Note re GARY McKINNON

This note is a summary of the Review Note

Overview

Between February 2001 and March 2002 Gary McKinnon gained unauthorised access to a number of US Government Computer networks belonging either to the military, security agencies or companies or agencies connected with them. Once accessed he deleted data resulting in systems becoming inoperable or having to be shut down due to concerns about the integrity of the system. The resulting damage to systems and impairment of their integrity and reliability is estimated to have cost over $700,000.

The National Hi Tech Crime Unit (the precursor to SOCA e crime) arrested Mr. McKinnon and interviewed him in March and August 2002 pursuant to a request for Mutual Legal Assistance submitted by the American authorities. He admitted responsibility for the intrusion and accepted that he had deleted files in order to conceal his activity. He claimed that he was searching for evidence of the existence of UFO's, free energy and the existence of a 'secret' government.

In 2002 CPS were approached to prepare a Letter of Request to the USA on behalf of the NHTCU. It became apparent that the US considered that they had ownership of the investigation which, given the sensitivities they wished to retain. The CPS subsequently met with US prosecutors to discuss the appropriate venue for prosecution following which it was agreed that the UK would cede jurisdiction to the US authorities.

Mr. McKinnon has contested his extradition. The Secretary of State has ordered his return, though this decision is the subject of an application for Judicial Review. Mr. McKinnon's solicitors Messrs Kaim Todner have submitted a bundle of material to CPS in support of a request that CPS consider initiating a domestic prosecution.

Evidence

Summary

147-A-4

To gain access to the US computers Mr. McKinnon would usually obtain an anonymous internet account, he would then access a US site, such as that belonging to a University from which he would then seek to obtain access to the Government sites, in this way he hoped to avoid detection. Using various tools, in particular software known as NT Info he would identify insecurities in computer networks and then install a programme called Remotely Anywhere (RA) which would allow him control over that computer. When installing RA he took steps to ensure that its presence could not be detected on the machines.

During the course of the investigation the US investigators obtained and examined computers belonging to Mr. McKinnon. They found that the 'hash' value of the Remotely Anywhere programme installed on his machine matched that of the programme installed on the US machines. Each digital file has a unique numerical value known as the MD5'Hash', sometimes referred to as a digital fingerprint .Any change in the data recorded on a file, no matter how slight will give a different hash figure.

US Investigators were also able to identify a number of IP addresses from which the attacks were launched. Many of these resolve to UK Companies, and some resolve to Tamsin Thomas who was Mr. McKinnon's girlfriend. Mr. McKinnon accepts that on occasion he used her account.

Mr. McKinnon has made admissions and accepted responsibly for most of the attacks. He is unable to recall all the sites he accessed and also says that he found evidence that many of these systems had been accessed by other hackers, many of Chinese origin. He accepts that where the IP addresses resolve to him or the attack bears his signature then he is responsible.

The review has been carried out on the basis of material on the CPS file from 2002, and from material supplied by Mr. McKinnon's solicitors.

The Evidence

The US Witnesses

Witness statements were obtained in 2002 from a number of US witnesses. All give evidence concerning unlawful access to various computers and computer networks. They all tend to refer to reports concerning the examination of machines by others

167-A-5

and their statements contain a lot of hearsay. Without sight of the reports themselves it is not necessarily possible to ascertain how much of this material may be admissible; there is no evidence that ACPO guidance concerning the examination of digital material has been followed nor is there evidence of continuity. It is also unlikely that these witnesses will agree to give evidence in the UK until such time as the extradition process has been concluded. Some of the witnesses, particularly Alvarez and Degnan, fail to particularise the individual computers that have been compromised.

It is also clear from the material submitted during the course of the extradition proceedings that since these statements were obtained further enquires were conducted and the court were given more information about the effects of Mr. McKinnon's activity which is said to have amounted to an attack on the critical security infrastructure of the USA.

Taken together the US witnesses describe a large number of computers. He is said to have compromised 97 computers and to have 'scanned' 73,000 others. One of the most significant attacks was that on Weapons Station Earle where he is said to have attempted to delete all of the files from one computer, where he deleted log files of his own activity rendering the some 300 computers inoperable immediately following September 11th . He is also said to have prevented access to some 2000+ computers belonging to the US Army for 24 hours causing significant disruption.

Mr. McKinnon is interviewed on 19 March 2002 and again on 8 August 2002. In summary he makes admissions to having targeted US military and related sites in order to obtain evidence of the existence of UFO's, free energy and the 'Secret Government'. He takes responsibility for any attack where the evidence points to it having originated with Tamsin Thomas. He also accepts that his methodology was to use anonymous ISP accounts and to install Remotely Anywhere and other software including NT Info scan on as many computers as he could. He would seek to gain access from sites such as Tobin International and others and once he had successfully gained access to a machine would use that access to locate other machines with vulnerabilities and seek to access those. He accepts that he deleted log files as a matter of routine and also accepts that he made other unauthorised modifications. He denies having caused any deliberate damage. He agrees that he left the message regarding disruption saying he was angry with US foreign policy. Perhaps not surprisingly he is unable to recall all of the computers or the systems

147-A-6

that he is said to have gained access to, essentially agrees that if his methodology used and if attacks linked to Tamsin Thomas computers then he was responsible. He does say that he found evidence that other hackers, specifically hackers from China had also gained access to many of these systems.

Section 9 Statement of Gary McKinnon

Dated 9 December 2008.
He states that he made full admission during the course of the interviews with the NHTCU. He agrees that the admissions he made then were true , makes admissions, without specifics to other offences of unauthorised modification to UK computers .
He states the files he deleted were created by him and not by the owners of the machines therefore there was no malice in the attacks. He says that he accepts committing an offence pursuant to section 2 of the Computer Misuse Act ("CMA") by gaining unauthorised access with intent to commit or facilitate the commission of further offences, namely the theft of password files and is willing to plead guilty to offences pursuant to section 2 of the CMA.
He said he was fully expecting to be charged in the UK and talks of the effect of the proceedings hanging over him.
He was arrested by NHTCU in March 02, October 04 US request extradition .June 05 arrested for extradition.
He states that the prospect of extradition and the publicity generated has prevented him from obtaining employment .
Has also had a bail condition not to access the internet.
He says he lost his flat due to the publicity and says the threat of a 10 – 12 years sentence with no prospect of repatriation has caused his health to suffer.

Code Test Review

This case has been reviewed in accordance with the Code for Crown prosecutors.

Evidential

Offences considered
The Computer Misuse Act 1990 (The law needs to be considered as at 2001/ 2)

147-A7

S1 Unauthorised Access

It is an offence to cause a computer to perform any function with intent to secure access to any program or data held in a computer where the access intended to be secured is unauthorised and the offender is knows that such access is unauthorised. The offence is summary only but has an extended statutory time limit of six months from the time when a prosecutor has sufficient evidence to warrant the proceedings but with an overall time limit of 3 years.

Section 2

It is an offence to commit a section 1 offence with intent to commit or facilitate an offence in which the sentence is fixed by law or which carries a maximum sentence on conviction of 5 years or more. This offence carries a sentence of 5 years imprisonment.

Section 3

It is an offence to cause an unauthorised modification of the contents of any computer with the requisite intent and knowledge.

The requisite intent is an intent to cause a modification and by so doing

a) Impair the operation of any computer
b) Prevent or hinder access to any program or data held in any computer
c) Impair the operation of any such program or the reliability of any such data

The requisite knowledge is knowledge that the modification is unauthorised.

Aviation and Maritime Security Act 1990

Section 12

Other acts endangering or likely to endanger safe navigation

(1) Subject to subsection (6) below, it is an offence for any person unlawfully and intentionally–

(a) to destroy or damage any property to which this subsection applies, or

(b) seriously to interfere with the operation of any such property,

where the destruction, damage or interference is likely to endanger the safe navigation of any ship.

In considering the evidential and public interest test I have to have regard for the Code for Crown Prosecutors. Of particular relevance are paragraphs 2.3 and 2.5.

147-A8

ensuring that the right offences are prosecuted and that all relevant evidence is put before the court .

Computer Misuse Act

Section 1

The statutory time limit in respect of an offence contrary to section 1 has now expired.

Section 2

Mr. McKinnon makes admissions, however it is clear that he is unable to recall precise details of his attacks. Essentially he accepts that where IP addresses resolve to his address and where an attack bears his signature then he is responsible. It should be noted that he claims he found existence of other hackers and denies accessing Air Force systems although it is put to him that there is evidence to show he was responsible. There are also instances of intrusions put to him in interview that do not appear to be mentioned by other witnesses. I consider that there is insufficient evidence to prosecute on the basis of the admissions alone because I am not able to frame charges which reflect the totality of the alleged offending.

