is possible to exploit such a failure, one still requires computers to send a huge number of messages to port 0 (the scale here is millions and billions). If such messages are not sent, then even if there is a security failure, it cannot be exploited.

49. It should be remembered, that even where such a failure exists, most website owners will not bother to repair it. If it is a website of a high school student glorifying himself and presenting photos of his family members, why would he bother to secure it? From his point of view, if anyone is willing to make such an effort that would cause the website to collapse for a certain period of time, he would regard it as a compliment. He would certainly not bother investing in fire-walls and/or the various types of security programs, inter-alia, because the measures and programs for security assurance are not cheap. Not every website owner can afford such equipment.

50. This example is characteristic of most security failures. Even if there is a possibility of inflicting damage to the website, there will be many who would not bother to correct it. As far as they are concerned, if there is damage, it is always temporary damage. And even if the website is completely destroyed, they will re-build it. We must remind ourselves again. When using the word "site" we are only referring to a computer - not necessarily a strong or a new one – that is connected to several lines and that sends information at people's request. Usually, the maximal damage caused by a collapse is recoverable from a backup.

After the lengthy background we shall move on to the legal framework.

<u>The Legal Background – The Offense of Accessing a Computer in Israeli Law</u>

51. Defendant was charged with violating section 4 of the Computers Law of1995. This section appears in chapter B which discusses computer offense and its phrasing is:

4. If a person unlawfully accessed [penetrated] computer material in a computer, then he shall be liable to three years imprisonment; for this purpose, "penetration of computer material" – penetration by means of communication, by connection to the computer, or by its operation, but not including penetration of computer material which constitutes monitoring under the Wiretapping Law 5739-1979.

Computer material. For the purpose of the computers law is defined in section 1 , which is the definitions section as:

"Computer material" – software or information

Software is also defined in the definition section:

"Software" - A set of orders expressed in computer reading language and capable of causing a computer to function or a computer to perform an operation, and embodied, contained or embedded in a device or an item, via electronic, electromagnetic, electrochemical, electro-optic means or via other means, or it is implanted or encapsulated in the computer in any manner whatsoever, or it is separate from it, and all if it is not designated for use in an auxiliary computer only.

<u>The problem in the definition of "penetration" and "unlawful"</u>

52. There is no adequate definition of the term "computer penetration". The very concept of "penetration" is a concept involving a physical world where objects have volume and mass. Penetration in the physical world means passing a border/fence/wall/barrier and/or any other tangible area. In order to penetrate there must be borders, which are circumvented and exceeded. What then is the meaning of penetration in regard to a computer?

53. The section does define **"penetration to computer material": as penetration by means of communication, or connection to the computer, or by its operation.** But, there is no clear definition of "penetration". The term "penetration" is defined by the use of the word

penetration, and hence the definition does not promote our inquiry. Is every connection to a computer a penetration? Does every interactive dialogue between computer A and computer B constitute a "penetration" of computer A to computer B? What are the boundaries that need to be passed in order to "penetrate"?

54. This of course, is only the first step – that not all penetrations are forbidden: only the “unlawful" penetrations that are prohibited. Even after we succeed in defining "penetration", the question is what is the meaning of the term "unlawful"? Does any case in which the website owner did not desire that kind of connection, constitute an unlawful penetration [or unauthorized access]? Is it sufficient that the penetration did not take place in accordance with the contract (specified or general) between the owner of the penetrated computer and the penetrator, in order to be considered unlawful? Is it even possible to relate to consensual civil norms? Is it necessary to have an explicit approval in order to have a lawful penetration? And so on.

The approaches in Israel and the world in regard to the offense of penetration

55. As noted by the prosecutor in his instructive summations, there are currently two approaches in the world regarding the question of penetrating a computer. The American approach is narrower and allows more “free dialogue” among computers in the Internet. American case law and legislation allow a sort of a penetration in principle, and penetration is only unlawful if accompanied by unauthorized use or infliction of damage on the computer. Moreover, in American law there is also the requirement of intent to commit a offense and that too is an extension.[12] The European approach (also adopted by other countries) is broader: accordingly: penetration to the computer itself is a offense regardless of any damage caused.

