IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT 14/85/CH**

BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT 14/120-126/CH**

BETWEEN:

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Respondents

WITNESS STATEMENT OF ERIC KING

I, ERIC KING,_Deputy Director of Privacy International of 62 Britton Street, London EC1M 5UY, SAY AS FOLLOWS:

1. I am the Deputy Director of Privacy International. I am authorised to make this statement on behalf of Privacy International.

2. I have worked on issues related to communications surveillance at Privacy International since 2011. My areas of interest and expertise are signals

intelligence, surveillance technologies and communications surveillance practices. I regularly speak at academic conferences, with government policy makers, and to international media.

3. The contents of this statement are true to the best of my knowledge, information and belief, and are the product of discussion and consultation with other experts. Where I rely on other sources, I have endeavoured to identify the source.

4. In this statement I will address, in turn, the following matters:

a. **Computer Network Exploitation: Introduction**

b. **The Five Eyes**

c. **What malware can do against an individual device**

   i. *Activating sensors*

   ii. *Obtaining stored data from devices*

   iii. *CNE as a alternative to intercept*

   iv. *Other CNE capabilities*

d. **What malware can do against a server or network**

   i. *CNE to redirect and capture communications*

   ii. *CNE to facilitate deployment of further CNE attacks*

   iii. *CNE for capturing bulk data*

   iv. *Other CNE capabilities*

e. **How malware is deployed**

f. **Additional harmful consequences of CNE**

   i. *Stockpiling of zero days*

   ii. *Affirmatively weakening security protections*

   iii. *Influencing technical standards*

   iv. *"Supply chain enabling, exploitation and intervention"*

   v. *Faking security updates*

   vi. *CNE technical failures*

   vii. *Inability to remove CNE malware*

g. **Targets not of national security interest**

   i. *Targeting companies to enable CNE missions*

   ii. *Targeting suspicionless people with CNE as a means to an end*

Computer Network Exploitation: Introduction

5. Smartphones, laptops and electronic devices have changed how we communicate and interact with others, express ourselves, and record and remember our thoughts and experiences. These devices have become prime targets for GCHQ and the NSA.

6. These intelligence agencies have developed hacking techniques they call "Computer Network Exploitation" (CNE) or "Active Signals Intelligence" (Active SIGINT), which, NSA documents explain, "offers a more aggressive approach to SIGINT. We retrieve data through intervention in our targets' computers or network devices. Extract data from machine."[1] With these capabilities to infect devices with intrusive malware,[2] GCHQ hopes to be able to "exploit any phone, anywhere, any time."[3] A GCHQ document explains: "if it's on the phone, we can get it."[4]

7. With the February 2015 publication of the *Equipment Interference Code of Practice*[5], CNE became an avowed technique in the United Kingdom. However, Five Eyes members have employed the term CNE since at least 1999[6].

8. Having now avowed the use of CNE, the Intelligence and Security Committee has reported that "a significant number" of GCHQ's intelligence reports contain

[1] Intelligent Command and Control (15 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140315-intercept-turbine_intelligence_command_and_control.pdf [Accessed 1 October 2015]

[2] Malware is specialized software that allows whoever deploys it to take control of or extract information from a target device. This is usually accomplished by circumventing any security software or other protections present on the device.

[3] Borger, J. and Hopkins, N. (1 August 2013) Exclusive: NSA pays £100m in secret funding for GCHQ, *The Guardian* [Online]. Available from: http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden [Accessed 1 October 2015]

[4] Capability - iPhone (28 January 2014) [Online]. Available from: http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data#img-3 [Accessed 1 October 2015]

[5] United Kingdom, Home Office (6 February 2015) Equipment Interference Code of Practice. [Online]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401863/Draft_Equipment_Interference_Code_of_Practice.pdf [Accessed 28 September 2015]

[6] iPhone Location Services (9 September 2013) [Online]. Available from: https://www.eff.org/files/2013/11/15/20130909-spiegel-smartphones.pdf [Accessed 28 September 2015]

information derived from the technique.[7] GCHQ and the other UK intelligence agencies may deploy CNE against "computers, servers, routers, laptops, mobile phones and other devices."[8]

