JUDICIARY OF
ENGLAND AND WALES

IN THE CROWN COURT AT LEICESTER (T20177165)
SENTENCING AT THE CENTRAL CRIMINAL COURT

THE QUEEN

- v -

KANE GAMBLE

SENTENCING REMARKS OF THE HON. MR JUSTICE HADDON-CAVE

Introduction

> "*The prevalence of computer crime, its potential to cause enormous damage, both to the credibility of IT systems and the way in which our society now operates, and the apparent ease with which hackers, from the confines of their own homes, can damage important public institutions, not to say individuals, cannot be understated. The fact that organisations are compelled to spend substantial sums combating this type of crime, whether committed for gain or out of bravado, and the potential impact on individuals such as those affected in this case only underlines the need for a deterrent.*" (*per* Lord Justice Leveson in *R v. Martin* [2013] EWCA Crim 1420 at [42]).

Pleas

1. On 8th September 2017, at a Plea and Trial Preparation Hearing at Leicester Crown Court, Kane Gamble pleaded (after earlier indications): (i) guilty to six offences contrary to section 1(1) of the Computer Misuse Act 1990 (Counts 1, 3, 4, 5, 6 and 9); (ii) guilty to two offences contrary to section 3(1) of the Computer Misuse Act 1990 (Counts 8 and 10), namely causing a computer to perform a function to secure unauthorised access to a program or data; and (iii) not guilty to three offences contrary to section 3ZA of the Computer Misuse Act 1990 (Counts 2, 7 & 11), namely unauthorised acts in relation to a computer causing or creating significant risk of serious damage to national security.

2. On 6th October 2017, Counts 7 and 11 on the indictment were replaced with further counts under section of 1(1) of the Computer Misuse Act 1990 to which Kane Gamble then pleaded guilty. The Crown offered no evidence on Count 2.

3. Kane Gamble stands, therefore, to be sentenced for eight offences contrary to section 1(1) of the Computer Misuse Act 1990 Act (for which the maximum penalty is 2 years imprisonment) and two offences under section 3(1) of the 1990 Act (for which the maximum penalty is 10 years imprisonment).

4. Kane Gamble was born on 2nd October 1999. He is now 18½ years old. He was:

   (i) aged 15/16 years when he committed Counts 1 and 3;
   (ii) aged 16 years when he committed Counts 4 to 11;
   (iii) aged 17 years when he pleaded guilty to Counts 1, 3-6 and 8-10;
   (iv) aged 18 years when he pleaded guilty to Counts 7 and 11.

5. I am grateful to Counsel for the Crown, Mr Lloyd-Jones QC and Ms Herbert, and Counsel for the Defence, Mr Harbage QC and Mr Barry, for their able assistance in this lengthy sentencing exercise.

The facts

6. I am going to set out the facts in some detail. This is in order to explain both the precise nature and sheer scale of Gamble's criminal activities on the Web and because it is relevant to the debate about the expert evidence regarding Gamble.

7. Gamble started an online group known as "*Crackas With Attitude*" ("CWA"). They operated as an internet quasi-hacking gang who worked together and encouraged each other. Other members included Nathan Henry who lived in Glasgow and various US citizens; Justin Liverman, Bradley Martin and Andrew Boggs. Their activities were politically motivated.

8. Over a period of eight months, between 1st June 2015 and his arrest on 9th February 2016, from his bedroom at home in Coalville, Gamble gained unauthorised access to the communication accounts of very high-ranking US intelligence officials and government employees and to US law enforcement and intelligence agency networks.

9. The group have been referred to as 'hackers' but more accurately should be called 'impersonators'. They used 'social engineering' and impersonation to hoodwink individuals and security systems and gain unauthorised access to email and other communication accounts. Social engineering involves psychological manipulation or tricking people such as call centres or helpdesk staff into performing actions or divulging confidential information, passwords and/or PIN numbers.

10. Gamble and the group's activities included often (i) subjecting victims and their families to sustained online abuse and harassment, (ii) posting substantial amounts of personal and sensitive data on the Internet, and (iii) publicising and bragging about their activities on social media, as I shall outline.

Count 1 – John Brennan (Director of the Central Intelligence Agency) ("CIA")

11. In June 2015, Gamble and CWA decided to target John Brennan, the then Director of the CIA. Gamble impersonated employees of a US American telecommunications company, *Verizon*, and Mr Brennan himself, in order to gain access to Mr Brennan's *Verizon* ISP account and obtain his personal details, router serial number, MAC address, telephone numbers and home address.

12. On 11th October 2015, Gamble impersonated Mr Brennan, gained access and changed Mr Brennan's *Verizon* account PIN number and security questions and posted on his *Twitter* account (*@phphax*) an image depicting CIA Director Brennan with a label across his forehead with the names "*Cracka*" and "*Cubed*" (online names for himself and Henry).

13. On 12th October 2015, using *Skype*, Gamble impersonated Mr Brennan and initiated a password reset in order to gain unauthorized access to Mr Brennan's *AOL* account. He boasted to Henry in an online chat that he was "*jacking*" Mr Brennan's account and had access to Mr Brennan's email contact list. Gamble held Mr Brennan's social security number and had accessed Mr Brennan's *iCloud*.

14. CWA also targeted Mr Brennan's wife, Kathy Brennan. On the 12th October 2015, Henry took over the *Twitter* account of Kathy Brennan and gave Gamble the new password. Kathy Brennan received notifications of unusual logins, password changes and account password changes when neither she nor her husband had made any such requests.

15. Gamble and CWA made other intrusions into the Brennan family's life. On 13th October 2015, Gamble boasted to Henry on *Skype* that he had gained remote access to Kathy Brennan's iPad and that he was going to "*wake everyone up*". He also gained access to Kathy Brennan's *AOL* account by impersonating her and persuaded *AOL* to change the account details, reset the password and change the answers to security questions to "*hacked*", "*hacker*" and "*V for Vendetta*" (a graphic novel and film about an anarchist freedom fighter who used terrorist acts to fight oppression). The alternative contact email address for the account was also changed a number of times; one of the new addresses provided incorporated the term MILF ("*mother I'd like to fuck*").

16. Gamble also made numerous telephone calls to the Brennan family home in the US. On 13th October 2015, he called Mrs Brennan whilst she was on the phone to *AOL* in the process of reporting that her account had been compromised. Between 13th and 16th October 2015 he called Kyle Brennan (Mr Brennan's son) eleven times.