[12] The American law has undergone changes lately due to the September 11th terror attacks and laws legislated following it. However, this is not the place to discuss it.

56. I agree with the prosecution that a reasonable interpretation of the Israeli law is that the penetration to a computer itself is an offense . The phrasing of the law is clear and unambiguous and accordingly, the actual penetration itself is forbidden. This Court explicitly ruled in another matter that deleting computer material is forbidden regardless of the damage caused.[13] And, by analogy from the case of deletion, we can make an inference to penetration. It is obvious that in the Israeli law there is no need for damage to be inflicted. But, what is a "penetration"?

57. The prosecution regards Europe as the relevant source for comparison, but there too there are different schools. Some limit the definition of penetration to cases in which the penetrator passes through some kind of a protection system. Norwegian law refers to: “Breaking a protective device”. Polish law refers to: “Special protection for that information”. Dutch law refers to :”Breaking through security system.” Italian law refers to “Protected by security measures” and so on.[14] Israeli law does not contain these specifications, and its definition of penetration is not clear.

58. However, this is not the question in hand. The question in hand is whether or not a security check of a website is permitted or not. Is this action welcome and lawful or to the very least not forbidden, or does it constitute an unlawful attempt to penetrate as the prosecution claims?

<u>The general complexity of a offense of computer penetration</u>

59. As Professor Orin Kerr recently argued, there is ambiguity in the legal definition of unauthorized access [referred to here as "computer penetration"].[15] Professor Kerr is puzzled by the fact that while the majority of countries have legislated laws that forbid unauthorized access, there is still no clear perception regarding the question of what constitutes unauthorized

[13] CrF 3813/99 *The State if Israel v Oded Refaeli,* Magistrate Court Cases, volume 16 p. 861
[14] The laws of various countries and their translations into English, see http://www.mosstingrett.no/info/legal.html
[15] Orin S. Kerr "Cybercrime's scope: Interpreting "access" and "Authorization" in computer misuse statutes" New York University Law Review (November 2003) Vol. 78 No. 5 pp. 1596-1668.

access and what are its primary characteristics. Hence, Professor Kerr made an interesting proposal, partially based on the rationale underlying most of the current computer legislation.

60. The Computer Law of 1995 was legislated at a time when the working environment was different. During the pre-Internet period and even for some time thereafter, any connection to a computer was effected by a username backed by an access password. In order to connect, one had to communicate, type in a username and a password, and only then the connection would be activated. At that time, it was very clear what an unauthorized access was. An unauthorized access meant penetration that bypassed the need for a username and a password, usually by using usernames and passwords of others. There was no need to explain the term.

61. The technological situation today is much different. Computers are connected to each other by peculiar methods. Electronic mail, automatic exchange of contents, music files available for all, television and radio broadcast via the Internet, live Internet cameras and many different applications, are all available for use. Some even operate almost automatically and are transparent to the user. In this situation of a continuous, busy and bustling work environment it is not always clear what constitutes an authorized access, what constitutes impolite access and what constitutes unauthorized access.

62. Professor Kerr argues that today, the term unauthorized access is defined too intuitively. In his view, the term “computer access ” has to be broadened to include any interactive communication between different computers. According to Kerr, in today’s situation of computer interaction, there is almost always a situation of access and the distinction between an authorized access and an unauthorized access must be made on the basis of “unauthorized”. He proposes distinguishing between access that is regulated by a contract between the parties and accesses that bypassed passwords and computer-code based measures. (Regulation by Code versus Regulation by Contract)

63. According to his approach, the fact that a computer owner does not welcome the access is insufficient. The fact that a website owner is not interested in the actions of others is irrelevant to the criminal law. If the penetration succeeded in bypassing obvious defensive means, and it's purpose was to bypass these defensive means, then, and only then does the access become unauthorized.

64. This perception can be debated, and especially his suggestion to omit the element of "access" all together and focus on the legality of the action ("authorized " or "unauthorized", that is the question according to Kerr). However, this is another proof of the complexity of the term "access".