9. One NSA presentation published by *Der Spiegel* highlights just how powerful this capability is with reference to George Orwell's *1984*. The author of the NSA document asks, "Who knew in 1984 that this [Apple co-founder Steve Jobs] would be Big Brother…and the zombies would be paying customers?"[9]

10. As I will present in more detail below, CNE gives intelligence agencies access to the most personal and sensitive information about an individual's life – information which can directly or indirectly reveal an individual's location, age, gender, marital status, finances, health details, ethnicity, sexual orientation, education, family relationships, private communications and, potentially, their most intimate thoughts. Furthermore, the logging of keystrokes, tracking of locations, covert photography, and video recording of the user and those around them enables intelligence agencies to conduct real-time surveillance, while access to stored data enables analysis of a user's movements for a lengthy period prior to the search.

11. CNE is thus far more than an alternative to intercept capabilities or a supporting technique for traditional human intelligence (HUMINT). It is the most powerful and intrusive capability GCHQ possesses, and its deployment has revolutionised how GCHQ operates.

The Five Eyes

12. It is well documented that the NSA and GCHQ co-operate very closely, in particular through the Five Eyes alliance, which also includes the intelligence agencies of Canada, Australia and New Zealand. They have co-operated as a

[7] Intelligence and Security Committee, Parliament of the United Kingdom (12 March 2015) *Privacy and Security: A modern and transparent legal framework* (hereafter "ISC Report"), at 67. The ISC Report covers the UK intelligence agencies' "IT Operations" primarily on pages 63-67.

[8] Ibid. at 14n.13.

[9] NSA slides on smartphones (9 September 2013) [Online]. Available from: https://www.eff.org/files/2013/11/15/20130909-spiegel-smartphones.pdf [Accessed 28 September 2015]

signals intelligence alliance for almost 70 years. While the alliance was founded when the agencies only carried out passive SIGINT collection, their co-operation has extended to other capabilities as they have become possible, including CNE.

13. **The Five Eyes share the development of CNE capability.** There are specialised Five Eyes teams, such as the Network Tradecraft Advancement Team[10], that seek to improve CNE capability. Security researchers have identified core malware development libraries of software that have been collectively created and used by the USA, the UK, Canada, Australia and New Zealand. These libraries serve as a foundation to allow each country to develop its own malware from a common basis, as well as shared Five Eyes malware.[11] Canadian Communications Security Establishment (CSE) documents highlight success stories that are a direct result of British GCHQ analysts identifying new ways to target mobile phones during an Australian Defense Signals Directorate (DSD) workshop.[12] Indeed, the malware itself is shared property of the Five Eyes, with documents explaining that codenamed programs such as WARRIORPRIDE, a key malware framework, is a "unified framework… [used] across the 5 eyes [sic]."[13]

14. **The Five Eyes work together to deploy CNE capability.** *The Intercept* has reported that the NSA and GCHQ have targeted anti-virus and other security companies such as Kaspersky Lab.[14] *The Globe and Mail* has also reported that

[10] NSA GCHQ CSEC Network Tradecraft Advancement [Online] (4 December 2014) [Online]. Available from: https://www.eff.org/files/2014/12/16/20141204-intercept-nsa_gchq_csec_network_tradecraft_advancement.pdf [Accessed 28 September 2015]

[11] Guarnieri, C. (27 January 2015) 'Everything we know of NSA and Five Eyes malware' [Online]. Available from: https://nex.sx/blog/2015-01-27-everything-we-know-of-nsa-and-five-eyes-malware.html [Accessed 28 September 2015]

[12] Synergising Network Analysis Tradecraft (21 May 2015) [Online]. Available from: https://www.eff.org/files/2015/06/30/20150521-cbc-synergising_network_analysis_tradecraft.pdf [Accessed 28 September 2015]

[13] CSEC Document on the Handling of Existing Trojans When Trojanizing Computers (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/23/20150117-speigel-csec_document_on_the_handling_of_existing_trojans_when_trojanizing_computers.pdf [Accessed 28 September 2015]