17. Gamble and CWA used this access to obtain sensitive documents referring to operations in Afghanistan and Iran, and Mr Brennan's email address list. From the 12th October 2015 onwards, Gamble's *Twitter* account *@phphax* tweeted references to CIA and images of John Brennan and his family. Gamble tweeted: "*You're now about to witness the strength of #CWA XD. @CIA Step your game up homies, we own everything of you :(*". He also posted *#FreePalestine #CWA* with an image of Mr Brennan's car insurance details. Gamble made further calls to the Brennan family and tried to re-activate Kathy Brennan's *AOL* account after she had cancelled it.

18. In a *Skype* exchange with Henry on 17th October 2015, Gamble expressed his wish to "*leak John Brennan's email list*" comprising over 700 email addresses. The pair discussed how and where they were going to post this information. In due course, over 1,300 contact email addresses were posted *via Pastebin*.

19. Gamble also spoke to a number of journalists including Wesley Bruer. When asked by Bruer on 19th October 2015 (*via* the CWA *Twitter* account) why the group had targeted John Brennan and Jeh Johnson (see below), Gamble said: "*John and Jeh are both very big people and high ranking people… if we hacked them they would be ashamed*"… "*It was really because the government are killing innocent people and they also fund for killing innocent Israel people to be killed*". He said that he was not scared to get caught. He promised to release more information soon.

20. After 21st October 2015, the information obtained by Gamble from the Brennan accounts was posted on the *Wikileaks* website. Gamble shared other emails and information that he had obtained (including employees' social security numbers) with other parties. The *@CWA Twitter* account posted a number of images showing various CIA data releases, including Mr Brennan's Standard Form 86 ("*SF86*") entitled "*Questionnaire for National Security Positions*" containing highly personal information about Mr Brennan and family members.

Count 3 – Jeh Johnson (Secretary of Homeland Security)

21. On 5th July 2015, Gamble boasted on *Skype* that he could socially engineer anyone and intended to obtain the social security number of the US Head of Homeland Security, Jeh Johnson. A series of calls were made on the same day from Gamble's *virtthe2nd Gmail* account to Mr Johnson's personal telephone number and the US Department of Homeland Security ("DHS").

22. On the 12th July 2015, Gamble bragged on *Skype* that he could listen to Mr Johnson's voicemails, send texts from his phone and had gained access to his *Comcast* account and call logs by "*doxing*" him, *i.e.* by collecting his personal information and using that to "*jack*" his account. Mr Johnson's contacts and their phone numbers were subsequently posted online.

23. Between 11th and 15th July 2015, a series of calls were made to Mr Johnson and his wife, Mrs DiMarco, from Gamble's *virtthe2nd Gmail* account. From the 15th July 2015 onwards, there were further CWA discussions on *Skype* about Mr Johnson with images from the personal *Comcast* account of the Johnson family. Gamble said: "*Head of homeland is egit retard, I called him and told him I shrekt him and he still hasn't done shit about his Comcast account. LOL fuckinga*".

24. On the 18th July 2015, multiple calls were made to Mr Johnson and his wife from Gamble's *virtthe2nd Gmail* account. Mrs DiMarco received a voicemail message on her personal mobile phone stating "*Hi Spooky, am I scaring you*?". Over a period of approximately one month, several calls to the landline and Mrs DiMarco's mobile were received from a blocked number. Further uploads of account information were also made. Gamble recounted that, during one call made to the house, the Secret Service had been there and commented "*This is so funny*☺".

25. On 26th July 2015, Gamble reported on *Skype* that he had made unauthorised changes to the Johnson's home devices *via* their *Comcast* account. A message was sent to a television stating "*I own you*". From the 27th July 2015, further calls were made to Mrs DiMarco and the DHS from Gamble's *virtthe2nd Gmail* account. Subsequently, Gamble boasted about "*owning*" Mr Johnson via a *Skype* message.

26. From 4th August 2015, further calls were made to Mrs DiMarco and the DHS from Gamble's *virtthe2nd Gmail* account. Gamble continued to share images of the DHS systems. Documents were uploaded by Bradley Martin to *Pastebin*. Forensic examination of a device seized from Martin revealed chat on the *KIK* messenger app where *Queryjy* (*i.e.* Martin) discussed being asked by *Cracka* (*i.e.* Gamble) to upload the Jeh Johnson information to *Pastebin* if *Cracka* was caught.

27. From the 20th August 2015 onwards, Mrs DiMarco continued to receive calls to her mobile phone. On 25th August, she received a text message stating "*This account in now under the control of FederalSecurity aka FedSec, we will leak everything on this account and everything of Jeh Johnson if the US Army does not stop killing innocent civilians in Iraq, Afghanistan, Egypt, Syria. #FreePalestine*". This text message appeared to originate from Mr Johnson's home telephone number in New Jersey.

28. On 27th August 2015, a *Skype* chat between Gamble and Henry involved Gamble sending pictures of Mr Johnson, obtained from a family *Shutterfly* account, and messages sent on *Facebook*. The pair mocked Mr Johnson. On 19th September 2015, Gamble posted a series of tweets from the *Twitter* account *@phphax* about Jeh Johnson in a similarly mocking vein. In September 2015 Gamble posted an image of Mr Johnson's daughter and a message saying that he would "*bang your daughter*".

29. From the beginning of October 2015, Gamble made a series of tweets with posted images in relation to Mr Johnson and Homeland Security. Including other taunts, he said:

- "*I might start my attacks again against @DHSGov and maybe ruin Jeh's life completely, maybe empty his CC [Credit Card]*"
- "*oh shit, meydey meydey, jeh Johnson of @DHSgov comcast account has been compromised yet again by me, oh noessss!*"
- "*I guess shit is going to get real again @DHSgov, lifes a bitch D:*"
- "*Stop killing innocent people or the leak will be posted again. Your leaders account had been jacked. D: @DHSgov*"
- "*I found your parents number in your call logs and he said I'm in deep shit, pls no drone me pls @DHSgov*"
- "*I have your number, If you call again, you're fucked! fuck u pussy fuck face I'll call u again and again till u cry pussy wrinkly fuck*"
- "*Would you look at that, every time Jeh's parents call him, they're forwarded to a Stop War Organisation. #StopWars*"

30. It would appear that Gamble had, meanwhile, deleted the information that he had on Mr Johnson, as a precaution, because Martin had been raided. He told Henry that he had had to spend time re-acquiring the information and to "*re-jack*" Mr Johnson's account. This coincided, from 4th October 2015 onwards, with further calls made to *Comcast*, Mr Johnson, Mrs DiMarco and the DHS. In addition, Gamble and Henry discussed phoning an online pharmacy to gain access to Mr Johnson's medical information; a call was duly made a few days later from Gamble's account.