About the problem of perceiving the website as a "place" that can be "penetrated" and inferences made from the criminal law in regard to the civil law

65. Considerable criticism has been voiced in the legal world regarding the metaphor of a website as a place. Some scholars argue that the term "cyberspace" itself is erroneous and damaging. The fact that we see the Internet as a place that can be penetrated causes us to make assumptions in regard to the Internet that are inferred from the tangible world. Thus, we view the Internet as a space in which each website has its own private place, over which it has exclusively ownership. This is completely opposed to the manner in which the Internet was constructed as belonging to the community at large without private ownership or control of its resources.

66. The most prominent of these critics is Professor Dan Hunter. [16] According to Hunter, these erroneous metaphors give rise to what he refers to as the Cyber Enclosure Movement. The perception of the Internet as a place causes us to divide it into portions that are privately owned, while the owners' purpose is primarily profit. But, as Hunter claims, this completely

[16] Dan Hunter "Cyberspace as Place and the Tragedy of the Digital Anticommons" 91 CALIF. L. REV. 439 (2003).

contradicts the principles on which the Internet was built. The net is composed of computers that exchange information packets and voluntarily send such packets from computer to computer. The net was built by thousands of engineers and scientists, who created protocols and cooperated for its success, all free of charge. This trend partially continues today. There are many websites on the net in which owners have uploaded extensive information to and for the entire public and solely for the benefit of the public. This information is massive and diverse. Ranging from thousands of literary creations accessible to all in the Gutenberg Project, [17] ancient maps of Jerusalem,[18] and tens of thousands of websites that operate voluntarily for no profit. According to Hunter, the Cyber Enclosure Movement may produce a situation in which public resources, that are currently taken for granted, will have to be shut down, because it will not be economically viable for individual persons to maintain them.

67. This is not the place to delve into that theoretical analysis. However, for our case it is important to understand that there is a justified criticism of the legal analogies that are made from regular criminal law as it relates to the physical world in regard to actions in the Internet world. While we do not share this opinion it is deserving of our attention.

68. In any case, even if the perception of the website as a place is problematic, it is convenient, and the prosecutor has used it numerous times. The prosecutor repeatedly compared defendant's actions to a person throwing a rock (or a feather) on an iron or a copper wall. (p. 20 in his summations) In another place he compared the defendant to a person knocking on a door, trying to open it, checking the locks etc. (p. 21 in his summations and in other places.)

[17] This is a 30 year old site that contains the full texts of thousand of literary pieces uploaded by volunteers. Its address is http://www.gutenberg.net/index.shtml. (last visited on February 2003).

[18] There are, of course, several sites that present ancient maps of Jerusalem. For example, see: http://maps-of-jerusalem.huji.ac.il/.

69. For the reasons I have mentioned, this analogy is misplaced. If we use a metaphor, a better example will be a driver that is driving on a road that belongs to all, and sees other cars with problems and malfunctions, like a flat tire, smoke issuing from under the engine hood, an open door etc. Another way would be to compare an examination of security measures to a person visiting the museum legally, and in the course of his visit he takes a look at the emergency exits, the museum windows etc. Although it may seem impolite, it is definitely not a criminal act.

Checking the security of a website is not forbidden by itself and depends on the circumstances

70. In light of what has been said thus far, what is the legal status of a security check of a website? Is a person allowed to check the security of a website that does not belong to him?

71. Our conclusion on this matter is simple and unequivocal. It is impossible to definitively determine that a security examination of a website is either always forbidden or always allowed. The legal classification of permitted or forbidden depends on the specific circumstances in which the examination was done, the purpose of the examination, and the examiner's intention. It is impossible to separate it from these circumstances. And, we should emphasize, this is in regard to a security examination and not a search for security gaps as a preliminary stage of an unauthorized access.

72. There is a social benefit gained by websites being examined by surfers and being notified if holes are found. Moreover, I would dare to say that there is nothing wrong with surfers publicly announcing that websites (and mainly Internet servers) are not secured. If such a list is advertised, it provides an incentive and catalyst for those responsible to repair their security gaps. Surfers that examine the vulnerability of websites, to a certain extent, act for the benefit of the public and if they do so in good intentions and not to harm, then they should be commended.

