IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	Criminal No.
v.	)	
	)	18 U.S.C. § 1030
GARY MCKINNON,	)	Fraud and Related Activity in Connection
	)	with Computers
Defendant	)	(Counts 1 through 7)
	)	

INDICTMENT

NOVEMBER 2002 Term - At Alexandria

Introduction

THE GRAND JURY CHARGES THAT:

1. At all times material to this Indictment:

a. The United States Army is a military department of the United States Government, which provides military forces to defend the United States and any occupied territory and to overcome any aggressor that imperils the peace and security of the United States.

b. The Department of the Navy is a military department of the United States Government, which provides naval forces that defend the United States and are capable of winning wars, deterring aggression and maintaining the freedom of the seas.

c. The Department of the Air Force is a military department of the United States Government, which provides military forces that defend the United States through the control and exploitation of air and space.

d. The Department of Defense is a department of the United States Government and is responsible for providing military forces that defend the United States and any occupied area, and overcome any aggressor that imperils peace and security of the United States.

e. The National Aeronautics and Space Administration ("NASA") is an agency of the United States Government, which conducts research into flight within and outside the Earth's atmosphere, including the exploration of space.

f. RemotelyAnywhere is a software program that provides a remote access and remote administration package for computers on the Internet and can be downloaded over the Internet from 03AM Laboratories PL, Hungary. Once installed on a host computer, RemotelyAnywhere allows the user to remotely control the host computer and access the host computer from any other computer connected to the Internet. RemotelyAnywhere provides the user with the ability to transfer and delete files or data, and the ability to access almost every administrative function available on the host computer.

g. Defendant GARY MCKINNON was an unemployed computer system administrator living in London, England.

h. The above introductory allegations are realleged and incorporated in Counts One through Seven of this indictment as though fully set out in Counts One through Seven.

COUNT 1
(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

2. Between on or about February 1, 2002, and on or about February 22, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, belonging to the United States Army.

3. Specifically, the defendant intentionally accessed a computer belonging to and used exclusively by the United States Army, Fort Myer, Virginia, with the Internet Protocol address of 160.145.40.25, which computer was used in interstate and foreign commerce and communication. The defendant then obtained administrator privileges and transmitted codes, information and commands that: (1) deleted approximately 1300 user accounts; (2) installed RemotelyAnywhere; (3) deleted critical system files necessary for the operation of the computer; (4) copied a file containing usernames and encrypted passwords for the computer; and (5) installed tools used for obtaining unauthorized access to computers. As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, a system and information, and that damage: (a) caused loss aggregating more than $5,000 in value during a one-year period to the United States Army; and (b) affected the use of the computer system used by a government entity, the United States Army, in furtherance of the administration of national defense and national security.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i) and 1030(a)(5)(B)(v)).

COUNT 2
(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

4. From in or about September 2001, through on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, belonging to the United States Army.

5. Specifically, the defendant intentionally accessed computers exclusively used by the United States Army, which computers were used in interstate and foreign commerce and communication. Then, the defendant obtained administrator privileges on these computers and installed RemotelyAnywhere. On several of the computers, the defendant installed tools used for obtaining unauthorized access to computers, deleted critical system files necessary for the operation of the computers and copied files containing unclassified information to his own computer. The computers accessed and damaged by the defendant included the following:

IP Address	Location
160.145.18.111	Fort Myer, VA
160.145.30.89	Fort Myer, VA
160.145.33.52	Fort Myer, VA
160.145.40.22	Fort Myer, VA
160.145.40.31	Fort Myer, VA
160.145.40.51	Fort Myer, VA
160.145.214.25	Fort McNair, Washington, DC
160.145.214.26	Fort McNair, Washington, DC
160.145.214.27	Fort McNair, Washington, DC
160.145.214.31	Fort McNair, Washington, DC
160.145.214.202	Fort McNair, Washington, DC
160.145.214.204	Fort McNair, Washington, DC
160.145.214.205	Fort McNair, Washington, DC

128.190.84.39	Alexandria, VA
128.190.130.16	Fort Belvoir, VA
128.190.178.21	Fort Belvoir, VA
128.190.224.22	Alexandria, VA
128.190.253.68	Fort A.P. Hill, VA
134.11.65.17	Arlington, VA
134.11.65.33	Alexandria, VA
134.11.237.129	Arlington, VA
134.66.12.64	Fort Irwin, CA
140.153.67.5	Fort Polk, LA
140.153.61.133	Hinton, WV
140.183.2.14	Fort Belvoir, VA
140.183.220.75	Fort Belvoir, VA
141.116.58.63	Arlington, VA
141.116.204.150	Pentagon, Arlington, VA
141.116.230.88	Pentagon, Arlington, VA
150.177.124.5	Fort Meade, MD
150.177.193.130	Fort Meade, MD
150.177.193.248	Fort Meade, MD
155.213.1.201	Fort Benning, GA
155.213.4.100	Fort Benning, GA
155.213.11.46	Fort Benning, GA
160.145.28.84	Fort Myer, VA
160.145.102.216	Fort McNair, DC
160.147.41.166	Fort Belvoir, VA
160.147.126.16	Fort Belvoir, VA
160.147.126.180	Fort Belvoir, VA
160.147.131.150	Alexandria, VA
160.151.76.10	Arlington, VA
160.151.76.56	Arlington, VA
160.151.77.78	Arlington, VA
160.151.77.118 (160.151.76.128)	Arlington, VA
199.114.42.111	Rosslyn, VA
199.122.33.10	Alexandria, VA
199.122.33.24	Alexandria, VA
199.122.41.3	Fort Meade, MD
199.122.45.7	Alexandria, VA
204.34.24.217	Great Lakes, MI
214.3.73.14	Alexandria, VA

As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, systems and

information, and that damage caused loss aggregating more than $5,000 in value during a one-year period to the United States Army.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

COUNT 3
(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

6. From in or about March 2001, through on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, belonging to the United States Navy.