Count 4 – Avril Haines (Deputy National Security Advisor)

31. On the 17th October 2015, Gamble and Henry discussed on *Skype* the details that they had collected for Avril Haines, a senior White House official and Deputy National Security Adviser, which included her name, phone number and home address. They planned to obtain further information by pretending to work for *Comcast* using the name 'Derek'. 'Derek' made calls to *Comcast* attempting to gain access to Avril Haines' account and asking for her MAC ID on their router and a password reset, quoting Ms Haines' name, phone number, the address in Washington and details of her *@comcast* email account. *Comcast* provided a new password.

32. Gamble and Henry then looked at the calls and emails Ms Haines had made on her *Comcast* account and discussed publicly releasing her information. In due course, several tweets from the CWA *Twitter* feed posted Ms Haines' call logs.

33. Gamble then set about, as he had done before, abusing the personal information that he had so obtained. On 18th October 2015, Gamble's *virtthe2nd Gmail* account made a call to the home number of Ms Haines' partner, David Davighi. On the 18th January 2016, *Motherboard.vice* published an article entitled "*Teens who hacked CIA Director also hit White House Official*". In the article, "*Cracka*" (*i.e.* Gamble) boasted about his other targets, including Avril Haines.

Count 5 – Amy Hess (Executive Assistant Director of FBI Science & Technology Branch)

34. In a *Jabber* conversation on 19th December 2015 between Gamble and Liverman, they discussed Amy Hess as a target. Amy Hess was an Executive Assistant Director at the FBI and oversaw the Bureau's Science and Technology Branch. Gamble had done some research and knew her background and career history, and was pleased she was on *Comcast*, whose security he could bypass. Liverman suggested that it was time "*to fuck her up*".

35. Gamble again used social engineering and pretended to be Ms Hess' husband, Robert Novotny, or a *Comcast Chat* employee. On 19th December 2015, Gamble, as 'Robert' had a *livechat* with a *Comcast Chat* employee. Gamble made several attempts to obtain the PIN number, account login, billing details and modem password on her *Comcast* account. On the fourth call, Gamble obtained her MAC ID and modem serial number and gained access to Ms Hess' *Comcast* device and her personal information which he downloaded onto his desktop computer.

36. On 19th December 2015 Gamble and Liverman discussed gaining access to Ms Hess' call logs and "*dumping*" them (*i.e.* making them public). On 23rd December they agreed that Gamble would do this.

37. On 24th December 2015, Ms Hess was notified by the FBI that subjects had posted her call logs on *CryptoBin*. She was also advised of a *Twitter* posting by "'*Cracka@dick.the reject*" stating: "*Merry Christmas@FBI Amy Hess Call Logs cryptobin.org*". The post provided the location and password to access her call logs.

38. Further, the film "*Hackers*" was recorded and saved onto Ms Hess' personal digital recorder at home. Gamble and Liverman exchanged screenshots of films downloaded onto this device ("*V for Vendetta*" and "*After Porn Ends*" as well as "*Hackers*"). Ms Hess' *Comcast* account list of equipment had also been changed to derogatory and obscene phrases. Gamble changed Amy Hess's voicemail settings from English to Spanish commenting "*lets hope this bitch knows Spanish*". Control was taken of her cable boxes; they were renamed, *inter alia*, as "*amy is a slut*" and "*fuck you*". On 19th December 2015, Gamble shared images of the equipment list with Liverman.

39. Ms Hess' husband received a number of calls and actually spoke to the caller. Examination of Gamble's v*irtthe2nd Gmail* account showed that: (i) 12 calls were made to *Comcast* on 19th December and 3 calls to Ms Hess; (ii) 5 calls were made to Ms Hess on 20th December; and (iii) 5 calls were made to Ms Hess on 22nd December 2015. During some of these calls, Gamble was simultaneously chatting online with Liverman about what was happening.

Count 6 & 7 – Mark Giuliano (Deputy Director Federal Bureau of Investigation) & FBI's LEEP (Law Enforcement Exchange Portal)

40. Between 29th October and 16th November 2015, Gamble gained unauthorised access to the *Comcast* communication and e-mail account of the then Deputy Director of the FBI, Mark Giuliano (Count 6). Again, 'social engineering' was used, with Gamble impersonating Mr Giuliano and obtaining personal information. Gamble obtained unauthorised access (*via* helpdesks) to the FBI's Law Enforcement Enterprise Portal ("LEEP") (Count 6). LEEP is described by the FBI as "…*a gateway providing law enforcement agencies, intelligence groups and criminal justice entities access to beneficial resources*". Once through the gateway, Gamble accessed various parts of the network (including the Regional Information Sharing Systems ("RISSNET"), FBI Special Interest Groups ("SIG") and the Joint Automated Booking System ("JABS")), obtained data and posted it on *Twitter*.

41. Between 30th October and 2nd November 2015, Gamble made numerous telephone calls to Mr Giuliano, *Comcast* and the FBI. Gamble, impersonating Mr Giuliano, gained personal information from *Comcast* about Mr Giuliano, gained unauthorized access to his account, and reset the password of Mr Giuliano's wife's *Comcast* account.

42. Mr Giuliano received multiple telephone calls to his official FBI phone, as well as calls to the family home phone, his wife's mobile phone and those of his children. Telephone calls were also made to family and friends, as well as local businesses used by the family. This went on for several weeks, resulting in the phone numbers and email addresses having to be changed. Due to the calls, the family required physical surveillance and protection from uniformed police officers.

43. On 1st November 2015, in *Jabber* chat with Liverman, Gamble stated his intention to do a 'hack' for the 5th of November. They discussed the information that Gamble had obtained thus far. Gamble was excited by the prospect of taking the account of the "*second highest dude in the FBI*". Gamble and Henry chatted again the next day. Gamble recounted the calls he had made to Mr Giuliano and people in his call logs. They discussed efforts to be made to counteract changes that Mr Giuliano had made to his username and password. They also made plans to 'phonebomb' his number, *i.e.* to divert all incoming calls to another number. Gamble did not personally 'phone bomb' Mark Giuliano's telephone account but did provide the requisite details to Liverman to enable him to make the repeated calls and leave threatening voicemails over the course of two days with a 'burner' phone.

44. Mr Giuliano describes how access was gained to his FBI accounts *via* the Law Enforcement Online ("LEO") helpdesk. His account password was changed and emails sent to others pretending to be him. Sensitive information about the identity of other law enforcement officers inside the United States was obtained. CWA members, including Gamble, posted this information online for others to see. Mr Giuliano states that in addition to the financial and reputational costs incurred, these actions created a tangible vulnerability to the safety of government personnel, whose personal information was compromised. In his view, the information could be used to further nefarious purposes by criminals, terrorists and nation states.

45. Once they had gained access to Mr Giuliano's LEO portal, CWA were able to access JABS. JABS contains information on alleged criminal offenders who have been arrested and booked in by a Federal, State or local agency. This information consists of biographical data, place and time of arrest, jail location, charge, armed description and other records.