73. To be more precise, it should be remembered that examining a website with a security software is a very easy task to perform. The examiner need do nothing more than type the address of the website into the software, and the program does all the rest. To remove all doubts, this is an act performed hundreds and thousands of times every day on many and various websites. As the security expert, Mr. Ofir Arkin noted, he receives thousands of such warnings every day. (see protocol of 18.12.03 at p. 30, lines 3-5). The prosecution witness, Mr. Erik Wolf, also testified that he experiences hundreds of such attacks every day. (at p. 9, line 26). The witness fairly admitted there are tens of thousands or hundreds of thousands of such "attacks", i.e., this is a general and daily phenomenon.

74. To remove all doubts, we emphasize that the act permitted is a security examination and nothing more. Any act of examination accompanied by an unauthorized access indicates that the examination itself is part of the penetration and will definitely constitute a criminal "attempt".

Why can't a website owner avoid the check by other surfers?

75. A website owner cannot [???לוותר ולגרש–] "expel" surfers who visit his website. From the perspective of public policy, it would be unwise to permit a website owner to publicly declare that he is not interested in any security examinations. Certainly, it shouldn't be possible for him to request that anyone who does so be considered a criminal offender. This is because all websites in the Internet are interconnected and the vulnerability of one website affects the vulnerability of another.

76. As we showed before, one of the most common attacks is called DOS (Denial of Service) and is based on "bombardment" of servers with false service requests until they collapse. However, in order to do so, attackers need to seize control of servers that do not belong to them so that they too can send exceeding service requests, i.e., the attacker will search the Internet for vulnerable servers, so that he can partially seize control over them and compel them to request services from the server under attack.

77. Every vulnerable computer in the net constitutes a threat not only to its owner and content but also to other properly protected computers. This is because it can be used to attack protected websites and servers. In other words, an unsecured server constitutes a threat to other secured servers. The fact that the owner of the unsecured server is not interested in a security examination does not affect the server's threat to secured servers.

78. Consider the example of a virus spreading rapidly through the net. The virus reaches an unprotected computer/network, multiplies itself and sends itself from that computer to the computer's regular recipients. If the computer is not secured, then damage is caused not only to the [unprotected] computer itself but also to other computers that normally communicate with it. Moreover, even if the computer is secured, then damage is still caused by the traffic to and from it being jammed due to an overload. This is also true for what we call spam. If all computers were secured against spam and forbade "spammers" to communicate with them, then the phenomenon would be avoided or at least significantly decreased.

79. Let us look at another example of forging an IP number. Some surfers do not want their IP number to be known (usually, for improper reasons). The attacker sends a packet to the target computer, but the address of packet's origin is not the real address. The target cannot know the origin of the packets since they have traveled through many computers on the way. For that reason there is a defense mechanism that operates routers. These routers check if the address on the packet is indeed the address of the computer it was sent from. The effectiveness of this defense is primarily when the first packet leaves the attacking computer, because only the first router knows which is the real computer. However, if the first router does not operate the defense mechanism, the attacker can forge numbers freely.

80. These examples indicate the interdependency and the collective responsibility of all users in the Internet. In the language of the Talmudic parable, in a somewhat different context: **"Rabbi Shimon Bar Yohai said:**

It is comparable to people were sitting in a boat and one of them took a drill and started drilling underneath him. His friends told him, what are you doing? And he told them, what should you care? Am I not drilling underneath me? And they said that the water is rising and sinking the boat." [19]

81. Anyone who is a pundit in the field knows that the Internet boat depends on all its surfers and all those who are connected to it. The Internet was founded, developed and exists today due to all to those elements that support, help and assure its integrity. A proper and correct public policy must be based on it and help this trend.

How does one know which security check is forbidden and which is allowed and even welcome?

82. As we explained above, the examination itself is not a "penetration". However, in most unauthorized access situations, the examination constitutes a preliminary stage. In order to commit the unauthorized access, the existence of a security gap must first be ascertained. It is true, that in a case of a specific attempt to access without authorization, (like a defined computer virus), the software examines the computer's vulnerability at a specific point only. However, quite often there is a comprehensive attempt to locate all the weak points of a certain computer.

83. If the examination constitutes a preliminary stage in an attempt to access without authorization, then it constitutes an attempted offense . But, if the examination is an independent act, not intended to harm, then it is perfectly legitimate. Consider a case in which a person wishes to perform a business transaction with a website (selling and buying, for example) and wants to check whether or not the website is properly secured. What harm can there be if the user runs a software examination on that website?