The following is required:

- Statements identifying each compromised computer.
- Statements producing an image of each computer.
- A report of the examination of each computer including evidence that RA found and its hash value including evidence of the seizure examination and results of examination of Mr. McKinnon's computers and the hash value of RA used by him and production of the files said to have been copied by him from US computers.
- Evidence of continuity and some evidence of compliance with ACPO standards concerning the examination of digital material or sufficient to prove the integrity of the forensic image.
- Sufficient evidence to allow a determination to be made as to whether material can be adduced as hearsay.
- Details of the nature of the systems to which access has been gained and the use to which those computers are put, how apparent would it have been that they were secure military sites?

- Details of why in some instances modification of the system resulted in impairment and further information explaining how losses have been calculated.
- Much more information about the attack on Weapons Station Earle, detailing the apparent attempt made by McKinnon on 23 September 2001 to delete all files on one machine.
- Evidence of the IP addresses associated with the attacks that have been recovered and their resolution to addresses associated with Mr. McKinnon.
- At the time the US witnesses made their statements it was clear that a number of investigations were still in process, the results of those investigations would be required.
- Further evidence in support of the assertion that Mr. McKinnon's activities left the computers vulnerable to further intrusion.
- Information as to the sensitivity of data held on these computer and the parameters for handling of exhibits and of defence access to them.

It is clear that Mr. McKinnon has gained unauthorised access to a large number of computers. Whilst it is unlikely that the computers used by Mr. McKinnon, such as the University of Tennessee were accessed without authorisation it is clear, either expressly of by implication that those belonging to the Military and similar agencies would have been. In interview Mr. McKinnon asserts that his sole reason for seeking access was to obtain information and that he had no malicious intent. The installation of Remotely Anywhere and the other so called hacking tools would have caused an unauthorised modification. Similarly his deletion of the log files of his activity would have amounted to an unauthorised modification, however he does not accept either in interview or in his section 9 statement that he had the necessary intent required by section 3 albeit that the reliability of the systems were impaired either as result of his intrusion or because the deletion of the log files caused the computers to experience problems in rebooting. Notwithstanding his posting of the message concerning disruption I consider that there is insufficient evidence to proceed in respect of a section 3 offence.

In relation to proving a section 2 offence it is necessary to show that he intended to commit or facilitate a specified offence. I am satisfied that we can show that Mr. McKinnon was aware that he was securing unauthorised access. It is also clear that his purpose in securing that access and in installing Remotely Anywhere and the

147-A10

other hacking software was to enable him to identify other computers in order to obtain access to them. He therefore has the necessary intent to commit further section 2 offences. Section 2 is a specified offence.

In his section 9 statement Mr. McKinnon states the offence he intended to commit was the Theft of passwords. What Mr. McKinnon actually did was to obtain passwords and subsequently use them to gain access, the passwords themselves are not property within the meaning of the Theft Act 1968, and they constitute confidential information.

Notwithstanding the difficulty in laying the evidential framework to corroborate the admission I have identified 9 occasions on which the admissions allow offences contrary to section 2 to be identified. (These are set out in full in the Review Note)

Aviation and Maritime Security Act 1990

The House of Lords suggested that Mr. McKinnon's activity would have amounted to an offence contrary to section 12. There is insufficient evidence in the papers that we have to show that any ship was placed in danger.

Alleged Criminality

Mr. McKinnon's alleged criminality is set out in the House of Lords judgement. This illustrates the disparity between that which it would be possible to prove as against that which is alleged, and which the American authorities would appear to be able adduce in evidence in the United States.

Paragraphs 2.4 and 2.5 of the Code state;
2.3 It is the duty of Crown Prosecutors to make sure that the right person is prosecuted for the right offence. In doing so, Crown Prosecutors must always act in the interests of justice and not solely for the purpose of obtaining a conviction.

2.5 It is the duty of Crown Prosecutors to review, advise on and prosecute cases, ensuring that the law is properly applied, that all relevant evidence is put before the court and that obligations of disclosure are complied with, in accordance with the principles set out in this Code.

I have also considered part 10 of the Code and the circumstances in which it is proper for a Crown Prosecutor to accept a guilty plea.

10.1 Defendants may want to plead guilty to some, but not all, of the charges. Alternatively, they may want to plead guilty to a different, possibly less serious, charge because they are admitting only part of the crime. Crown Prosecutors should only accept the defendant's plea if they think the court is able to pass a sentence that matches the seriousness of the offending, particularly where there are aggravating features. Crown Prosecutors must never accept a guilty plea just because it is convenient.

The inability to frame charges which reflect the totality of the offending means that the evidential test has not been met.

In 2007 the Attorney General issued guidance entitled "*Guidance for handling criminal cases with concurrent jurisdiction between the United Kingdom and the United States of America*". In accordance with this guidance the Crown Prosecution Service has recently engaged in further discussions with the US authorities. For the reasons set out below the US still wishes to retain jurisdiction and I am satisfied that the United States remains the appropriate venue for a prosecution:

- The fact that the 'harm' occurred in the United States. The activity was directed against the military infrastructure of the United States.
- That the investigation commenced in the United States and was ongoing.
- The witnesses of whom there were a large number were mostly located in the United States.
- That the bulk of the 'real' evidence was located in the United States. The task of gathering sufficient evidence to initiate proceedings in the UK would have been immense.
- That the United States prosecutors were able to frame charges which reflected the extent of McKinnon's criminality.
- The bulk of the 'unused' material was located in the United States. This material was likely to include sensitive material which would be best dealt with by the Courts in the United States.

Public Interest

147-A12

As I do not consider the evidential test to be met I do not go onto consider the public interest test.

Material supplied by Kaim Todner

Statements, affidavits and letters have been supplied by psychiatrists, US Lawyers, members of McKinnon's family and others concerning his mental health / personality disorder, the conditions in US prisons and the likely length of sentence and possible repatriation.

The material supports the following conclusions;
1. That McKinnon suffers from Aspergers Syndrome, that imprisonment in the US is likely to be detrimental and may result in him attempting suicide or otherwise will significantly affect his mental health

2. He is likely to receive a substantial prison sentence, and may be incarcerated in a supermax prison subject to SAMs which practices have been condemned by Human Rights bodies He is unlikely to be repatriated to serve his sentence in the UK.

3. That having the proceedings hanging over him for such a lengthy period is having an adverse affect on him.

Many of the issues that the statements address have been canvassed in the extradition proceedings and the courts have not found them to constitute a bar. The statutory extradition proceedings impose an obligation on the courts to consider whether extradition is compatible with Mr. McKinnon's ECHR rights.

Conclusion

There is insufficient evidence currently available to prosecute Mr. McKinnon. The public interest test does not therefore arise.

Russell Tyner
26.2.09

Review Note

GARY McKINNON

Overview

Between February 2001 and March 2002 Gary McKinnon gained unauthorised access to a number of US Government Computer networks belonging either to the military, security agencies or companies or agencies connected with them. Once accessed he deleted data resulting in systems becoming inoperable or having to be shut down due to concerns about the integrity of the system. The resulting damage to systems and impairment of their integrity and reliability is estimated to have cost over $700,000.

The National Hi Tech Crime Unit (the precursor to SOCA e crime) arrested Mr. McKinnon and interviewed him in March and August 2002 pursuant to a request for Mutual Legal Assistance submitted by the American authorities. He admitted responsibility for the intrusion and accepted that he had deleted files in order to conceal his activity. He claimed that he was searching for evidence of the existence of UFO's, free energy and the existence of a 'secret' government.

In 2002 CPS were approached to prepare a Letter of Request to the US on behalf of the NHTCU. It became apparent that the US considered that they had ownership of the investigation which, given the complexities and sensitivities they wished to retain. The CPS subsequently met with US prosecutors to discuss the appropriate venue for prosecution following which it was agreed that the UK would cede jurisdiction to the US authorities.

Mr. McKinnon has contested his extradition. There is a judicial review pending of the Secretary of States order to return Mr. McKinnon to the US.

Mr. McKinnon's solicitors Messrs Kaim Todner have submitted written representations dated 23rd December 2008 and a bundle of supporting documentation to CPS in support of a request that CPS consider initiating a domestic prosecution. They provided further material undercover of a letter dated 4th February 2009.

147-A-14

Review Note 3

Much of the evidence in this case is technical and ordinarily the reviewing lawyer would have the benefit of a case officer to assist in understanding of the material.