46. Gamble made concerted attempts to access the LEEP portal (Count 7). This began on 3rd November 2015 with calls using an archived user ID belonging to Mark Giuliano. At the same time, Gamble claimed in a news article to be targeting more US Government officials and boasted on *Twitter* about targeting Mr Giuliano. As "*Cracka*", he posted *Comcast* screenshots as proof of this. Gamble obtained the last four digits of Judy Giuliano's credit card and made repeated demanding and alarming calls to her hairdressing salon in Grayson, Georgia. In a statement from the Bella Flore Salon, employees describe receiving demanding and alarming calls several times a day.

47. In an online chat with Liverman, Gamble shared with him the fruits of his unauthorised access to the LEEP portal using Mr Giuliano's credentials. He said "…*this is so serious im fucking shaking*". Gamble had obviously been able to explore many, but not all, parts of the LEEP portal. Gamble clearly appreciated the scale of what he had done. In chat, Gamble remarked that it was a huge database which he was clearly keen to search for Officer's details: "…*this has to be the biggest hack ever - i have access to all tools feds use for bg [background] checks*". He described all the different systems he had access to and what they contained, and speculated that he might have access forever. Gamble also ran a search for a journalist William Turton and for Jeremy Hammond, a convicted hacker, and claimed that he had seen his fingerprints in the hacked files. He discussed being caught and how the activity would just look like Mr Giuliano accessed the data. Gamble then stated he may have lost access to the system and called the helpdesk.

48. The FBI confirmed that, on 4th December 2015, Gamble made determined efforts to unlock the account and re-gain access to LEEP. He socially engineered a password change but was then locked out. That day he had additionally accessed, within the portal, RISSNET and SIG. The SIG is open to all sworn and non-sworn FBI personnel; effectively, it is an address book. Prior to being locked out, Gamble was able to obtain at least 1,000 names in the members' list of the SIG.

49. A forensic examination of Gamble's desktop computer revealed two text documents containing names of Officers, organisation details and contact details. The first text document was 593 pages long; the second text document was 327 pages long. Some of this information, and the JABS search query for hacker Jeremy Hammond, were posted to *Pastebin*. Documents containing Mr Giuliano's personal details were also found.

50. From 6th to 14th November 2015, Gamble continued his efforts to regain access by repeatedly calling the FBI and CJIS ("Criminal Justice Information Services") helpdesks. He made calls impersonating both Mr Giuliano and a Marcus Bramer of the FBI. He tried to bluff a call handler who, as a matter of coincidence, had been at the same school as Judy Giuliano. Examination of Gamble's computer showed that, on 21st November 2015, a slow and deep network mapping scan had been undertaken of the CJIS website.

51. In tweets, Gamble made reference to information found within the LEEP portal, in particular, the details of Officer Darren Wilson. Officer Wilson was the US Police Officer who shot and fatally wounded Michael Brown, an 18 year old unarmed black man, in Ferguson, Missouri on 9th August 2014. Gamble posted Officer Wilson's personal details and email address. Gamble acknowledged that, as he thought, his actions were putting lives at risk. On 6th November 2015, during a *Jabber* conversation with Liverman about releasing details of government employees, Gamble said:

- "*it turns out what we have is a lot more sensitive than we thought*"
- "*i think it'd get more attention when we release more*"
- "*i thought about not releasing any more info because it put lives at risk but then i thought, they are killing innocent people everyday*"

52. In December 2015 and into January 2016, Gamble continued discussing online what he had done inside the FBI and CJIS networks and within LEEP. On 18th January 2016, Gamble boasted to a journalist regarding the LEO breach: "*lol, ye mann, that was the best breach everrr - basically owned all of united states convicts…. i have every fbi employee's name, position, email, city and state too*".

53. The Crown are unable to place a financial loss on this network intrusion. However, it is clear that a considerable number of staff members were affected by Gamble's activities, ranging from FBI Executive Management down to tech developers and system administrators. At least 100-140 hours of staff time over a period of months was spent conducting damage control. As a result, numerous other projects were postponed or cancelled. All three helpdesks, LEEP, LEO and CJIS, suffered loss and disruption in the form of unexpected overtime and reprioritisation of staff. As a result of the posting of the screenshots on external web sites, LEEP suffered serious impact to its brand integrity and trust within its user community. There was loss of membership, as the site was no longer trusted, and individuals felt personally hurt by their identity being disclosed in a public manner. Several law enforcement partners decided to disconnect their services until the FBI could prove that changes had been made.

Count 8 – James Clapper (Director of National Intelligence)

54. Forensic examination of Gamble's laptop device revealed a *Notepad*++ document that contained the personal address and phone number for the US Director of National Intelligence, James Clapper. The document also contained Mr Clapper's account number, PIN, username, password, WiFi password, network name, security question answer and further account details. The file was created on 5th January 2016. The same day, *Verizon* customer support received calls from someone posing as Mr Clapper asking about the account number. Using his *Skype* account *Jerr.Strong*, Gamble, armed with the correct PIN, was able to change the user ID and obtain a temporary password for the account. In further chat, Gamble was able to reset the password and thus take control of the account. In *Jabber* chat conversations with Liverman, Gamble confirmed and proved that he had hacked Mr Clapper's *LinkedIn* account and that he had access to Mrs Susan Clapper's email and Mr Clapper's private email. He wanted access to Clapper's government email. He said "*that's where the juicy shit is*".

55. Unauthorised access and abuse of Mr Clapper's account continued. Evidence supporting Gamble's involvement was again found on his laptop. On 9th January 2016, Gamble, pretending to be Mr Clapper, called *Verizon* to enquire about call forwarding. In due course, Gamble, having compromised the account, caused further disruption by altering the Clapper home phone so as to forward all incoming calls to the number for the *Free Palestine Movement*.

56. Between 10th and 11th January 2016, Gamble tweeted a number of times as *@Dickreject* referring to James Clapper in derogatory terms. He boasted on *Twitter* about what he had done and proved his successes to an author and a journalist by sending images of Susan Clapper's Yahoo Mail account, her call logs and files and folders relating to the National Geospatial Intelligence Agency ("NGA"), the National Security Agency ("NSA") and other government documents. Gamble initially claimed that someone called 'Shady' carried out the hack, but stated: "*i know everything about this breach i was there for the whole thing*". Subsequently, Gamble using *@Dickreject* admitted that it was him who carried out the attack and not 'Shady'.