[19] Va'ikra Raba (Vilna), Chapter 4, 4-5. *s.v.* Tni Hezkia

84. On the other hand, we might find that the examined computer also contains attacking programs that do not just check but also cause harm; there might be signs that after the examination, other actions took place; if the examination constituted a phase; then, the examination itself constituted a forbidden attempt. As explained above, there is a substantial difference between examining for security gaps, and actually exploiting them, so in fact it is a difficult to make a mistake.

85. It should be noted that I have not dealt with the necessary mens rea element, although in my view, the same mens rea required in any criminal offense , namely, sections 19-20 of the Penal Law, is valid here as well.

Regarding the need to interpret the Computers Law in a manner compatible with the spirit and structure of the Internet

86. There are fierce debates about the purpose of legislation. Some argue that the law should reflect the values of the society; the economic analysis of law approach argues that its purpose is to maximize public benefits, and Marxists argue that its purpose is to help the ruling class to perpetuate its power. And, this is not even the tip of the iceberg of the variety of opinions that deal with the topic. But, common to all those opinions, is the understanding that law cannot be separated from the reality in which it is applied.

87. Our position in principle is that we should be cautious when drawing analogies from regular criminal laws for purposes of laws dealing the Internet world. The ordinary criminal laws relate to a world based on a clear and defined private property, private interests and players who are first and foremost concerned about themselves. The Internet is based on cooperation, volunteering, trust, consent and resources, which are freely available for all.[20]

[20] On the repercussions of the Internet on the substantive law see: A. Tennenbaum "The Repercussions of the Internet on the Substantive Law", *Shaarei Mishpat* (2) Kislev, 5758 (December 1997) pp.133-188. The article is online at several websites, see:

88. Quite naturally, the coin has two sides. The same trust in the Internet community that caused it to thrive and blossom, also has negative ramifications. The openness and cooperation can be abused, and indeed, they are often abused. The phenomenon of spam is an explicit example of an abuse of the trust of users. Because of the architecture of the Internet and the equality of resource allocation, we are in a situation in which a large percentage of electronic mail in the net is made up of spam that no one asked to receive, and which is forced upon the public

89. In regard to the Internet, legislation should be interpreted in a way that helps the Internet to continue its progress for the benefit of the public and not in a way that limits, interferes with, and impedes such progress.

90. According to this principle, security examinations of websites are a positive action in principle, and, in principle should be encouraged; we should therefore avoid discouraging such acts, even though they may seem contemptuous with regard to website owners. However, we must stress that that this is not just a matter of adopting a forgiving approach. The very same principle will demand firm and even aggressive interpretation with respect to those who damage the infrastructure of the Internet, an infrastructure which, as we have mentioned, is very vulnerable because of the foundations of cooperation, partnership and trust upon the Internet is built. Those who spread viruses and harmful content should be punished strictly, and the correct interpretation will be one that broadens their responsibility and not let them evade liability on the basis of sundry excuses.

<u>From theory to practice – What did the Accused do in the case before us?</u>

91. We must, first, be reminded of the indictment and we shall quote it in full.

---

http://www.mishpat.ac.il/courses/tennenbaum/index/main/articles/data/Internet%20Implicitions-Heb.pdf

1. **On September 22, 2002, at about 19:25 the defendant unlawfully penetrated computer material from his home in Jerusalem.**
2. **The defendant connected by communicating to the website of The Institute for Special Activities (The Mossad) of the State of Israel, address: www.mohr.gov.il (henceforth: the website)**
3. **The defendant activated penetrating and deciphering programs against the website, which sent many attempts at deciphering the website's various defense codes.**
4. **The defendant even produced a printout of the results of the "attack" that enables knowledge of the website's security failures.**
5. **The defendant requested assistance on the Internet in interpreting the data printout, which he could not interpret himself. The defendant performed the foregoing despite his presumption that it was illegal.**

92. I think that the prosecution's claim about deciphering and penetrating programs that send numerous attempts at deciphering the many and varied defense codes are somewhat exaggerated, and I shall not elaborate.