Evidence

Summary

To gain access to the US computers Mr. McKinnon would usually obtain an anonymous internet account, he would then access a US site, such as that belonging to a University from which he would then seek to obtain access to the Government sites, in this way he hoped to avoid detection. Using various tools, in particular software known as NT Info he would identify insecurities in computer networks and then install a programme called Remotely Anywhere which would allow him control over that computer. When installing RA he took steps to ensure that its presence could not be detected on the machines.

Evidence from US witnesses show that the intrusions came from a number of different sources including;
Neptune 13 belonging to the University of Tennessee
Front Line Solutions Arenadevsrvr
US Navy IP address [redacted]
Louisiana Department of Education
Tobin International
Information Management Centre
Uniform Health Service
US Army Land Information Warfare Activity

Mr. McKinnon accepts that he accessed Tobin International, the University of Tennessee, the Army Information system and numerous Army medical sites. He accepts that he accessed Frontline Solutions and the Louisiana Dept of Education but cannot necessarily recall doing so. Similarly, in relation to the Navy computer IP [redacted] he says that he recalls the 199 prefix.

During the course of the investigation the US investigators obtained and examined computers belonging to Mr. McKinnon. They found that the 'hash' value of the Remotely Anywhere programme installed on his machine matched that of the programme installed on the US machines. Each digital file has a unique numerical value known as the MD5'Hash', sometimes referred to as a digital fingerprint. Any

147-A15

change in the data recorded on a file, no matter how slight will give a different hash figure.

US Investigators were also able to identify a number of IP addresses from which the attacks were launched. Many of these resolve to UK Companies, and some resolve to Tamsin Thomas who was Mr. McKinnon's girlfriend. Mr. McKinnon accepts that on occasion he used her account.

Mr. McKinnon has made admissions and accepted responsibly for most of the attacks. He is unable to recall all the sites he accessed and also says that he found evidence that many of these systems had been accessed by other hackers, many of Chinese origin. He essentially accepts that where the IP addresses resolve to him or otherwise the attack bears his signature then he is responsible.

The US Witnesses

The witnesses Shaver, Sternal, Dusen, Milner, Degnan and Alvarez all give evidence concerning unlawful access to various computers and computer networks. They all tend to refer to reports concerning the examination of machines by others and their statements contain a lot of hearsay. Without sight of the reports themselves it is not necessarily possible to ascertain how much of this material may be admissible; there is no evidence that ACPO guidance concerning the examination of digital material has been followed nor is there evidence of continuity. Some of the witnesses, particularly Alvarez and Degnan fail to particularise the individual computers that have been compromised.

Material on CPS file

Statements

JIM SZOPINSKI

Employee of Binary Research International Inc USA. His Company distributes software known as 'Remotely Anywhere' ("RA") The software allows a person to control their home computer from another computer situated anywhere in the world. He checks the data base which shows the software having been downloaded to Tamsin Thomas with an e-mail address. Without information as to the way in which the database is compiled it is potentially hearsay, however it is likely to be admissible pursuant to 117 CJA 2003 as Business Hearsay. Mr. McKinnon agrees that he

downloaded RA from the Internet saying he downloaded it on more than one occasion.

JOSEPH DEGNAN

US Navy Special Agent. The hacking incident began at the Supervisor of Shipbuilding SUPSHIP. He describes the attacks and also lists the IP addresses from which the attacks have originated. He gives evidence of what he is told by others about an attack in March 2001 and states that 16 servers and one workstation had been compromised by having RA installed on them.

He lists the computers that were accessed;

1. grctmaster IP address [redacted] accessed between 19th March and 20 March 2001.From his previous comment it appears that Remotely Anywhere was installed on this machine.
2. grctapps IP address [redacted] accessed between 17 and 20 March 2001.

As a consequence of having to reconstruct systems the cost is estimated at $25,930.

Mr. McKinnon accepts that he targeted SUPSHIP but has some trouble recalling specifics. During the interview the officers put it to him that he used the name 'Tate'. He denies this initially saying he used the name 'Solo'. Clearly the officers have the name Tate from the US investigators, either Mr. McKinnon is lying, has forgotten or there is another person who has hacked the system. However later he says that he may have used the name Tate that the name rang a bell but there were other hackers on the system.

Without evidence of the hash value matches and the IP address that resolve to Mr. McKinnon the evidence is insufficient.

12 computers were compromised at Weapons Station Earle sometime before July 2001. It appears that the Remotely Anywhere software installed. He does not give evidence of either the precise dates of compromise or the details of the machines involved. He gives evidence of IP addresses from which attacks were launched and the communication service providers to whom they resolve, all of this is hearsay with insufficient information to seek to adduce it evidentially.

147-A-17

Review Note 3

On 23 September Mr. McKinnon using a machine upon which he had installed Remotely Anywhere previously, deleted files from a number of machines and attempted to delete all files on the machine. Clearly this needs further explanation as it appears to be evidence of Mr. McKinnon seeking to impair the systems rather than to simply cover his tracks. As a result of this activity the Command was shut down from 23 September to 1 October 2001 and in a reduced state of activity for a while thereafter. 30 machines had the RA software installed on them. Clearly this was a critical time for the US armed forces. The cost is said to be $121,424.
As well as RA other hacking software was found to have been installed including L0phtCrack3, NTinfoScan and PsLoglist. Mr. McKinnon accepts that he has used this software, it does not appear to be suggested that this software also had hash values which matched that used by Mr. McKinnon.
Mr. McKinnon accepts that he attacked Earl and deleted log files to cover his tracks.
Degnan states that he examines 6 machines. He exhibits what appear to be reports of his examinations. He produces IP addresses associated with the attacks which resolve to the UK.

Without evidence of the hash value matches and the IP address that resolves to Mr. McKinnon the evidence is insufficient.

Degnan states that he is aware of an intrusion into a US Navy computer assigned to the Australian Foreign Military Sales. He examines that machine which had an IP address of [redacted] and is used to access many of the US Army machines.
He states that the investigation is ongoing into intrusions into systems in the US, UK and Singapore.
He then goes on to discuss a report prepared by another investigator in relation to the Patuxent River Naval Warfare Centre Aircraft Division Computer Network and established the following intrusions;
[redacted] Print server between 28 December 2001 and January 5 2002. RA had been installed
Naval Medical Centre – a connection made and RA installed.

He goes on to report an intrusion into the Naval Telecommunications Command Europe based in the UK where again RA was installed. There is no detail of the computers affected but the cost is said to be $22,000.

147-A-18

Next he reports the intrusion to 1/COMSCWESTPAC Singapore where RA installed on computer with IP [redacted]. The intruder accessed via University of Tennessee.

FTP Server Pearl Harbour Naval Shipyard Hawaii IP [redacted] where again RA installed, he says from an IP range in the UK which matches those involved in other intrusions. It is not clear whether he means that the machine was modified or RA used to gain access. There is much of hearsay, the statement lacks precise details and is technical. However it serves to illustrate the location and nature of the systems that have been attacked.

MICHAEL MILNER

He is a Special Agent for National Aeronautical and Space Administration NASA
He is told that [redacted].GOV had been compromised
He conducts a review of logs. It is not clear how these are obtained or how generated.
[redacted].gov was also compromised.

In respect of both computers RA and NTInfo had been installed. Mr. McKinnon accepts that he accessed [redacted] and that he installed RA and accepts using NTInfo. Again though he says he is unable to recall exactly without specifics of each incident.

Milner lists other computers that have been compromised in a similar way; he doesn't explain how he has come by this information.

[redacted].GOV on 17.9.01 RA installed and NT info scan

[redacted].GOV on 10.9.01 RA and NTInfo

[redacted].GOV on 9.9.01 RA and NTInfo , Mr. McKinnon accepts this intrusion.

[redacted].GOV on 16.9.01 RA and NT Info SCAN

[redacted].GOV on a Date unknown RA and NT

Review Note 3

[redacted]gov on 12.9.01 Ra AND ntiNFO

[redacted]gov on 17.9.01 RA and NT info

[redacted]GOV on 10.9.01 Ra AND nt INFO

[redacted]GOV on 10.9.01 Ra AND nt INFO

[redacted]gov on 11.10.01 RA and NT Info

[redacted].gov on 10.12.01 RA and NT Info

[redacted] on 13.10.01 RA and NT Info

[redacted].com on a date unknown in January 2002 RA and NT Info

In total 15 systems compromised plus one belonging to a NASA contractor with damage totalling $100k. The installation of RA and NT Info rendered any data on the systems unreliable.