Count 9 – Vonna Weir Heaton (Former Director of the National Geospatial Intelligence Agency)

57. Gamble gained unauthorised access to the communication account of the former Director of the NGA, Vonna Weir Heaton. He did this by using his control of Mr Clapper's account. In *Jabber* chat on 10th January 2016, Gamble said "*this email of clapper's is very useful to fool these retards into thinking im him ;)……i cant waitt lmao ... want me some docsszszsz*". Gamble was able to use James Clapper's account to pose as Mr Clapper and ask Ms Heaton to send him sensitive documents relating to the NGA. The size of the files requested meant that this was ultimately unsuccessful. Gamble commented "*she keeps*

calling me sir thinking im him lmao". Forensic examination of Gamble's laptop identified a number of documents that relate to the NGA, including briefings, governance plans, employee details and all of Ms Heaton's personal security information.

58. In her statement, Ms Heaton describes how, during January 2016, she realised that her social media accounts had been hacked and that inappropriate messages were being sent to her family and friends as though from her. Hate-speech and profane messages were posted on Ms Heaton's compromised social media causing her huge upset. She also became aware that her *LinkedIn* account had been compromised. Gamble was controlling these accounts. Examination of Gamble's laptop identified access to Ms Heaton's *LinkedIn*, *Twitter* and *Facebook* accounts. In messages exchanged with Liverman, Gamble confirmed that he had forwarded on to *Wikileaks* documents sent by Ms Heaton. He explained that he had been able to defeat her efforts to re-gain control of her *Facebook* account. Gamble said to a journalist in a direct *Twitter* message regarding Ms Heaton's *Facebook*: "*shes a government retard and deserves everything bad to happen to her just like every other gov loser thats gonna be breached*".

Count 10 – John Holdren (White House Science & Technology Advisor)

59. John Holdren, a White House Science and Technology Advisor, also became a target for Gamble. In *Jabber* chat with Liverman on 17th January 2016, Gamble said "*I hope I fuck over these whitehOuse fags*" referring to Mr Holdren. Gamble had a link to the White House website and to the Office of Science and Technology Policy showing Mr Holdren as the Director. On 18th January 2016, Gamble created a *Notepad* document listing Mr Holdren's *Comcast* user account details and password and a list of his call logs. Gamble had extensively searched the internet in order to build up a portfolio of personal information about Mr Holdren and his family.

60. Gamble used the same methods as before to gain unauthorised access to Mr Holdren's *Comcast* account. Gamble made calls to the Holdren home telephone number. When chatting online to journalist Mr Lorenzo, Gamble asserted that both he and Henry had called Mr Holdren. Advanced Call Forwarding was then activated for the John Holdren account, forwarding his incoming calls, again to the *Free Palestine Movement*.

61. Further *Jabber* chat claimed that a CWA member Fearz got into Mr Holdren's account, using '*spear phishing*' by sending Mrs Cheryl Holdren an email, claiming to be her husband John, asking what the password for their *Xfinity* account was. A *Jabber* conversation on 18th January 2016 found on Gamble's laptop, revealed that Gamble believed that he still had access to the *Xfinity* account. On the same day Gamble offered Mr Holdren's logs to Liverman for posting and uploaded them to *Pastebin* for Liverman to inspect.

62. On 18th and 30th January 2016, hoax calls were made to the Falmouth Police Department resulting in armed officers being sent to John Holdren's address. The practice was known as '*swatting*' (after the law enforcement Special Weapons And Tactics ("SWAT") teams. This would involve a collective of individuals using the *Skype* conference call facility to call the local police and make a false report of a violent act in progress; one member of the collective making the call whilst the others listen. They are aware that in the US any violent report will likely lead to the deployment of a SWAT team. Such deployments are often heavily reported in the media, including live coverage. The collective will then watch live media reporting and enjoy the harassment, alarm and distress the hoax causes. Gamble was well aware of what 'swatting' entailed and the ensuing 'chaos' caused, having previously undertaken a number of such calls himself. He was well aware that US police officers are routinely armed and that they would inevitably treat, with the utmost seriousness, a call from an intruder claiming to be inside the home address of a senior White House official.

Count 11 – US Department of Justice

63. Between 26th January and 4th February 2016, Gamble gained extensive unauthorised access to the US Department of Justice ("DOJ") network using compromised details about a former employee, Joe Green. Again, using 'social engineering' *via* contacts with the helpdesk, Gamble gained user level access to the Civil Division Network and, within that, the Case Information Management System ("CIMS"). He gathered documents and 'exfiltrated' data. Gamble obtained access over six different days for some twenty-eight hours in total.

64. Gamble obtained a substantial amount of information from his unauthorised access to the DOJ network, including files on civil court cases such as the BP Deepwater Horizon oil spill, forensic reports and, more importantly, details of 9,000 DHS and 20,000 FBI employees. In *Jabber* chat with Henry on 27th January 2016, Gamble boasted that he had a list of all DHS employees.

65. Gamble shared this data with Henry and in February 2016 posted the DHS and FBI employee details on *CryptoBin*. The lists went through in alphabetical order from A to Z and the posts were entitled "*This is for Palestine*" and "*Long Live Palestine*".

66. The US DOJ spent over $39,760 (£27,509) to resolve the issues arising from this intrusion to their network and have also suffered substantial reputational damage.

Arrest of Gamble

67. Gamble was arrested by the South East Regional Cybercrime unit on the 9th February 2016 at his home in Coalville, Leicestershire. His arrest was brought forward at the request of the FBI. The full extent of the data taken from the DOJ network was of such concern that it was thought vital to secure this data before any further sensitive information could be publicly released.

Basis of plea

68. The Defence submitted a detailed Basis of Plea (undated) and an Addendum to Basis of Plea document, dated 6th October 2017, which I have read carefully and take into account. Gamble stated that his motivations were "…*to draw attention to perceived injustices and wrongs for which he held the law enforcement and intelligence authorities in the USA responsible*". He denied seeking to profit financially from any of his criminal actions.

69. Gamble's Basis of Plea was not fully accepted by the Crown. I am satisfied, to the requisite standard of proof, that the Crown's objections to Gamble's Basis of Plea are justified and the Crown's version of the disputed facts is broadly correct. In particular:

    (1) Gamble fully appreciated the personal upset and alarm that his actions were causing. Indeed, this was very much his intention, by his actions, to upset, annoy and harass his targets and their family members. He held them in contempt, repeatedly referring to them online as "*retards*".

    (2) Gamble founded the CWA "*Crackas with Attitude*" group. In *Jabber* chat with a journalist, Gamble was asked by Mr Lorenzo how CWA started and replied: "…*[I]t all started by me getting more and more annoyed at how corrupt and cold blodded the us gov are, so I decided to do something about it*". When asked why the group ended Gamble said "*because it was just me doing all the work*".

(3) Whilst it is not known whether Gamble spoke to John Brennan's children, it is clear that between 13th and 16th October 2015 he called Kyle Brennan's phone 11 times, as set out above.