93. In light of the testimonies in this case I make the following factual findings:

- The defendant is not a computer security pundit nor is he presuming to be one.
- Over a long period, the defendant was interested in joining the Mossad. When the Mossad's website went online, the defendant logged into it for the purpose of joining the Mossad, and suspected that it was an insecure website. There are no means in the website to communicate with its managers except for the application form, so that this could not have been verified by way of the website's managers.
- The defendant in our case, turned to a website that deals, among other things, with computer security (and their unauthorized access as well) and downloaded from it a freebie program to examine security failures. He chose that specific program since according to the website it was very popular and the number of downloads was the highest. It is an anonymous program, which the defendant did not know much about. As

with most programs in this category, all that is required is primarily to type in the website's address and click "start" and the program does the rest.

- The program produced a certain log (output/printout), which the defendant could not understand. He turned to a number of Internet chat rooms for assistance but received no reply.
- When the accused gave up, he abandoned the entire matter, and even deleted the program.

94. It should be noted that the parties argued extensively over certain issues, but I saw no substantive reason to address these claims. For example, there was a serious dispute regarding whether the website was secure on particular days that preceded the act of the defendant (though there is no dispute that the website was secured on the day the defendant logged into it). The prosecution, for instance, argued that the website was secure and the defendant had clear knowledge of that fact. The defense, on the other hand, claimed that the website was not secured. Personally, I have no doubt that the website was secure, but it is unclear to what extent was the defendant aware of it, and in any case, it makes no difference.

95. The parties argued extensively over the question of whether or not the defendant registered in the website with the intention of joining the Mossad. The prosecution claims that the fact that he did not register shows that he was not concerned about security issues. The defense argued that the defendant did in fact register. It was precisely because of his intention to register and thereby disclose private details, that he wished to know whether or not the website to which he was sending his details was secured or not. I do not regard this point as being of central importance.

96. My conclusion is that the defendant indeed thought that the website was not secure and that was his reason for attempting to examine it. The prosecution asserts that the defendant wished to examine the site in order to later impress the people of the Mossad or any other organization. The defense claims that the defendant did it in order to make sure that the details that he intended to send were indeed secure. It is reasonable to assume that

both parties are right to an extent, but I did not find these points relevant in light of the conclusion I have reached, which will be specified forthwith.

Examples of examinations performed by the program used by the defendant

97. We will not get into all the failures examined by the program, but we will present three of them as an example. On page 1 of P/1 it can be seen how 3 attempts were registered to enter port 0. As we have mentioned, sending a pocket to port 0 can create problems and most security check programs do so.

98. Another example is on the last line of page 1 in which the command *cmd.exe* appears. This command checks if the system is accessible from outside the operating system *dos*. *Cmd* is a legitimate and legal command in every Windows system that brings the user straight into the *dos* level (an operating system that preceded Windows but installed in it). Whoever enters *dos* can perform various harmful actions. The novelty here, is that this command checks whether *dos* can be accessed from outside the website. Again, like in any security failure, this is insufficient. Even if we know that we can access from outside the *dos* operating system, one must be an expert with profound understanding to know whether damage can be inflicted and what kind of damage.

99. Another example is at line 17 from the bottom that uses *web-misc webhits.exe.* This line checks if it is possible to activate the command *webhits* from outside the website. This command is associated with web applications and it indeed it can be activated from the outside and if the activator is an expert, then he can cause certain applications to be exposed to him. Theoretically, if this information regards credit cards in an application that deals with purchasing, then the expert can use it to find out numbers of the credit cards. It should be noted, this check is merely the first step, and deep knowledge is required in order to move on. Another point too should be noted: when dealing with a website that does not have web-based

transactions or web-based applications, the website owner will not bother to fix that "gap", because it does not concern him.

100. My impression is that the program is not as effective as the prosecution would have us determine. However, it is a program that allows examining for security failures, that was good for its time. This is probably the reason why the number of downloads of that program was the greatest.

How did the police track down the defendant?