He sets out the information provided by INTERPOL re the IP addresses provided to him in October 2001.

DAVID SHAVER

US Army Computer Forensic Examiner. He is a US Government contractor employed by Sytex Inc USA and refers to Mr. McKinnon as GM.
He lists 57 computers that have had the program Remotely Anywhere installed without authorisation. It is not clear whether this comes from his own examination or reports that have been made to him. He states that a number of computers have yet to be examined.
He examines a computer belonging to the University of Tennessee known as Neptune [redacted] and he produces report DSS/1 I assume therefore that he conducts the examination. McKinnon accepts having attacked US Army sites from Neptune. He determines that RA installed had the same Hash value as those recovered from McKinnon's personal computer. The person who installed RA also

added a further user account SOLO and deleted critical files which prevented the computer from re booting. From there the subject connected to 2 US Government computers, analysis shows that they were compromised in a similar manner. Again it is not clear whether he is speaking from own knowledge or whether this is hearsay, nor precisely what the similarities are, I presume it is the hash value of RA. Mr. McKinnon agrees that he used the name SOLO.

The computers accessed were:

[redacted] Located Fort McNair , McKinnon accepts this was him.

[redacted] Fort Myer McKinnon accepts this was him. But unclear whether RA installed on these

Dates of compromise are not clear but appear to be prior to 22.2.02.

Although GM accepts he used the name SOLO I consider the evidence to be presently insufficient without clarification as to whether this witness carried out the examinations himself or whether some or parts of his evidence are hearsay.

He examines Front line solutions Inc Computer – [redacted] produces report as DSS/2 this computer compromised he says by unknown means by having RA installed prior to 22.1.02 RA was loaded on the computer. This computer operates as a server and analysis shows that 6000 files downloaded from 3 US Gov computers

[redacted]

[redacted]

[redacted]

He says the subject scanned 2 computers which had RA installed namely

[redacted]

[redacted] US Army Signal Activity Fort Belvoir

It is not clear what scanned means, he says these both had RA installed, again it is not clear whether this is from his own knowledge or is hearsay

A scan was also conducted of over 130 additional computers in a possible attempt to locate future victims; again this is vague and doesn't specify the computers concerned.

A SAM file was downloaded to US Army computer [redacted] – see DSS/12 [redacted] - he can't tell if this was compromised or not.

He goes on to say that having analysed the IP address which connected to the Front Line Solutions Inc a number of IP address are identified which resolve to the UK.

Review Note 3

Mr. McKinnon has agreed that he accessed US Army a site though is unable to recall whether this was from Frontline or not. He also accepts having accessed Pentagon computers. Further he accepts that he has downloaded files but from his interview it is not possible to ascertain which computers they were downloaded from. However this would be available in the report of the examination of GM computers.

Examines US Army Computer [redacted] Fort Belvoir Fire Dept FQDN of [redacted] produces DSS/3. RA installed prior to 1.2.02 deleted critical log files to avoid detection and used the computer to scan other computers the RA file matched the hash value of GM computers.

US Army Computer report DSS/4 FQDN of [redacted] mil Office of Staff Judge Advocate, RA with GM has value installed prior to 11.2.02 – log files deleted.

US Army Computer report DSS/4 FQDN [redacted] .mil Office of Staff Judge Advocate ,RA matching GM hash value installed prior to 3.2.02 evidence shows accessed from [redacted] an IP address registered to the US Navy. This is the Australian Foreign Military Sales machine referred to by Degnan.

US Army Computer DSS/5 CID [redacted] Fort Irwin CID compromised prior to Jan 23 02 from [redacted] RA with GM hash

US Army Computer DSS/6 FQDN of [redacted] US Dental Research Detachment accessed from IP [redacted] Louisiana Dept of Education, RA loaded prior to 24.2 02 , altered systems logs to avoid detection match to GM hash value.

US Army computer DSS/7 IP [redacted] FQDN of [redacted] US Army Signal Activity RA installed prior to 21.2.02 match to GM hash value, evidence of him connecting from 4 other computers. This is the same computer used to access Canon_SOLD

US Army computer DSS/8 FQDN of [redacted] Pentagon compromised from [redacted] egistered to US Army prior to 18.2.02 US RA with GM hash value installed

147-A-22

Review Note 3

DSS/9 US Army computer FQDN of [redacted] US Army Information Systems Command Pentagon installed RA prior to 7.2.02 match to GM evidence of log on from [redacted] He then scanned 2500 other US Gov computers including 5 which had RA installed, not specified which computers or whether these have already been referred to in his statement.

DSS/10 US Army computer [redacted] US Army USAIC Fort Benning RA prior to 4.2.02 match to GM he copied files to [redacted] Charter communications and [redacted] NTL UK .He also scanned a number of other computers from this computer. Again I am not sure what scan means. Does it mean he gained access?

DSS/11 [redacted] Fort Myer Primary Domain Controller US Army Directorate of Information RA installed prior to 22.2.02 match to GM he deleted 2455 user accounts and left a message saying "*I will continue to disrupt at the highest levels*". The complete network became inoperable as a result. This message is the clearest evidence that GM motive was not simply to obtain information in respect of either UFO's or the secret Government. Mr. McKinnon accepts responsibility for this message. He is not asked about the deletion of files in the interview. Despite this clear admission without clarification as to the status of the reports and whether they are hearsay and whether they are potentially admissible I am not satisfied that there is sufficient evidence.

DSS/12 [redacted] US Army Directorate of Information RA with GM match prior to 20.1.02 log files deleted

DSS/12 [redacted] US Army Battle Lab Fort Benning prior to 4.2.02 RA with GM match.

DSS/12 IP [redacted] belonging to US Army Di Lorenzo Tri Care Health Clinic the SAM file for this computer was recovered from the Frontline Solutions Computer, he is unable to tell if this machine compromised or not .

DSS/ 18 – [redacted] mil Army Claims Service RA match to GM prior to 10.3.02 the access came from the Uniformed Services University.

147-A23

Review Note 3

DSS/13 [redacted] 311th Theatre Signal Command RA prior 3.3.02 RA match to GM then commenced a scan of other computers, he logged in from Louisiana Dept of State Education.

DSS/ 13 re IP [redacted] 311th Theatre Signal Command prior to 3.3.02 RA match to GM scanned 92 other computers

DSS/13 [redacted] 902nd Military Intelligence RA prior to 6.3.02 match to GM

DSS/14 [redacted] HQ and HQ Command Special Activities Fort Belvoir prior to 10.3.02 RA match to GM log files deleted.

[redacted] US Army Directorate of Information prior to 21.2.02 RA match to GM log files deleted.

[redacted] – 018 US Army Walter Reed Army Medical Centre prior to 1.2.02 RA match to GM log files deleted.

[redacted] US Army Walter Reed Army Medical Centre 2.2.02 RA installed match to GM log files deleted

DSS/15 CANON_SOLD Soldiers Magazine 18.3.02 RA with GM match scanned other computers logged on from [redacted] see DSS/ 5 , I don't think we can date this sufficiently to say it occurred on a different occasion than in DSS/5

[redacted] 10.3.02 RA with GM match used to scan other computers

[redacted] Fort Myer Resident Agency CID prior to 2.2.02 RA with GM match connected from [redacted] used to scan other computers.

HINDSMON prior to 20.1.02 this belonged to the Computer Science Corporation (but he says it's an Army computer. (This could do with clarification) RA with GM match used to scan 22 other US computers.

147-A-24

Review Note 3

[redacted] prior to 6.3.02 again this belongs to the Computer Science Corp RA with GM match.

DSS/16 [redacted]mil US Army Directorate of Information Management 22.2.02 RA with GM Hash deleted file which prevented computer from re- booting which prevented use of the server

US Army Directorate of Information Management Fort McNair [redacted]RA 21.2.02 with GM hash deleted critical system files which prevented system from re-booting preventing use of the server

US Army Directorate of Information Management Fort McNair [redacted]RA prior to 22.2.02 with GM hash deleted critical system files which prevented system from re-booting preventing use of the server

US Army Directorate of Information Management Fort McNair [redacted]RA 22.2.02 with GM hash deleted critical system files which prevented system from re-booting preventing use of the server

US Army [redacted]mil US Army Directorate of Information Management Fort McNair 3.3.02 RA with GM hash system files deleted prevent system re-booting preventing use of the server

[redacted]mil US Army Directorate of Information Management Fort McNair 22.2.02 RA with GM hash files deleted prevent system re-booting preventing use of the server

[redacted]mil US Army Directorate of Information Management Fort McNair 22.2.02 RA with GM hash files deleted prevent system re-booting preventing use of the server

[redacted]mil US Army Directorate of Information Management Fort McNair 22.2.02 RA with GM hash files deleted prevent system re-booting preventing use of the server

147-A25

Review Note 3

US Army Directorate of Information [redacted]RA with GM hash files deleted prevent system re-booting preventing use of the server.