(4) It is accepted that others ('Cubed') took over the *Twitter* account of Kathy Brennan, although Gamble was provided with the new password. Gamble took an active interest in the intrusions into the Brennan family's life, for example the taking control of Kathy Brennan's iPad.

(5) Gamble asserts that he did not threaten Jeh Johnson. However, (i) on 18th July 2015 calls were made from Gamble's *Gmail* account (*wirtthe2nd*) to Mr Johnson and his wife, Mrs DiMarco. A voicemail left for Mrs DiMarco said "*Hi Spooky, am I scaring you?*"; (ii) in September 2015 Gamble posted an image of Jeh Johnson's daughter and a message saying that he would "*bang your daughter*"; and (iii) in October 2015, Gamble tweeted regarding calls to Mr Johnson and his wife saying, *inter alia*, "*fuck u pussy fuck face I'll call u again and again till u cry pussy wrinkly fuck*". He contemplated re-starting his attacks and "*maybe ruin Jeh's life completely*".

(6) It is correct that Gamble did not 'phone bomb' Mark Giuliano's telephone account. He did, however, provide the requisite details to Liverman (*d3f4ult*) who made the repeated calls and left threatening voicemails over the course of two days with a 'burner' phone.

(7) It is correct that Gamble did not call James Clapper's wife. He did, however, provide the requisite contact details to the reporter Mr Lorenzo, then deleted the call log of his contact with Mr Lorenzo.

(8) Gamble claims that he did not ring John Holdren on 18th January 2016. However, when chatting online to journalist Mr Lorenzo, Gamble asserted that both he and his associate Henry had called Mr Holdren.

(9) Gamble does not accept that he intended or expected that armed officers would attend following the hoax calls that he made to the Falmouth Police Department. However, he was very well aware of what 'swatting' entailed (see above).

Sentencing young people

70. I have had careful regard to the guidance given in the Sentencing Council's *Definitive Guideline - Sentencing Children and Young People* and, in particular, the following principles:

(1) "When sentencing children or young people the court must have regard to the principal aim of the youth justice system which is to prevent offending by children and young people and the welfare of the child or young person" [1.1];

(2) "The approach to sentencing should be individualistic and focused on the child or young person as opposed to the offence. The sentence should focus on rehabilitation where possible. A court should consider the effect the sentence is likely to have on the child or young person as well as any underlying factors contributing to the offending behaviour" [1.2];

(3) "The primary purpose of the youth justice system is to encourage children and young people to take responsibility for their own actions and promote reintegration into society rather than to punish" [1.4];

(4) "It is important to bear in mind any factors that may diminish the culpability of a child or young person. The children and young people are not full developed and they have not obtained full maturity. As such, this can impact on their decision making and risk taking behaviour. It is important to consider the extent to which the child or young person has been acting impulsively and whether their conduct has been affected by inexperience, emotional volatility or negative influences. They may not fully appreciate the effect their actions can have on other people and may not be capable of fully understanding the distress and pain they cause to the victims of their crimes. …When considering a child or young person's age their emotional and developmental age is of at least equal importance to their chronological age (if not greater)" [1.5].

(5) "For these reasons, children and young people are likely to benefit from being given an opportunity to address their behaviour and may be receptive to changing their conduct. They should, if possible, be given the opportunity to learn from their mistakes without undue penalisation or stigma…" [1.6].

71. Paragraph 1.10 of the Sentencing Guidelines provides as follows:

> "1.10 Section 142 of the Criminal Justice Act 2003 sets out the purposes of sentencing for offenders who are over 18 on the date of conviction. That Act was amended in 2008 to add section 142A which sets out the purposes of sentencing for children and young people, subject to a commencement order being made. The difference between the purposes of sentencing for those under and over 18 is that section 142A does not include as a purpose of sentencing 'the reduction of crime (including its reduction by deterrence)'. Section 142A has not been brought into effect. Unless and until that happens, deterrence can be a factor in sentencing children and young people although normally it should be restricted to serious offences and can, and often will, be outweighed by considerations of the child or young person's welfare"

72. The Guidelines deal with the sentencing problems that occur when a significant age threshold is crossed between commission of the offence and sentence:

> "*Crossing a significant age threshold between commission of offence and sentence*
>
> 6.1 There will be occasions when an increase in the age of a child or young person will result in the maximum sentence on the date of *the finding of guilt* being greater than that available on the date on which the offence was *committed* (primarily turning 12, 15 or 18 years old).
>
> 6.2 In such situations the court should take as its starting point the sentence likely to have been imposed on the date at which the offence was committed. This includes young people who attain the age of 18 between the *commission* and *the finding of guilt* of the offence but when this occurs the purpose of sentencing adult offenders has to be taken into account, which is:
>
> • the punishment of offenders;
> • the reduction of crime (including its reduction by deterrence);
> • the reform and rehabilitation of offenders;
> • the protection of the public; and
> • the making of reparation by offenders to persons affected by their offences.

> 6.3 When any significant age threshold is passed it will rarely be appropriate that a more severe sentence than the maximum that the court could have imposed at the time the offence was committed should be imposed. However, a sentence at or close to that maximum may be appropriate."

73. Offences contrary to sections 1(1) & 3(1) of the Computer Misuse Act 1990 are 'either way' offences. For either way offences, offenders aged 15-17 years can be sentenced to a Detention and Training Order with a maximum length of 24 months.

74. Recently, in *R v* Clarke [2018] EWCA Crim 185, the Lord Chief Justice The Lord Burnett of Maldon emphasised the importance of looking carefully at the age, maturity and progress of the young offender in each case:

> "5. Reaching the age of 18 has many legal consequences, but it does not present a cliff edge for the purposes of sentencing. So much has long been clear. The discussion in *R v Peters* [2005] EWCA Crim 605, [2005] 2 Cr App R(S) 101 is an example of its application: See paras [10]-[12]. Full maturity and all the attributes of adulthood are not magically conferred on young people on their 18th birthdays. Experience of life reflected in scientific research (e.g. 'The Age of Adolescence': thelancet.com/child-adolescent; 17 January 2018) is that young people continue to mature, albeit at different rates, for some time beyond their 18th birthdays. The youth and maturity of an offender will be factors that inform any sentencing decision, even if an offender has passed his or her 18th birthday."

Dispute on expert psychiatric evidence

75. There was a dispute regarding expert psychiatric evidence and whether Gamble should be sentenced on the basis that he has Autism Spectrum Disorder ("ASD"). The Defence relied upon the evidence of Consultant Forensic Psychiatrist Dr Steffan Davies who said Gamble did have ASD. The Crown relied upon the evidence of Consultant Forensic Psychiatrist Dr Philip Joseph who was of the opinion that Gamble did not have ASD (or, alternatively, only in a minor way). Both experts served detailed written reports.