101. In order to remove all doubt, the Mossad's website is not located on the Mossad's computer and is unrelated to it (which is the way it should be). This website is located on the governmental ministries' server site. (Tehila). Tehila is a body that maintains many governmental websites and as such it has its own security mechanisms. Among these means there is a fire wall program[21] and also a Snort program. The Snort program indicated the features of a security failure examination as indicated in the printout that was submitted to me in that matter P/4.

102. These characteristics found by the program were sent from the IP address 62.0.144.27 (as can be seen in printouts P/4 and P/5). This is an Israeli address and, as it transpired, it belongs to the Internet provider Netvision (henceforth: "the provider"). The provider randomly hands out addresses to clients that connect through it (each time to a different client but of course, no two clients can have the same number simultaneously).

103. The provider has a regular registration of clients that received IP numbers at anytime, including this number. The police turned to the provider and by a court warrant, requested the identity of the person who used that number on that day (The user name and the telephone number he used). Netvision handed the user's details, the telephone company (Bezeq) handed

[21] As can be seen in the printout, this is a Linux machine fire wall

the telephone line's details and that is how the defendant, who did not even try to hide, was found.

The unequivocal conclusion – the defendant did not commit any offense

104. From all the circumstances surrounding the case, it is obvious that the defendant committed no offense. He did not attempt to conceal anything and from the very beginning he cooperated fully with the investigators. The defendant pleaded incessantly from the start that all he wished to do was to examine whether or not the Mossad's website was properly secured. No suspicious material or programs that could find and exploit security holes were recovered from the defendant. All the prosecution knows about the software he used, we have learnt from him, and him only, since to this day it is not clear which program he used. I will add that the defendant is a far cry from being a security/penetrating expert, nor did he purport to be one. The fact that he performed all of his actions in the open, making no attempt to conceal his address (the Internet one) is also indicated of the absence of criminal culpability.

105. It should be stressed that had the defendant been caught lying, or had he concealed details from his investigators or if harmful penetrating software had been found among his possessions, it could have been considered to be a circumstance inveighing against him, and as proof that this was an attempted penetration. However, none of these was found.

106. I was impressed by the defendant and heard his witnesses and I hereby make an unqualified factual determination that the defendant did not penetrate but rather that he attempted to examine the website's security. Again, I do not conclude conclusively whether he did so in order to impress the website's managers (as the prosecution claims) or because he wanted to verify that he was sending his details to a secured website (as he claims). It is reasonable to assume that the truth is somewhere in between but this is irrelevant for our purposes.

107. The defense elaborated on the question of the mens rea required for the commission of the offense. However, in light of my factual conclusions that there was no intent, there is no need to discuss the question.

In view of which, the defendant should be acquitted.

Is the defendant entitled to the abuse of process protection ?

108. The parties argued at length argued over the question of abuse of process and this issue should be addressed, even if only out of respect for them. While it wasn't stated explicitly, it is obvious for both sides that if it weren't the Mossad's website, but rather the Department of Fishing and Water Agriculture in the Ministry of Agriculture or a website about the Weekly Torah Portion in the Department of Jewish Law in the Justice Department,[22] no one would have even cast a glance at the defendant, let alone to make the effort to search for the defendant, find him, interrogate him and prosecute him.

109. The essence of the defense's arguments regarding that point is clear and simple. Hundreds of such attacks take place every day on governmental websites, why of all these attacks did the prosecution focus on Avi Mizrachi? (The truth is that the defense was not accurate and there are thousands if not tens of thousands of such attacks every day). However (and this was hinted at by the defense), someone wished to satisfy the public by making a point that anyone dealing with the Mossad would pay a heavy price, and it was just the defendant's bad lack to be made an example of.

110. The essence of the prosecution's arguments regarding that point is also simple. It is impossible to enforce the law on everyone and the police did its best. Most attacks are committed from outside of the country and in general they are relatively severe attacks. As for our case, in regard to a website of

[22] Their addresses are http://www.mop-zafon.org.il/fish/index.html and http://www.justice.gov.il/MOJHeb/MishpatIvri/ParashotShavua/ respectfully and we certainly do not undermine the significance of these bodies.

such serious security repercussions, it is not surprising that the decision was made to prosecute this case to the full extent of the law.