[14] Fishman, A. and Marquis-Bore, M. (22 June 2015) Popular Security Software Came Under Relentless NSA And GCHQ Attacks [Online], *The Intercept*. Available from: https://firstlook.org/theintercept/2015/06/22/nsa-gchq-targeted-kaspersky/ [Accessed 28 September 2015)

the Canadian CSE and the NSA jointly targeted Brazil's Ministry of Mines and Energy.[15] Even intelligence agencies that are not part of the Five Eyes alliance have been brought in for joint CNE operations, with GCHQ receiving redirected communications traffic from the Swedish National Defence Radio Establishment (FRA), allowing them to inject malware into emails.[16]

15. Much of the covert infrastructure to support CNE capability is jointly operated out of Five Eyes bases. NSA documents refer to deploying CNE from RAF "Menwith Hill Station" and "with help from GCHQ".[17] For a period of time, the NSA was seemingly unable to inject malware into users of Google services, with *Der Spiegel* explaining that this "can only be done by Britain's GCHQ intelligence service, which has acquired QUANTUM tools from the NSA."[18]

16. **The Five Eyes share the data that is collected from many CNE operations, regardless of who initiated it.**[19] Documents show that "almost all" of the data from GCHQ CNE operations flows into a Five Eyes joint database, and that "lots" of data from NSA does the same.[20]

17. Throughout this statement, I will refer to many documents that hold security classification markings "TOP SECRET//REL TO: FVEY", indicating that they were shared with all members of the Five Eyes alliance. While some of the references might be to American NSA documents or to Canadian CSE documents, this statement will make use of such documents to illustrate to the

[15] Freeze, C. and Nolen, S. (7 October 2013) Charges that Canada spied on Brazil unveil CSEC's inner workings [Online], *The Globe and Mail. Available from:* http://www.theglobeandmail.com/news/world/brazil-spying-report-spotlights-canadas-electronic-eavesdroppers/article14720003/ [Accessed 28 September 2015)

[16] Xkeyscore Sweden Meeting (12 November 2013) [Online]. Available from: https://www.eff.org/files/2014/01/02/20131211-svt-xkeyscore_sweden_meeting.pdf [Accessed 28 September 2015]

[17] MHS Leverages XKS for QUANTUM (12 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140312-intercept-mhs_leverages_xkeyscore_for_quantum.pdf [Accessed 28 September 2015)

[18] *Spiegel* staff (29 December 2013) Inside TAO: Documents Reveal Top NSA Hacking Unit, *Der Spiegel* [Online]. Available from: http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-2.html [Accessed 28 September 2015]

[19] XKeyscore for Counter-CNE (1 July 2015) [Online]. Available from: https://www.eff.org/files/2015/07/06/20150701-intercept-xks_for_counter_cne.pdf [Accessed 28 September 2015]

[20] Ibid

Tribunal the types of CNE capabilities being used by the Five Eyes. Due to the high level of operational integration among the Five Eyes members, and the fact that these documents share the "TOP SECRET//REL TO: FVEY" classification markings, I will treat them as relevant regardless of which agency authored the documents.

What malware can do against an individual device

18. When CNE is deployed against an individual's mobile phone or computer, there are few limits on what that malware can do. Unlike bugging or intercept, there is no set way CNE may be used. Instead, it is a capability that can be deployed in any number of configurations to do any number of different things. The Five Eyes have a diverse arsenal of malware tools, each highly sophisticated and customisable for different purposes.

Activating sensors

19. Far from being simply passive storage devices, smartphones are portable sensors that monitor the world around them. Vic Gundotra, Google's Vice President of Social on Android, describes a mobile phone as having "eyes, ears, a skin, and …[it] knows your location. Eyes, because you never see one that doesn't have a camera. Ears, because they all have microphones. Skin because a lot of these devices are touch screens. And GPS allows you to know your location."[21]

20. Hacking a mobile phone gives governments (or others) total control of features like the camera, microphone and keyboard, which may be utilised, manipulated and turned against the user of the device. Internal GCHQ documents explain that the agency is interested in "[n]ot just collecting voice and SMS and geo-locating phone, but getting intelligence from all the extra functionality that iPhones and BlackBerrys offer."[22]

[21] Gundotra, V. (10 December 2012) Google+ Post [Online]. Available from: https://plus.google.com/+VicGundotra/posts/f3274job3aN [Accessed 28 September 2015]