7. Specifically, the defendant intentionally accessed computers exclusively used by the United States Navy, which computers were used in interstate and foreign commerce and communication. Then, the defendant obtained administrator privileges on these computers and installed RemotelyAnywhere. On several of the computers, the defendant installed tools used for obtaining unauthorized access to computers and deleted system logs. The computers accessed and damaged by the defendant included the following:

IP Address	Location
144.247.5.1	Groton, CT
144.247.5.22	Groton, CT
144.247.5.6	Groton, CT
144.247.5.14	Groton, CT
144.247.5.17	Groton, CT
144.247.5.11	Groton, CT
144.247.5.5	Groton, CT
144.247.5.40	Groton, CT
144.247.5.29	Groton, CT
144.247.5.4	Groton, CT
144.247.5.10	Groton, CT
144.247.5.8	Groton, CT
144.247.5.3	Groton, CT
144.247.5.7	Groton, CT
198.97.72.252	Patuxent River, MD
199.211.89.77 (199.211.89.146)	Crystal City, VA

131.158.84.161	Patuxent River, MD
131.158.65.9	Bethesda, MD
204.34.154.59	Pearl Harbor, HI
199.211.163.7	Wayne, PA

As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, systems and information, and that damage caused loss aggregating more than $5,000 in value during a one-year period to the United States Navy.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

COUNT 4
(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

8. From in or about September 2001, through on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, belonging to NASA.

9. Specifically, the defendant intentionally accessed computers exclusively used by NASA, which computers were used in interstate and foreign commerce and communication. Then, the defendant obtained administrator privileges on these computers and installed RemotelyAnywhere. On several of the computers, the defendant installed tools used for obtaining unauthorized access to computers, deleted system log files and copied a file containing usernames and encrypted passwords. The computers accessed and damaged by the defendant included the following:

IP Address	Location
192.42.75.135	Hampton, VA
128.157.55.97	Houston, TX
198.122.128.114	Houston, TX
139.169.118.33	Houston, TX
139.169.118.28	Houston, TX
139.169.18.77	Houston, TX
128.183.158.148	Greenbelt, MD
198.116.200.1	Huntsville, AL
198.119.37.16	Greenbelt, MD
128.155.18.249	Hampton, VA
192.150.38.45	Moffett Field, CA
192.150.38.14	Moffett Field, CA
192.150.38.51	Moffett Field, CA
192.150.38.125	Moffett Field, CA
128.183.144.73	Greenbelt, MD

198.116.36.16	Herndon, VA

As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, systems and information, and that damage caused loss aggregating more than $5,000 in value during a one-year period to NASA.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

COUNT 5
(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

10. Between in or about February 2001, and on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, belonging to the United States Department of Defense.

11. Specifically, the defendant intentionally accessed computers exclusively used by the United States Department of Defense, which computes were used in interstate and foreign commerce and communication. Then, the defendant obtained administrator privileges on this computer and installed RemotelyAnywhere. The defendant accessed and damaged the following computers:

IP Address	Location
150.177.2.192	Fort Meade, MD
150.177.178.130	Fort Meade, MD

As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, a system and information, and that damage caused loss aggregating more than $5,000 in value during a one-year period to the United States Department of Defense.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

COUNT 6
(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

12. Between in or about February 2001, and on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, belonging to the United States Air Force.

13. Specifically, the defendant intentionally accessed a computer exclusively used by the United States Air Force, which computer was used in interstate and foreign commerce and communication. Then, the defendant obtained administrator privileges on this computer and installed RemotelyAnywhere. The defendant accessed and damaged the following computer:

IP Address	Location
209.22.51.6	Crystal City, VA

As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, a system and information, and that damage caused loss aggregating more than $5,000 in value during a one-year period to the United States Air Force.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

COUNT 7
(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

14. From in or about September 2001 through on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, belonging to the companies identified in paragraph 15.

15. Specifically, the defendant intentionally accessed computers belonging to the companies identified below, with the Internet Protocol addresses and locations described below, which computers were used in interstate and foreign commerce and communication.

IP Address	Location	Company
204.2.33.22	Houston, TX	Tobin International
128.169.32.181	Knoxville, TN	University of Tennessee
206.245.175.40	Wayne, PA	Frontline Solutions
206.218.158.90	LaFourche, LA	Louisiana Technical College
206.166.40.243	Colfax, IL	Martin Township Library
206.245.141.46	Bethlehem, PA	Bethlehem Public Library

Then, the defendant obtained administrator privileges and installed RemotelyAnywhere. On some of the computers, the defendant installed tools used for obtaining unauthorized access to computers. As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, systems and information, and that damage caused loss aggregating more than $5,000 in value during a one-year period to the identified companies.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

A TRUE BILL

_____
FOREPERSON

_____
Paul J. McNulty
United States Attorney

By: _____
Justin W. Williams
Assistant United States Attorney
Chief, Criminal Division

_____
Scott J. Stein
Michael J. Elston
Assistant United States Attorneys