111. The abuse of process defense is an awkward one in the world of justice. In regard to this defense it is irrelevant if the defendant has committed the offense or not. Moreover, this defense does not appear in legislations and it is entirely created by the case law.

112. There are three accepted models in the issue of abuse of process. The first model is the model of "inherent power". According to that model, the court has inherent power to examine whether or not there was an exploitation of the criminal justice system for unsuitable purposes. The court is the one responsible to ensure that no person or body, including State authorities exploits the criminal justice system for unsuitable purposes.

113. The second model is called the "administrative model". According to that model the court analyzes the discretion of the administrative power in its decision to prosecute a person and its conduct throughout the trial. Usually, administrative considerations are reviewed by a [special] court [empowered to] adjudicate such petitions, but not here. The uniqueness of the abuse of process defense is that in some instances the injustice is so extreme, that the forum that adjudicates the criminal case should also review the administrative discretion in deciding to prosecute.

114. The third and final model is the constitutional model, whereby in extreme cases there should be an examination as to whether the right to due process was violated. If indeed it was violated, further examination is required regarding whether, despite that violation, the criminal procedure should continue. It is true that in Israeli law we do not have the right to a abuse of process, however, the regular claim made of late in our law is that this right is derived from Basic Law: Human Dignity and Liberty.[23]

[23] About the three models, see Isgav Nakdimon's Book, "Abuse of Process Defense" , Nevo Publishing 2003

115. While there are indeed some scholars who regard the recognition of such a defense as evidence of progress,[24] this Court takes a decidedly different view. A great deal of discomfort attaches to the abuse of process defense. After all, there is a law in Israel, and our charge is the rule of law. If a person violates the law, and is unanimously regarded as having committed that violation, where does the court get the freedom to determine that the criminal procedures against him should be dropped? Even if the authority acted illegally at one point or another, this is unrelated to the defendant's violation of the law. Experience shows that where justice is trampled upon, the victim has the benefit of a number of legal defenses that have been developed over the years. There is no need to add another, poorly defined defense. Moreover, courts have been criticized (rightly, perhaps) for usurping authority that was not granted to them and I am not convinced that it is necessary to elaborate.

116. Reality shows that claims regarding abuse of process are brought up by those who are remote from being weak and oppressed. Abuse of process claims were brought up, of all trials, during the "bankers" trial (CA [Criminal Appeal] **2910/94, Yefet et al. v. The State of Israel 84 d[2] p. 221**). Irrespective of our opinion of that trial and its outcome, no one could disagree that the defendants were a long way away from being a part of the weaker part of society. Should that sector of defendants, of all sectors, be the one in need for a unique defense of abuse of process?

117. There are respectable opinions that argue that such a defense should have never been established. And now, since it has already been established, it should only be applied in times of crisis. This court belongs to the school that argues that a abuse of process defense should be asserted only in extreme and unusual cases. Cases in which the injustice is extreme. Cases in which any bystander would agree that the injustice is blatant and harsh. This is not the case before us. The prosecution clearly stated that if it

[24] From reading Nakdomin's books it seems that he thinks so as well. This is probably also Segal and Zamir's view in their relatively new article. (Prof. Ze'ev Segal and Avi Zamir, "Abuse of Process Defense as Grounds for Dismissal of Indictment – on the Borderline between Criminal Justice and Public Justice", The Counsel 47, volume A pp. 42-76)

were possible they would prosecute many others, however resources are limited and therefore it is impossible to do so. There is no harm caused by prosecuting a single case solely in order to teach the public that such an act is forbidden. My inclination is therefore to determine that the defendant's right of due process was not breached and there is no point in elaborating, in light of our previous conclusion.

Conclusion

118. Summing up, after hearing the parties and in light of the evidence and testimonies I have decided to acquit the defendant of all charges.

At this opportunity, I would like to commend the prosecutor, attorney Amos Cohen and the defense attorney, Omri Cabiri for conducting this trial efficiently and fairly without amassing procedural difficulties on each other (which would have been exceedingly easy in this case)

Right of appeal within 45 days to the District Court

The secretariat will send a copy of the verdict to both sides.

Given in my chambers in the parties' absence' and with their consent today, Sunday 7 Adar, 5764 (February 29, 2004)

Abraham N. Tennenbaum
Judge