[22] Borger, J., Harding, L. and Hopkins, N. (2 August 2013) GCHQ: inside the top-secret world of Britain's biggest spy agency, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden [Accessed 28 September 2015]

21. This ability to activate features is not limited to mobile phones. One malware implant deployed by the NSA – codenamed UNITEDRAKE – can be used with a variety of "plug-ins" that enable the agency using it to gain total control of an infected computer. For example, an implant plug-in named CAPTIVATEDAUDIENCE is used to hijack a computer's microphone and record any conversation or audio taking place near the device. Another, GUMFISH, can secretly activate a computer's webcam and take photographs of whoever is in sight.[23]

22. A similar, possibly identical, suite of tools – codenamed WARRIOR PRIDE – is used by GCHQ. This framework includes a range of capabilities: using DREAMY SMURF, GCHQ are able to turn on a mobile phone that is apparently switched off; NOSEY SMURF allows the agency to activate the device's microphone; and TRACKER SMURF allows the agency to activate the device's GPS location tracker.[24]

23. Modules of another piece of Five Eyes malware, Flame, have been analysed by security researchers, who noted the sophistication of many aspects of the malware. In the Flame malware, a screenshot module takes snapshots of whatever is on the screen every 15 seconds when a communication application, such as instant messaging or Outlook, is being used, but decreases this to once every 60 seconds when other, potentially less interesting applications are being used.[25]

24. To ensure that the presence of malware is not detected, PARANOID SMURF helps the malware to remain hidden on the device.[26]

[23] Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 28 September 2015]

[24] Ball, J. (28 January 2014) Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data [Accessed 28 September 2015]

[25] Zetter, K. (28 May 2012) Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers, *Wired* [Online]. Available from: http://www.wired.com/2012/05/flame/ [Accessed 28 September 2015]

[26] Ball, J. (28 January 2014) Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data [Accessed 28 September 2015]

25. GCHQ is able to record every keystroke pressed on a device using QWERTY, a keylogger plug-in for the WARRIORPRIDE malware framework, designed to collect and exfiltrate all keyboard keys pressed by the victim and record them for later inspection.[27] This enables the agency to see everything that the user has typed, including not just the contents of communications and documents, but also any text that was subsequently deleted, and any passwords that the user entered.

Obtaining stored data from devices

26. For an increasing number of people, personal digital devices contain the most private information they store anywhere. Computers and mobile devices have replaced and consolidated our filing cabinets, photo albums, video archives, personal diaries and journals, address books, and correspondence. They are also slowly replacing our formal identification documents, and our bank and credit cards. They hold information that may never have been set down or communicated elsewhere.

27. Whatever information is stored on our computers and mobile phones becomes immediately obtainable with CNE. From text messages, emails and phone records, to address books, notes and calendars, as one GCHQ document explains, "if it's on the phone, we can get it."[28]

    a. *Communications, social networks and* contacts: Whether it's an email, iMessage, Facebook chat or SMS (text message), almost all communications are now sent using either a computer or mobile phone. With CNE, it does not matter what kind of communication is transmitted if a record of this communication is stored on an electronic device, or access to records can be sought via the device – the malware will be able to obtain it. Address books, friends lists, followers –all are there to be exfiltrated and analysed.

[27] Malware from the Five Eyes (27 January 2015) [Online]. Available from: http://www.spiegel.de/media/media-35668.pdf [Accessed 28 September 2015]

[28] Ball, J. (28 January 2014) Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data [Accessed 28 September 2015]

b. *Documents*: Personal and work documents are stored on the storage drives of devices being targeted by CNE. Accessing cloud file storage services (such as Dropbox, Google Drive or Office 365) via our phones or computers means that deploying malware against these devices may results in the entire electronic document history of the target being obtainable. This is very different from intercept of material that a target has chosen to communicate after a warrant has been issued. The collection of data may go back many years.

c. *Location*: While TRACKER SMURF allows GCHQ to activate the GPS location tracker on a phone to obtain its current location, historical location information can be also be discovered by placing malware on a mobile phone. Many popular smart phones store historical location information.[29]

28. Information that only exists on that device and was never intended to be sent, copied or shared can be obtained via CNE.