76. In order to resolve this dispute, I heard live evidence from both experts on 19th January 2018 who were examined in chief and cross-examined by Counsel. I also considered detailed and helpful written submissions from Counsel on the expert evidence for which I am grateful.

Dr Davies's evidence

77. Dr Davies, who has a particular interest in this field, was of the firm opinion that Gamble was, and is, suffering from ASD. He describes his presentation and social isolation as very typical and entirely consistent with the results of the diagnostic assessment carried out by Emma Woodhouse, a neuro-developmental specialist. The crux of Dr Davies' evidence was that Gamble was only 15-16 years old at the time of offending but his emotional maturity would have been even lower, such that he did not appreciate the impact his offences would have in the real world or their seriousness. Dr Davies specifically attributed Gamble's lack of emotional maturity to his ASD. In evidence, Dr Davies noted that Gamble did not think about the consequences of his action in the real world at the time; and, due to his ASD, Gamble's understanding of social relationships and emotional impacts was below that of an average 15 year-old; and he not realise the seriousness of what he was doing until he was in a police cell. Towards the end of his evidence in chief, Dr Davies gave his opinion that Gamble was operating more like a 12 or 13 year-old at the time.

Dr Joseph's evidence

78. Dr Joseph, a renowned forensic psychiatrist of extensive experience, doubted whether Gamble suffered from ASD (but said, if he did, it was only mild in nature). Dr Joseph said there was a danger of attributing features to autism when there might have other explanations: for example, Gamble's vomiting phobia may have caused him to become socially isolated. Emma Woodhouse's tests were not, of themselves, diagnostic and they should not be considered in isolation. There was no evidence of the typical impairments associated with ASD. The Child & Adolescent Mental Health Services assessment on Gamble in March 2015 immediately prior to the instant offending concluded that he did not have ASD. ASD is a neuro-developmental disorder that manifests from an early age and is easier to diagnose in young children. The accounts of Mrs Gamble regarding her son's early years were not consistent with ASD: for example, she reported to Dr Davies that Gamble had achieved his developmental milestones and had been reactive and smiling as a baby. It was clear that Gamble had strong political views and could empathise with others: for instance, with victims of drone strikes. In Dr Joseph's view and on the facts, Gamble clearly understood what he was doing and the impact of his actions. He appreciated the upset caused to the victims of the 'hacks', who prided themselves on their security, would feel shame (a sophisticated emotion) upon being hacked. This was all inconsistent with ASD.

Conclusion on the expert evidence

79. I prefer the evidence and opinion of Dr Joseph. I am not satisfied that Kane Gamble suffers or has suffered from ASD - or, if he does so, it is only to a very mild degree. I have reached this conclusion for the following reasons.

80. First, Gamble's traits and apparent social isolation are probably explained by other factors, such as (a) his vomiting phobia, (b) being bullied and racially teased at school, (c) domestic anger at the home and/or (d) his teenage obsession with online activities alone in his bedroom at home.

81. Second, it is clear that Gamble is and was capable of empathising and understanding the emotions and feelings of others, as evidenced by (a) the motivation for his hacking campaign against high ranking US officials which was directly borne out of his empathy for those whom he saw as victims of, *e.g.* racial injustice in US and US-backed Israeli violence in the Middle East; (b) the nature of his hacking campaign, which was deliberately designed to cause as much political, professional and personal embarrassment to high-ranking US officials in the national security or cyber-security worlds; (c) the personal pleasure and satisfaction he took in causing maximum upset to his targets and their families by his intrusions into their professional and domestic lives; and (d) his use of obviously homophobic, racist and discriminatory language which was plainly intended to insult and upset his victims and he knew it would do so. Indeed, as a matter of common sense, had Gamble not intended to inflict harm there would have been little to be gained by his carefully conceived and executed campaign of cyber-harassment for political ends.

82. Third, the methods used by Gamble to gain unauthorised access to, and control of, his targets' e-mail and other accounts required 'social engineering' skills and not merely dry 'computer-hacking' skills. 'Social engineering' requires considerable inter-personal skills such as impersonating people, interacting with call centre or helpdesk staff, manipulating people into doing what he wanted them to do and being articulate, quick witted and mentally agile. He did this on numerous occasions with many different people, adroitly adapting to every new situation. These encounters were not face-to-face but required considerable inter-personal skills. It is striking that Gamble was often concurrently 'chatting' online with CWA associates, updating them as to the progress he was making and the challenges he was encountering.

83. Fourth, Gamble clearly revelled in what he was doing and felt able to brag about his activities to other CWA associates and to journalists, and articulate his motivations and justificatons.

84. Fifth, it is clear that Gamble knew exactly what he was doing and did not have 'limited insight' as Dr Davies suggests. Gamble was fully aware of (a) the sensitivity of the data he was accessing and posting; (b) the scale of what he was doing – "*this is so serious im fucking shaking"… "this has to be the biggest hack ever*"; (c) the risks his actions were posing to lives – "*i thought about not releasing any more info because it put lives at risk but then i thought, they are killing innocent people everyday*"; (d) the consequences of his actions and the impact that they were having on the targeted institutions, officials and their families and friends. The whole point of his campaign was to achieve maximum impact.

Summary

85. For these reasons, I reject the Defence case on the expert evidence and proceed to sentence Gamble on the basis that he does not suffer from ASD or alternatively if he does, it is only to a very mild degree.

Aggravating features

86. There are the following serious aggravating features in this case:

(1) There was a significant degree of sophisticated planning. The methodology used was similar in each. First, targets were carefully chosen and discussed by members of the CWA group. Second, a significant amount of background research on targets was done using open sources. Third, the information gleaned was then used to exploit weaknesses in the security systems. Fourth, once access and control of the targets' account(s) was obtained, this was ruthlessly exploited.

(2) Gamble's conduct was persistent and involved multiple counts and cyber-manipulation on a significant scale. The campaign lasted over eight months. Gamble acted in concert with others. They were, in effect, a cyber-gang engaged in a form of cyber-terrorism.

(3) Gamble and CWA targeted ten different victims (eight individuals and two organisations) and then subjected them and members of their families to intense cyber-manipulation, abuse, threats and harassment and posted significant amounts of personal and sensitive material on the Web. This was an extremely nasty campaign of politically-motivated cyber-terrorism.

(4) Gamble's criminal activities involved a gross intrusion into the personal, family and/or organisational lives of his numerous victims, and were deliberately designed to cause maximum distress and disruption and did so. The victims would have felt seriously violated.

(5) Gamble was reckless and unconcerned as to the harm that might be caused by his posting of the personal details of thousands of personnel; and he continued to release information regardless of the fact that, in his own mind at least, he was putting lives at risk.