There is no information to explain why the deletion of the log files prevented these systems from re- booting, or what in fact re- booting means . Further explanation is required as to why it is that on some occasions the deletion of the log files prevented the systems re- booting where in other cases it did not.

DSS/17 US Army Computer [redacted]mil owned by The Pentagon compromised prior to 11.2.02 RA with GM hash deleted log files.

[redacted]Department of Defense Network Information Centre 20.1.02 RA with GM hash

[redacted]Information Systems Command Directorate of Automation Services Systems technology and Networks Division time not known RA with GM hash log files deleted

US Army [redacted]– Fort Benning RA with GM hash 6.2.02

He then produces a report of the examination of Mr. McKinnon's computers as DSS/19 There is no evidence producing them. He finds that;
19 files copied which were not publicly accessible from [redacted]t is unclear but this seems to be from the US Army Family Support
15 from [redacted]311th Theatre Signal
73 from [redacted]– VIDEOSERVER MCKENNA
9 from Dilorenzon health clinic
9 from Dental command
SAM files from –[redacted]and [redacted]
GM scanned 73,885 separate computers using NT Info Scan
GM admin account was SOLO
The unauthorised files (not specified but I assume he means RA) recovered from 48 US Army and 3 civilian computers match the files on Mr. McKinnon's computers. This is a reference to the hash value but again as with the reports there is no evidence of the hash values being ascertained of either the files on Mr. McKinnon's computers or those files on the compromises systems.

147 - A26

Review Note 3

HAROLD DUSEN

Army Special Agent. He produces a number of logs that have been obtained by his office. He is also reliant on work carried out by others. He states the forensic examination was carried out by SHAVER, he then lists the machines which have been compromised, nearly all of these match those described by SHAVER. He states that systems were compromised but doesn't explain what is meant by this.
He details the attacks and the source computer that launched the attacks;
Tobin International
University of Tennessee
Information Management Centre IMCEN Pentagon
Frontline Solutions
Uniform Health Service
Louisiana Dept of Education
US Army Land Information Warfare Activity LIWA and US Army Computer Emergency Response Team

PAUL K STERNAL
Special Agent Defense Criminal Intelligence Service.
Received a preliminary incident report PKS/1. It appears his statement is taken from this report which must be hearsay and whether admissible or not is difficult to determine without sight of it.
2.3.02 The Fort Meade network detected that it was being scanned by a computer of the Louisiana Dept of State Education.
RA installed on 4 computers
Local Admin account [redacted] winnttest RA installed 3.3.02
DCS [redacted] accessed
[redacted] DTAO – no evidence
[redacted] 13TH Theatre Signal Command
All of these feature in the statements of Shaver and Degnan. All this appears to be hearsay.
Re DCS Computer [redacted] winnttest this is one of the Fort Meade compromised computers he examines this computer, there is no evidence as to where this came from, or continuity or ACPO issues etc .RA found installed from IP address [redacted] on 3.3.02 states the hash value matches Mr. McKinnon.

147-A-27

States that DCS suffered a loss of $145k as a result, DTAO $340K and DOD CERT $19600K . It is not clear how these figures have been calculated.

PAUL ALAVAREZ

US Air force Computer Crime Investigator.

Notified of an intrusion from the Louisiana Technical College and the installation of RA on to a JSFPO Joint Strike Force Program Office computer Pearl Harbour.

He then collected images of the system hard drives he also had access to files from Mr. McKinnon's computers, again continuity and hearsay issues. He then reviews the material produced by other examiners. Mr. McKinnon denies having accessed any Air force systems.

RA and other hacking software installed on system with hash values matching those of Mr. McKinnon, using the system he attempted to access to other computer systems associated with the military.

He says that log files recovered from Mr. McKinnon's computer show him logging in to the LTC computer and from there to the JSFPO system and to Pearl Harbour Navy Shipyard, he downloaded hacking tools to the JSFPO system. He also connected to US Army systems for JSFPO. Total cost $19,446 by AFOSI and $4,29 K ? by JSFPO

Mr. McKinnon accepts having accessed Naval computers.

I2 Chart

This shows connections between a number of computers, it illustrates connections to computers from those such as Tobin International. Many of the computers are those referred to by the US Witnesses, many are not referred to. Without the assistance of an officer I am unable to analyse this chart.

MATERIAL SUPPLIED BY Kaim Todner

Records of Interview

At the time the interviews were conducted the information held by the police was limited and as a consequence they were not able to put each specific intrusion to Mr. McKinnon. Instead they focus on the systems that were attacked.

147-A-28

He is interviewed on 19 March 2002 and again on 8 August 2002. In summary he makes admissions to having targeted US military and related sites in order to obtain evidence of the existence of UFO's, free energy and the 'Secret Government'. He takes responsibility for any attack where the evidence points to it having originated with Tamsin Thomas or where other evidence exists to implicate him. He also accepts that his methodology was to use anonymous ISP accounts and to install Remotely Anywhere and other software including NT Info scan on as many computers as he could. He would seek to gain access from sites such as Tobin International and others and once he had successfully gained access to a machine would use that access to locate other machines with vulnerabilities and seek to access those. He accepts that he deleted log files as a matter of routine and also accepts that he made other unauthorised modifications. He denies having caused any deliberate damage. He agrees that he left the message regarding disruption saying he was angry with US foreign policy. Perhaps not surprisingly he is unable to recall all of the computers or the systems that he is said to have gained access to, essentially agrees that if his methodology used and if attacks linked to Tamsin Thomas computers then he was responsible. He does say that he found evidence that other hackers, specifically hackers from China had also gained access to many of these systems.
He denies accessing Air Force sites and also denies initially, though later with less force, to using the name Tate. It is to be assumed that the evidence to show that he was responsible both for the attacks on the Air Force and to connect him with Tate is the same as for the other attacks. It also appears apparent that other IP addresses, unconnected with Mr. McKinnon were also involved in attacks supporting his contention that he was not the only hacker who had gained access to these systems, because in interview a French IP address is put to him but quickly withdrawn.

I have done my best to draft charges from the admissions. Save for one instance, I have been unable to specify an individual machine. The charges therefore are vague and relate to admitted activity against a system which would involve the unauthorised access to more than once machine, however I consider they are not duplicitous as they relate to a single course of conduct. Were Mr. McKinnon to be charged these counts might perhaps best be presented as multi offending counts.

In March 2002 there were 3 Interviews:
M 1 – 52 pages
M 2 – 41

Review Note 3

M3 - 20

In August there were 2

A 1 - 33 pages
A 2 - 22

COMPUTER SYSTEM	ADMISSION PAGE NO
SUPSHIP	M1 28
	33
17 – 20 March 01	
	M3 2
NAVAL COMMAND CENTRE	M1 40
NWS Earl	46
18- 21 June 01	49
	M2 3
	A 1 27
	M3
NASA	M2 10
LMSSER2	12
4.0 – 6.9 O1	M3 4
MARSHALL SPACE FLIGHT CENTRE	M3 4

147-A-30

10.9.01	
	M2 13
NASA	38
HERCULES	
9.9.01	M3 4
US ARMY	M2 19
	21
3.9.01	39
22.2.02	M3 6
1- 4.10.01	
US ARMY PENTAGON INFORMATION SYSTEMS	M2 22
1.10.01	M3 8
	16

Potential Charges

1

On a day between the 16 and 21 March 2001 within the jurisdiction of the Central Criminal Court secured unauthorised access to a computer belonging to the United States Navy known as SUPSHIP with intent to commit or facilitate the commission of further offences namely to secure unauthorised access to any program or data held within computers belonging to the United States Navy with intent to commit or facilitate the commission of further offences.

Contrary to section 2(1) of the Computer Misuse Act 1990

2

On a day between the 17 and 22 June 2001 within the jurisdiction of the Central Criminal Court secured unauthorised access to a computer belonging to the United States Navy at the Naval Command Centre Earl with intent to commit or facilitate the

147-A-31

commission of further offences namely to secure unauthorised access to any program or data held within computers belonging to the United States Navy with intent to commit or facilitate the commission of further offences.
Contrary to section 2(1) of the Computer Misuse Act 1990

3
On a day between the 3 and 6 September 2001 within the jurisdiction of the Central Criminal Court secured unauthorised access to a computer known as LMSSER2 belonging to the United States National Aeronautics and Space Administration with intent to commit or facilitate the commission of further offences namely to secure unauthorised access to any program or data held within computers belonging to the National Aeronautics and Space Administration with intent to commit or facilitate the commission of further offences.