CNE as an alternative to intercept

29. Information that could otherwise be obtained by intercept is also available. As phone calls are connected, the malware on the device can copy audio from phone calls and transmit it back to GCHQ in real-time. The same is true for emails being sent from a computer, or indeed any other form of communication that can be transmitted from a computer or mobile device.[30]

30. Video chats using Skype or FaceTime can also be captured using CNE and sent back to GCHQ in real-time.[31]

[29] Ball, J. (28 January 2014) Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data [Accessed 28 September 2015]
[30] JTRIG Tools and Techniques (14 July 2014) [Online]. Available from: https://www.eff.org/files/2014/07/14/jtrigall.pdf [1 October 2015]
[31] Ibid

31. Other malware tools used by GCHQ include FOGGYBOTTOM, which records logs of internet browsing histories, and GROK, which is used to log keystrokes, allowing the agency to collect login details and passwords for websites and email accounts.[32]

Other CNE capabilities

32. Intelligence agencies are interested in obtaining more than just the information from an individual's computer. NSA documents list other goals such as the ability to "manipulate, disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves."[33] This is unsurprising: once access to an electronic device has been secured, it is as easy to delete material or insert new material as it is to exfiltrate it.

33. A diverse range of malware has been created in order to achieve different objectives, for example preventing someone from gaining access to a certain website, or preventing an individual from downloading a file from the internet. Malware can be employed to corrupt a target's file downloads. Remote control of a computer allows intelligence agencies to send fake messages from the infected device, or plant or delete documents or data on that computer remotely.[34] CNE provides a wide range of powerful options.

What malware can do against a server or network

34. Despite this already long list of what intelligence agencies can achieve using malware, these capabilities become more advanced if we consider the deployment of malware against networks of computers.

[32] Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 28 September 2015]

[33] Gellman, B. and Nakashima, E. (30 August 2013) U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html [Accessed 28 September 2015]

[34] Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 28 September 2015]

35. In the words of an NSA analyst, “there are a plethora of things you could do once you get CNE access to a router…suffice it to say, getting access to a router is very good for the actor, and very bad for the victim.”[35]

36. One team at the NSA – Tailored Access Operations (TAO) – has software templates to break into common brands and models of “routers, switches and firewalls from multiple product vendor lines.”[36]

37. Targeted systems and networks are often large-scale and sit at the heart of a company’s or a country’s communications infrastructure. The same NSA analyst quoted above (paragraph 35) explains: “I’m not talking about [hacking] your home ADSL router. I’m talking about bigger routers, such as Ciscos/Junipers/Huaweis used by ISPs [internet service providers] for their infrastructure”.[37]

38. Far from being a capability of last resort for extreme circumstances, it appears this kind of large-scale attack is being deployed regularly against both company and country communications networks. As one document explains “Hacking routers has been good business for us and our 5-eyes [sic] partners for some time.”[38]

[35] Targeting System Administrator Accounts to Access Networks (20 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140320-intercept-targeting_system_administrator_accounts.pdf [Accessed 28 September 2015]

[36] Gellman, B. and Nakashima, E. (30 August 2013) U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html [Accessed 28 September 2015]

[37] Targeting System Administrator Accounts to Access Networks (20 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140320-intercept-targeting_system_administrator_accounts.pdf [Accessed 28 September 2015]

[38] Five Eyes Hacking Large Routers (12 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140312-intercept-five_eyes_hacking_large_routers.pdf [Accessed 28 September 2015]

39. One document reveals that, by deploying CNE against entire mobile phone networks, the NSA are able to automatically exfiltrate phone billing records and the location of everyone connected to that phone network.[39]

40. As early as 2008, a published GCHQ Intelligence Services Act 1994 warrant referenced the fact that the "[c]apability against Cisco routers developed by this means has allowed a CNE presence on the Pakistan Internet Exchange which affords access to almost any user of the internet inside Pakistan."[40]

CNE to redirect and capture communications

41. GCHQ is deploying CNE against core communications infrastructure of other countries in order to obtain access to the communications of any user within the target country. This is done to acquire communications that GCHQ would otherwise have had to seek in partnership with the law enforcement or security forces of that country. GCHQ bypasses such partnerships by routing the hacked communications so they flow past a mass surveillance collection point like TEMPORA where they can be processed and analysed.[41]

42. Under one CNE programme codenamed GENIE, the NSA reveals a similar system in which they "provide high quality voice collection by delivering implants [meaning malware] that can identify select conversations of interest within a target network and exfiltrate select cuts back to NSA."[42] Such techniques in effect steal the processing power of the target's computer to do the agency's work for it.