(6) Gamble revelled in the distress and disruption he was causing and openly boasted about it.

(7) Significant sums have been expended by the organisations involved in dealing with the problems caused; but, more importantly, they and their systems have suffered significant reputational damage with a resultant loss of confidence in the use of law enforcement portals.

Mitigation

87. I have listened carefully to everything that has been said ably by Mr Harbage QC on behalf the Defence and there are significant factors by way of mitigation:

(1) Gamble's pleas of guilty at the earliest opportunities for which I give maximum 1/3rd credit.

(2) Gamble's lack of previous convictions.

(3) Gamble's age – importantly he was only 15-17 when these offences took place and is now just 18 and a half.

(4) Gamble is a young, vulnerable adult, who has characteristics of naivety and immaturity; and it is common ground between the psychiatrists that he would find it difficult to cope with a sentence of immediate imprisonment.

(5) Delay – there has been a considerable period of delay between Gamble's arrest and sentencing, with this hanging over him. This has been due in part to the need to resolve the psychiatric issues raised by the Defence.

(6) Gamble co-operated in disclosing his passwords when arrested; he has not repeated any offending whilst being on bail; and there is evidence of him giving some IT assistance to one or two companies for which he was rewarded.

(7) Gamble was not motivated by money (although this is balanced by his determined political motivation).

Deterrent sentences

88. In *R v. Martin* (*supra*), the Court of Appeal upheld a sentence of two years imprisonment for four counts of breach of section 1 and five counts of breach of section 3 of the Computer Misuse Act 1990. In 2011 and 2012, when 19 and 20 years old, the appellant in that case had engaged in multiple DOS (Denial of Service) attacks on Oxford and Cambridge University websites, as well as inserting *Trojan* malware onto an individual's computer and seizing his personal and financial information. I quote an important passage from Lord Justice Leveson's judgment at the beginning of these sentencing remarks.

89. In the case of *R v. Mudd* [2017] EWCA Crim 1395, the Court of Appeal upheld a sentence of two years detention for breaches of section 3 of the Computer Misuse Act 1990. In 2011 and 2012, when about 15 years old, the appellant had run a DDoS (Distributed Denial of Service) programme which he had sold on the Web to thousands of users and customers to carry out DDoS attacks. Gross LJ at [35] cited the pertinent words of the sentencing judge, HHJ Topolski, who said this about the need for deterrent sentences:

> "38. The wider implications of such crimes for society cannot be ignored. Offences such as these, have the potential to cause great damage to the community at large and the public, as well as to the individuals more directly affected by them. Further, it is fortuitous and beyond the control of those who perpetrate them, whether they do so or not. This finds reflection in the maximum sentence which may be passed of ten years imprisonment for an offence contrary to section 3(1) of the Act and five years imprisonment for an offence contrary to section 2(1) of the Act. These offences are comparatively easy to commit by those with the relevant expertise, they are increasingly prevalent and the public is entitled to be protected from them. In our view, it is appropriate for sentences for offences such as these to involve a real element of deterrence. Those who commit them must expect to be punished accordingly."

90. It is open to the Court to pass a deterrent sentence in this case (see paragraph 1.10 and 6.2 of the Guidelines cited above).

91. I bear in mind that Gross LJ re-iterated in *R v. Mudd* (*supra*) at [43], there is no 'cliff edge' just because a defendant has reached 18. One has to look at all the aspects of the defendant and the circumstances, which I do.

Deprivation Order

92. I make a Deprivation Order under s.143 of the Powers of Criminal Courts (Sentencing) Act 2000 in respect of the following four items:

1. Emachines laptop (TCJ18LC4)
2. Advent desktop computer (CG18LC9)
3. Samsung tablet (CG18LC6)
4. iPhone (CG18LC4)

Serious Crime Prevention Order

93. The Crown apply for a Serious Crime Prevention Order under section 19 of the Serious Crime Act 2007. However, I am not minded to grant one in this case. First, because Gamble has not offended whilst on bail these past two years. Second, because Gamble's future employment prospects clearly lie in IT once he is released and rehabilitated.

Sentence

Kane Gamble, stand up please.

94. The offences to which you have pleaded guilty are so serious that only an immediate sentence of detention is appropriate. The sentence of detention which I am about to impose upon you is intended to punish you and reflect the overall criminality of your conduct and the harm you have caused to your many victims and confidence in the systems that you interfered with. It is also intended to act as a warning and deterrent to others who might be tempted to engage in the same sort of criminal conduct.

95. In my view, given in particular your good behaviour these past two years whilst on bail and the other mitigating factors, this is not one of those rare cases in which it is appropriate to pass a more severe sentence than the maximum that would have been imposed at the time the offending was committed (*c.f.* paragraph 6.3 of the Guidelines). Nevertheless, a deterrent element is called for. First, because the nature and scale of offending in this case was very serious (as outlined above). Second, because cyber crime of all types is seriously on the rise. Third, because deterrent sentences are called for, even (or perhaps particularly) now to deter younger people from engaging in this sort of criminal enterprise.

96. Given all the circumstances of this case which I have outlined in detail, and given the very considerable seriousness of your offending, had you been an adult of good character without any vulnerabilities and contesting a trial of these matters, I would have passed a total sentence in the order of 6 years imprisonment. However, in the light of your age at the time of your offending, the psychiatric evidence, the pre-sentence report, the delays in the case and the other significant mitigating features of your case, I am able to reduce that figure substantially to a period of 3 years. I also then reduce that figure by a full one third for your early pleas of guilty. That reduces the net total period of sentence to 24 months.

97. So, Kane Gamble, I sentence you to:

    (1) a Detention and Training Order for a period of 24 months in respect of each of the section 3(1) counts (Counts 8 and 10) concurrent to each other; and

    (2) a Detention and Training Order for a period of 12 months in respect of each of the remaining section 1(1) counts (Counts 1, 3, 4, 5, 6, 7, and 9), concurrent to each other and concurrent to Counts 8 and 10.

98. This makes a total sentence of 24 months.

Suspension

99. This is not a sentence which should be suspended, in my view, in light of the time span of your offending, the seriousness of your offending, the high level of your culpability and the harm both caused and intended. There must be a real element of deterrence in the sentence.

100. Accordingly, Kane Gamble I sentence you to a Detention and Training Order in a Young Offenders Institution for a total period of 24 months.

101. I also make the usual Victim Surcharge Order.

Postcript

102. Finally, Kane Gamble let me say this to you and others. The message should go out loud and clear to anyone, young or old, who thinks they can engage in these sorts of criminal cyber activities with impunity: you can expect condign punishment and severe sentences of detention and imprisonment from the Courts. Please go with the officers.

THE HON. MR JUSTICE HADDON-CAVE
20th April 2018