4
On 9 September 2001 within the jurisdiction of the Central Criminal Court secured unauthorised access to a computer known Hercules belonging to the United States National Aeronautics and Space Administration with intent to commit or facilitate the commission of further offences namely to secure unauthorised access to any program or data held within computers belonging to the National Aeronautics and Space Administration with intent to commit or facilitate the commission of further offences.

Contrary to section 2(1) of the Computer Misuse Act 1990

5
On 10 September 2001 within the jurisdiction of the Central Criminal Court secured unauthorised access to a computer as situated with in the Marshall Space Flight Centre belonging to the United States National Aeronautics and Space Administration with intent to commit or facilitate the commission of further offences namely to secure unauthorised access to any program or data held within computers belonging to the National Aeronautics and Space Administration with intent to commit or facilitate the commission of further offences.

Contrary to section 2(1) of the Computer Misuse Act 1990

6

On 3 September 2001 within the jurisdiction of the Central Criminal Court secured unauthorised access to a computer belonging to the United States Army with intent to commit or facilitate the commission of further offences namely to secure unauthorised access to any program or data held within computers belonging to the United States Army with intent to commit or facilitate the commission of further offences.

Contrary to section 2(1) of the Computer Misuse Act 1990

7

On a day between 1 and 5 October 2001 within the jurisdiction of the Central Criminal Court secured unauthorised access to a computer belonging to the United States Army with intent to commit or facilitate the commission of further offences namely to secure unauthorised access to any program or data held within computers belonging to the United States Army with intent to commit or facilitate the commission of further offences.

Contrary to section 2(1) of the Computer Misuse Act 1990

8

On 22 February 2002 within the jurisdiction of the Central Criminal Court secured unauthorised access to a computer belonging to the United States Army with intent to commit or facilitate the commission of further offences namely to secure unauthorised access to any program or data held within computers belonging to the United States Army with intent to commit or facilitate the commission of further offences.

Contrary to section 2(1) of the Computer Misuse Act 1990

9

On 1 October 2001 within the jurisdiction of the Central Criminal Court secured unauthorised access to a computer belonging to the United States Army Pentagon Information Systems with intent to commit or facilitate the commission of further

147-A-33

offences namely to secure unauthorised access to any program or data held within computers belonging to the United States Army Pentagon Information Systems with intent to commit or facilitate the commission of further offences.

Contrary to section 2(1) of the Computer Misuse Act 1990

Section 9 Statement of Gary McKinnon Dated 9 December 2008

Mr. McKinnon states that he made full admission during the course of the interviews with the NHTCU. He agrees that the admissions he made then were true, and makes admissions, without specifics to other offences of unauthorised modification to UK computers.
He states the files he deleted were created by him and not by the owners of the machines and therefore there was no malice in the attacks.
He says that he accepts committing an offence pursuant to section 2 of the CMA by gaining unauthorised access with intent to commit or facilitate the commission of further offences, namely the theft of password files and is willing to plead guilty to offences pursuant to section 2 of the CMA.
He said he was fully expecting to be charged in the UK.
He talks of the effect of the proceedings hanging over him.
He was arrested by NHTCU in March 02. In October 04 the US request extradition and in June 05 he is arrested for extradition.
States that the prospect of extradition and the publicity generated has prevented him from obtaining employment.
Has also had a bail condition not to access the internet.
He says he lost his flat due to the publicity.
He says the threat of a 10 – 12 years sentence with no prospect of repatriation has caused his health to suffer.

Offences considered
The Computer Misuse Act 1990 (The law has been considered as at 2001/ 2)

S1 Unauthorised Access
It is an offence to cause a computer to perform any function with intent to secure access to any program or data held in a computer where the access intended to be secured is unauthorised and the offender is knows that such access is unauthorised.

147-A-34

The offence is summary only carrying but has an extended statutory time limit of six months from the time when a prosecutor has sufficient evidence to warrant the proceedings but with an overall time limit of 3 years.

Section 2

It is an offence to commit a section 1 offence with intent to commit or facilitate an offence in which the sentence is fixed by law or which carries a maximum sentence on conviction of 5 years or more. This offence carries a sentence of 5 years imprisonment.

Section 3

It is an offence to cause an unauthorised modification of the contents of any computer with the requisite intent and knowledge.

The requisite intent is an intent to cause a modification and by so doing

a) Impair the operation of any computer
b) Prevent or hinder access to any program or data held in any computer
c) Impair the operation of any such program or the reliability of any such data

The requisite knowledge is knowledge that the modification is unauthorised.

Aviation and Maritime Security Act 1990

12 Other acts endangering or likely to endanger safe navigation

(1) Subject to subsection (6) below, it is an offence for any person unlawfully and intentionally–

(a) to destroy or damage any property to which this subsection applies, or

(b) seriously to interfere with the operation of any such property, where the destruction, damage or interference is likely to endanger the safe navigation of any ship.

Code Tests

I have applied the Code for Crown prosecutors ("the Code"). I have to be satisfied that there is a realistic prospect of conviction. If and only if there is do I go onto consider the public interest test. Paragraphs 2.3 and 2.5 of the Code state;

2.3 It is the duty of Crown Prosecutors to make sure that the right person is prosecuted for the right offence. In doing so, Crown Prosecutors must always act in the interests of justice and not solely for the purpose of obtaining a conviction.

167-A-35

Review Note 3

2.5 It is the duty of Crown Prosecutors to review, advise on and prosecute cases, ensuring that the law is properly applied, that all relevant evidence is put before the court and that obligations of disclosure are complied with, in accordance with the principles set out in this Code.

Evidential

Aviation and Maritime Security Act 1990

The House of Lords suggested that Mr. McKinnon's activity would have amounted to an offence contrary to section 12 of the above Act. There is insufficient evidence in the papers that we have to show that any ship was placed in danger.

Computer Misuse Act

The statutory time limit in respect of an offence contrary to section 1 has now expired.

Mr. McKinnon makes admissions, however it is clear that he is unable to recall precise details of his attacks. Essentially he accepts that where IP addresses resolve to his address and where an attack bears his signature then he is responsible. It is interesting that he claims he found existence of other hackers and denies accessing Air Force systems although it is put to him that there is evidence to show he was responsible. There are also instances of intrusions put to him in interview that do not appear to be mentioned by other witnesses.

The following is required:

- Statements identifying each compromised computer.
- Statements producing an image of each computer.
- A report of the examination of each computer including evidence that RA found and its hash value including evidence of the seizure examination and results of examination of Mr. McKinnon's computers and the hash value of RA used by him and production of the files said to have been copied by him from US computers.
- Evidence of continuity and some evidence of compliance with ACPO standards concerning the examination of digital material.
- Sufficient evidence to allow a determination to be made as to whether material can be adduced as hearsay.

147-A-36

- Details of nature of the systems to which access has been gained and the use to which those computers are put, how apparent would it have been that they were secure military sites?
- Details of why in some instances modification of the system resulted in impairment and further information explaining how losses have been calculated.
- Much more information about the attack on Weapons Station Earle, detailing the apparent attempt made by McKinnon on 23 September 2001 to delete all files on one machine.
- Evidence of the IP addresses associated with the attacks that have been recovered and their resolution to addresses associated with Mr. McKinnon.
- At the time the US witnesses made their statements it was clear that a number of investigations were still in process, the results of those investigations would be required.
- Further evidence in support of the assertion that Mr. McKinnon's activities left the computers vulnerable to further intrusion.
- Information as to the sensitivity of data held on these computer and the parameters for handling of exhibits and of defence access to them.

It is clear that Mr. McKinnon has gained unauthorised access to a large number of computers. Whilst it is unlikely that the computers used by Mr. McKinnon, such as the University of Tennessee were accessed without authorisation it is clear, either expressly or by implication that those belonging to the Military and similar agencies would have been. In interview Mr. McKinnon asserts that his sole reason for seeking access was to obtain information and that he had no malicious intent. The installation of Remotely Anywhere and the other so called hacking tools would have caused an unauthorised modification. Similarly his deletion of the log files of his activity would have amounted to an unauthorised modification and fall within section 3 (b). However he does not accept either in interview or in his section 9 statement that he had the necessary intent required by section 3 albeit that the reliability of the systems were impaired either as result of his intrusion or because the deletion of the log files caused the computers to experience problems in rebooting. Notwithstanding his posting of the message concerning disruption I consider that there is insufficient evidence to proceed in respect of a section 3 offence.