[39] Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/27/20150117-spiegel-supply-chain_interdiction_-_stealthy_techniques_can_crack_some_of_sigints_hardest_targets.pdf [Accessed 28 September 2015]

[40] Application for Renewal of Warrant GPW/1160 (22 June 2015) [Online]. Available from: https://theintercept.com/document/2015/06/22/gchq-warrant-renewal/ [Accessed 28 September 2015]

[41] Guarnieri, C. (27 January 2015) 'Everything we know of NSA and Five Eyes malware' [Online]. Available from: https://nex.sx/blog/2015-01-27-everything-we-know-of-nsa-and-five-eyes-malware.html [Accessed 28 September 2015]

[42] NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf [Accessed 1 October 2015]

43. Other documents confirm specific codenamed programs used by the NSA and GCHQ to achieve such redirection. For instance, when deploying malware on "network infrastructure devices" one NSA document explains it can use HAMMERMILL for "targeted copying" which permits the redirection of only targeted communications, not everything that is flowing over the network.[43]

44. However "targeted copying" is not the limit of the capability that can be achieved with CNE. A program codenamed BRAVENICKEL allows the capture "an entire [communications] link without selection."[44]

45. GCHQ also engages in bulk redirection, as a 2008 warrant explains: "[o]ur presence on routers likewise allows us to re-route selected traffic across international links towards passive collection systems."[45]

46. Telecommunications companies are often the targets of these redirection attacks. Just within Germany, several communications have been compromised by GCHQ. Deutsche Telekom AG, which provides mobile phone, internet and landline service to 60 million people in Germany, was hacked by GCHQ.[46] Likewise, Netcologne, which operates a fiber-optic network and provides telephone and internet services to 400,000 customers, was targeted by GCHQ, as were German satellite operators Stellar, Cetel, and IABG.[47]

47. Redirection via CNE appears to be part of an international Five Eyes strategy. One NSA document explains the agency will continue to develop its redirection capabilities to "more effectively handle the increasing volumes" of data the agency seeks to acquire, as well as to minimize "unnecessary exposure of the

[43] Analytic Challenges from Active-Passive Integration. (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/23/20150117-speigel-explanation_of_apex_shaping_to_put_exfiltrating_network_traffic_into_patterns_that_allow_plausible_deniability.pdf [Accessed 1 October 2015]

[44] Guarnieri, C. (27 January 2015) 'Everything we know of NSA and Five Eyes malware' [Online]. Available from: https://nex.sx/blog/2015-01-27-everything-we-know-of-nsa-and-five-eyes-malware.html [Accessed 1 October 2015]

[45] GCHQ Application for Renewal of Warrant GPW/1160 (22 June 2015) [Online]. Available from: https://theintercept.com/document/2015/06/22/gchq-warrant-renewal/ [Accessed 1 October 2015]

[46] Grothoff, C. et al (14 September 2014) Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies, *The Intercept* [Online]. Available from: https://firstlook.org/theintercept/2014/09/14/nsa-stellar/ [Accessed 1 October 2015]

[47] Ibid

covert infrastructure.[48] As evidence of how valuable such redirection programs are perceived to be, the NSA has allocated more than $650 million for their use in 2013, with the projected budget passing a $1 billion in 2017.[49] Such redirection also enables GCHQ to acquire large quantities of intercept without intercepting the content of every communications link.

CNE to facilitate deployment of further CNE attacks

48. Redirecting communications is not the only thing that can be done when CNE is deployed against a network. There are other reasons why GCHQ attacks networks. GCHQ's deployment of CNE against Belgium's largest telecommunications provider, Belgacom, provides a useful example.