In relation to proving a section 2 offence it is necessary to show that he intended to commit or facilitate a specified offence. I am satisfied that we can show that Mr. McKinnon was aware that he was securing unauthorised access, it is also clear that his purpose in securing that access and in installing Remotely Anywhere and the other hacking software was to enable him to identify other computers in order to obtain access to them. He therefore has the necessary intent to commit further section 2 offences. Section 2 is a specified offence.

In his section 9 statement Mr. McKinnon states the offence he intended to commit was the Theft of passwords. What Mr. McKinnon actually did was to obtain passwords and subsequently use them to gain access. The passwords themselves are not property within the meaning of the Theft Act 1968, and they constitute confidential information.

Having considered the admissions I have identified 9 offences of unauthorised access with intent contrary to section 2 of the Computer Misuse Act. We are unable to lay the evidential framework to corroborate the admissions. The charges relate to admitted activity against a system which involved the unauthorised access to more than once machine. Arguably they are not duplicitous as they relate to a single course of conduct. Were Mr. McKinnon to be charged these counts might perhaps best be presented as multi offending counts.

Of greater significance is the inability to reflect Mr. McKinnon's alleged criminality. This is summarised in the Judgement of the House of Lords 2008 WL 2872468 30 July 2008.

The appellant's alleged criminality

11 *Using his home computer the appellant, through the internet, identified US Government network computers with an open Microsoft Windows connection and from those extracted the identities of certain administrative accounts and associated passwords. Having gained access to those accounts he installed unauthorised remote access and administrative software called "remotely anywhere" that enabled him to access and alter data upon the American computers at any time and without detection by virtue of the programme masquerading as a Windows operating system. Once "remotely anywhere" was installed, he then installed software facilitating both further compromises to the computers and also the concealment of his own activities.*

Using this software he was able to scan over 73,000 US Government computers for other computers and networks susceptible to similar compromise. He was thus able to lever himself from network to network and into a number of significant Government computers in different parts of the USA.

***12** The 97 computers the appellant accessed were: 53 army computers, including computers based in Virginia and Washington that control the army's military district of Washington network and are used in furtherance of national defence and security; 26 navy computers, including US Naval Weapons Station Earle, New Jersey, which was responsible for replenishing munitions and supplies for the deployed Atlantic fleet; 16 NASA computers; one Department of Defense computer; and one US Air Force computer.*

***13** Having gained access to these computers the appellant deleted data from them including critical operating system files from nine computers, the deletion of which shut down the entire US Army's Military District of Washington network of over 2000 computers for 24 hours, significantly disrupting Governmental functions; 2,455 user accounts on a US Army computer that controlled access to an Army computer network, causing these computers to reboot and become inoperable; and logs from computers at US Naval Weapons Station Earle, one of which was used for monitoring the identity, location, physical condition, staffing and battle readiness of Navy ships, deletion of these files rendering the Base's entire network of over 300 computers inoperable at a critical time immediately following 11 September 2001 and thereafter leaving the network vulnerable to other intruders.*

***14** The appellant also copied data and files onto his own computers, including operating system files containing account names and encrypted passwords from 22 computers comprising: 189 files from US Army computers, 35 files from US Navy computers (including some 950 passwords from server computers at Naval Weapons Station Earle); and six files from NASA computers.*

***15** The appellant's conduct was alleged to be intentional and calculated to influence the US Government by intimidation and coercion. It damaged computers by impairing their integrity, availability and operation of programmes, systems, information and data, rendering them unreliable. The cost of repair was alleged to total over $700,000.*

***16** Analysis of the appellant's home computer confirmed these allegations. During his interviews under caution, moreover, he admitted responsibility (although not that he had actually caused damage). He stated that his targets were high level US Army, Navy and Air Force computers and that his ultimate goal was to gain access to the US military classified information network. He admitted leaving a note on one army*

computer reading:
"US foreign policy is akin to government-sponsored terrorism these days ... It was not a mistake that there was a huge security stand down on September 11 last year ... I am SOLO. I will continue to disrupt at the highest levels ..."

From the foregoing it is clear that we are unable to frame charges that adequately reflect the alleged criminality. I consider that the inability to prosecute for offences representing the totality of offending mean that the evidential test is not met. Although Mr. McKinnon has stated his intention to plead guilty, I consider it would be an abrogation of the Code to initiate a prosecution on such a basis.

I would also need to be satisfied the prosecution would be able to discharge their duty in relation to unused material given the undoubted existence of sensitive material.

I have also considered paragraph 10 of the Code and the circumstances in which it is proper for a Crown Prosecutor to accept a guilty plea.

10.1 Defendants may want to plead guilty to some, but not all, of the charges. Alternatively, they may want to plead guilty to a different, possibly less serious, charge because they are admitting only part of the crime. Crown Prosecutors should only accept the defendant's plea if they think the court is able to pass a sentence that matches the seriousness of the offending, particularly where there are aggravating features. Crown Prosecutors must never accept a guilty plea just because it is convenient.

The inability to frame charges which reflect the totality of the offending means that the evidential test has not been met.

I am mindful of the duty imposed by paragraph 2.4 of the Code which states;
Crown Prosecutors should provide guidance and advice to investigators throughout the investigative and prosecuting process. This may include lines of inquiry, evidential requirements and assistance in any pre-charge procedures. Crown Prosecutors will be proactive in identifying and, where possible, rectifying evidential deficiencies and in bringing to an early conclusion those cases that cannot be strengthened by further investigation.

147-A-40

In 2002 following discussions with the United States Prosecutors a decision was made to cede jurisdiction, the factors relevant to that decision included;

- The fact that the 'harm' occurred in the United States. The activity was directed against the military infrastructure of the United States.
- That the investigation commenced in the United States and was ongoing.
- The witnesses of whom there were a large number were mostly located in the United States.
- That the bulk of the 'real' evidence was located in the United States. The task of gathering sufficient evidence to initiate proceedings in the UK would have been immense.
- That the United States prosecutors were able to frame charges which reflected the extent of McKinnon's criminality.
- The bulk of the 'unused' material was located in the United States. This material was likely to include sensitive material which would be best dealt with by the Courts in the United States.

In 2007 the Attorney General issued guidance entitled "*Guidance for handling criminal cases with concurrent jurisdiction between the United Kingdom and the United States of America*". In accordance with this guidance the Crown Prosecution Service has recently engaged in further discussions with the US authorities. For the reasons set out above the US still wishes to retain jurisdiction and I am satisfied that the United States remains the appropriate venue for a prosecution.

Public Interest

As I do not consider the evidential test to be met I do not go on to consider the public interest.

Material submitted by Kaim Todner

File 1

Judgement of the House of Lords 30 July 2008

The judgement includes a summary of the allegations set out above. Reference is also made to the attempt by the US authorities to negotiate a basis of plea which would involve Mr. McKinnon's travelling voluntarily to the US. This appears to have taken place between November 2002 and June 2003. The basis of the offer to Mr.

McKinnon was that he would receive a sentence of 3- 4 years imprisonment and that after serving between 6 and 12 months could be repatriated to the UK to serve the remainder with his release date being determined in accordance with UK law. In essence he would serve between 18 months and 2 years.

The request for extradition was submitted on 7 October 2004. The district judge sent the case to the Secretary of State on 10 May 2006. The Secretary of State informed Mr. McKinnon on 4 July 2006 that he had made the order for extradition. Mr. McKinnon subsequently appealed both decisions.

The principle argument advanced on behalf of Mr. McKinnon was the disparity between the sentence anticipated if he was to co operate in contrast with that if he refused which amounted to impermissible pressure to surrender his legal rights .

Judgement of the Divisional Court 3 April 2007

Appeal against decision of the District Judge and the Secretary of State.
The judgement sets out some of the evidence found on Mr. McKinnon's home computers.
The issues raised on the appeal;
That the designation of the USA as a state that was not required to furnish prima facie evidence was unlawful and ultra vires
That Mr. McKinnon's conduct did not amount to an extradition offence
That extradition was barred on the basis of extraneous considerations that the prosecution was brought because of his political opinions and the passage of time.
That extradition was incompatible with his human rights including likely length of sentence and conditions under which any sentence would have to be served.
Abuse of process, delay and possibility of substantial period of imprisonment far in excess of any likely to be imposed in the UK
That the USA had flagrant disregard for speciality

It is to be noted that the court agreed with the district judge's view that the decision of the CPS not to prosecute Mr. McKinnon was unquestionably correct.

Psychiatric Report prepared by Dr Berney on 23 August 2008

Conclusion

147-A-42

That Mr. McKinnon's combination of difficulties amount to a Pervasive Developmental disorder, that he has Aspergers Syndrome both of which are part of the Autistic Spectrum of Disorder, he also has characteristics suggesting other developmental disorder which are also associated with Autism.

He considers that Mr. McKinnon would have difficulty in judging what constitutes a serious offence. He is vulnerable to anything that is unfamiliar or novel, if he is unable to withdraw from complex situations into something more autism friendly he is likely to develop a pathological anxiety state which may result in him developing an acute psychotic disorder

Letter to Ms K Todner from the Cambridge Lifespan Asperger Syndrome Service by Professor Simon Baron- Cohen dated 8 September 2008

The assessment was to be further to that of Dr Berney.

Conclusions
Mr. McKinnon has a high score in the Autism Spectrum Quotient meaning he scores high in the number of autistic traits that he has.
His Empathy Quotient suggests he has extreme difficulties with social awareness and empathy consistent with Aspergers Syndrome.
His Childhood Autism Spectrum Test is high indicating a number of autistic traits present in childhood and consistent with having Aspergers Syndrome in childhood
His Adult Aspergers Assessment confirms his diagnosis of having Aspergers.
He concludes that, having discussed his motivation for hacking with him that he had no terrorist agenda nor did he wish to cause harm damage or loss to the US. He says he committed a crime without having any real understanding or the social legal or political importance or consequences.
His condition causes him to obsess and focus on single issues to the exclusion of almost all else.
He is presently suffering fear, distress anxiety and depression of being sent to prison and even suicidal. This comes from his parents rather than from McKinnon himself. His parents feel he lacks the social skills to cope with prison.
He considers that his emotional age or social intelligence is that of a child and in terms of criminal responsibility it is more appropriate for him to judged as having the mind of a child who inadvertently breaks a rule.

He concludes that in view of the high risk of deterioration in McKinnon's health if incarcerated in the USA there is a risk of suicide.

A number of background and academic papers are appended to his report.

Letter to Ms K Todner from the Cambridge Lifespan Asperger Syndrome Service by Professor Simon Baron- Cohen dated 4 December 2008

This is an addendum report to that of September.
He states that to the best of his knowledge Mr. McKinnon did not cause damage nor did he cause the transmission of any program.
It appears that Mr. McKinnon has expressed suicidal intentions, and fears of rape and physical assault, he believes that long term solitary confinement could increase the risk of depression and suicide. He states that Mr. McKinnon's mental health has deteriorated over the years from not knowing what is going to happen to him – this is the first time this aspect has been addressed.

He concludes that Mr. McKinnon would suffer from the following if imprisoned:
1. Aggression from other prisoners
2. Aggression from prison guards
3. Being expected to share a cell
4 Loud noises and sensory overload
5. Having to live with a large group of other people

He states with some force his concerns that Mr. McKinnon will not survive prison.
He states that the condition is not easily treatable.
He also feels that Mr. McKinnon may have difficulty understanding the trial process or participating in it properly.

Letter to European Court of Human Rights from Human Rights Watch dated 27 August 2008 with accompanying documentation

Letter concerns the possibility of Mr. McKinnon being incarcerated in a supermax high security prison and the view of Human Rights Watch that such conditions violate US treaty obligations.

Affidavit of Thomas Franklin Loflin III with attachments

167-A-44

He is a US Lawyer. He examines documentation prepared for the purpose of the extradition.
He concludes;
The US delayed in seeking extradition in order to take advantage of the new 2003 US /UK extradition treaty
That US courts do not strictly apply the doctrine of speciality
That Mr. McKinnon could be turned over to face indefinite detention without charge
That Mr. McKinnon might face special administrative measures SAMs relating to his detention
The likelihood of Mr. McKinnon be confined in a supermax prison or in a military prison
That if convicted in a Federal Court his likely sentence he gives various possible permutations but concludes that a sentence of 45 – 60 years without parole is a possibility.

Statement of Thomas Franklin Loflin III
Deals with sentencing and the conditions in Supermax prisons and Special Administrative Measures (SAMs)
The harsh conditions in supermax prisons where prisoners are frequently subject to long periods of solitary confinement.
SAMs apply to prisoners who are alleged to have endangered US security and can include without access to the outside world and have his lawyer client privileges abridged.

FILE 2
Statement of Joshua L Dratel

US Lawyer. Gives evidence concerning Sentencing in particular the plea bargaining system
Concludes that McKinnon will no longer be able to take advantage of the offer made in the proposed plea agreement and any subsequent offer will contain harsher terms

Supplemental statement of Joshua L Dratel
Considers that Mr. McKinnon is likely to be refused bail if extradited to the US

Statement of Sylvia Royce

Review Note 3

US Lawyer Describes the system for transferring prisoners serving sentences in the US to other countries and concludes that the prosecutor is able to veto any transfer.

Supplementary statement of Sylvia Royce

Statement of Karen Todner
Concerns the proposed plea agreement.

Supplemental statement Karen Todner
View that US considered any UK sentence to be too light.

Witness statement of Edmund Lawson QC
Concerns the plea agreement

Section 9 Statement of Gary McKinnon dated 9 December 2008
He indicated willingness to plead to an offence or offences contrary to section 2 of the Computer Misuse Act 1990.

Transcripts of the Interviews of McKinnon in March 2002

Letter from the NHTC
Undated, clearly prior to October 2002 states that Mr. McKinnon bail cancelled as US are to seek his extradition

Transcripts of the Interviews of Mr. McKinnon in August 2002

Statement of Janis Sharp mother of Gary McKinnon dated 22 December 2008

Concerns reasons for the late diagnosis of her son's condition.. She states that the past 7 years has taken its toll on his health and is now suffering from extreme stress, anxiety and depression, she also states that he is getting some help from Professor Baron-Cohen

Letter to DPP from Mrs Sharp dated 16 December 2008
Sets out the deterioration in McKinnon's mental and physical health due to the extradition process.

147-A-46

Review Note 3

Statement of Wilson Sharp
McKinnon's stepfather

Material supplied by Kaim Todner accompanying letter dated 4 February.

1. Witness statement of Karen Todner dated 19 January 2009
This statement adds little to her statement dated 28 December 2008. She explains that following an appearance on TV a member of the public contacted her saying that she suspected Mr. McKinnon was suffering from Aspergers syndrome and that prompted his assessment by Professor Baron – Cohen.

2. Statement of Gary McKinnon dated 5 January 2009. He states that on 19 March Geoff Donson of the NHTCU informed him of the following;

- that the NHTCU had his internet activity under surveillance
- that at no time had they observed him sending commands or codes that would cause or damage any computer
- That he would most likely be sentenced to a six month community service order.

3. Letter from Mark Spragg Solicitor of Messrs Jeffrey Green Russell Solicitors dated 21 January 2009.
Mr. Spragg was the solicitor for the 'Natwest Three' the UK bankers extradited to the US who feature in R v Bermingham and others. He explains that the then AG Lord Goldsmith and later Baroness Scotland made representations to the US authorities that bail be granted to his clients once in the USA. These representations were apparently successful. I am not entirely sure why this letter has been supplied to us, it may be suggested that these three were granted special treatment that is not available to McKinnon.

Supplied by letter on 10 February

Newspaper Article by Joseph Gutheinz dated February 2009.
States that the US criminal justice system is unable to unwilling to meet the needs of the mentally ill

Review Note 3

Comment on material supplied.

The material supports the following assertions;

1. That Mr. McKinnon suffers from Aspergers Syndrome, that imprisonment in the US is likely to be detrimental and may result in him attempting suicide or otherwise will significantly affect his mental health.

2. He is likely to receive a substantial prison sentence, and may be incarcerated in a Supermax prison subject to SAMs which practices have been condemned by Human Rights bodies. He is unlikely to be repatriated to serve his sentence in the UK.

3. That having the proceedings hanging over him for such a lengthy period is having an adverse affect on him.

These issues go to the public interest; however in so far as I am obliged to consider them I have done so. It is also clear that these issues have been canvassed in the extradition proceedings to date and have not been found to constitute a bar. The extradition process provides protection for Mr. McKinnon's ECHR rights.

Conclusion

The evidential test in the Code is not met because given the limited evidence I have, I am unable to frame charges which reflect the totality of the alleged offending.

Russell Tyner
CPS Organised Crime Division London
26 February 2009

447-A48