49. GCHQ documents explain the attack was "successful"[50]" which in part allowed GCHQ to redirect communications as I describe above. But, the attack against Belgacom was also designed to accomplish something else. The ultimate goal of hacking Belgacom appears to have been to "enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM [man-in-the-middle] operations[51] against targets roaming using Smart Phones."[52] In other words, GCHQ wanted to use Belgacom's network to launch further CNE operations against phones that used the network.[53]

[48] NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf [Accessed 1 October 2015]

[49] Guarnieri, C. (27 January 2015) 'Everything we know of NSA and Five Eyes malware' [Online]. Available from: https://nex.sx/blog/2015-01-27-everything-we-know-of-nsa-and-five-eyes-malware.html [Accessed 28 September 2015]

[50] CNE Access to BELGACOM (13 December 2014) [Online]. Available from: https://www.eff.org/files/2015/01/23/20141214-intercept-gchq_nac_review_april_june_2011.pdf [Accessed 2 October 2015]

[51] A "man in the middle" attack deploys malware without the active participation of the target. The attack interrupts, or gets in the middle of, a request by the target device to access internet content. For instance, a target computer might be requesting to connect to a particular website. The agent will intercept that request, and respond to it, often by impersonating the website. In their response, the agent will send back malware instead of, or sometimes in addition to, the requested content.

[52] Operation Socialist (24 October 2013) [Online]. Available from: https://www.eff.org/files/2013/11/15/20130920-spiegel-belgacom.pdf [Accessed 1 October 2015]

[53] Gallagher, R. (13 December 2014) Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco, *The Intercept* [Online]. Available from: https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story/ [Accessed 1 October 2015]

50. Documents show that the Five Eyes have dedicated malware for this task, codenamed STRAITBIZARRE.[54] When deployed, the malware takes control of the target network infrastructure, which can be used to inject malware into other networks, computers or phones.[55]

51. Another GCHQ program, HACIENDA, exists to scan the communications networks of entire countries, looking for vulnerable computers to attack. According to one GCHQ slide from 2009, GCHQ completed scans of 27 different countries and are prepared to do more.[56] One goal of the scanning is to create what the Five Eyes have dubbed Operational Relay Boxes (ORBs). These are not target computers, but third party computers owned by individuals, companies and governments. Because they are easily vulnerable to exploitation from GCHQ, these ORBs are the initial CNE targets, allowing the agency to control them and use them as relays for further CNE attacks. The ORBs then sit between the attacker and the target, obscuring the true origins of an attack.[57]

52. Not getting caught is part of the operation; an NSA document explains, "[s]ystem logs and processes are modified to cloak the intrusion, facilitate future access, and accomplish other operational goals."

CNE for capturing bulk data

53. CNE can also facilitate the acquisition of "bulk data." Indeed, GCHQ told the Independent Reviewer David Anderson QC that they needed to maintain the "ability to acquire bulk data, including through the use of new techniques, such as CNE."[58]

[54] Quantum Shooter SBZ Notes (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-quantumshooter_implant_to_remote-control_computers_from_unknown_third_parties.pdf [Accessed 1 October 2015]
[55] Ibid
[56] What is HACIENDA? (15 August 2014) [Online]. Available from: https://www.eff.org/files/2014/08/18/nsa-gchq-csec-hacienda-heise-14-0816.pdf [Accessed 1 October 2015]
[57] NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf [Accessed 1 October 2015]
[58] Anderson, D. - Independent Reviewer of Terrorism Legislation (June 2015) A Question of Trust: Report of the Investigatory Powers Review [Online]. Available from:

54. A series of attacks by the Five Eyes signals intelligence agencies against companies to obtain the encryption keys used secure mobile phone communications demonstrates what can be done.

55. In one CNE operation against a European company, Gemalto, GCHQ sought to obtain the encryption keys used by SIM cards (a small card containing a computer chip which is used in mobile phones to store identifying information and help encrypt communications). Gemalto makes 2 billion SIM cards a year, which are distributed to mobile phone service providers around the world. A GCHQ presentation states the operation was so successful that GCHQ "believe we have their [Gemalto's] entire network"[59] allowing the agency to begin "harvesting [data] at scale."[60]

56. Other Five Eyes partners are deploying similar attacks to obtain data in bulk, including from other SIM card manufactures. The New York Times reported Australia's signals intelligence agency, DSD, infiltrated an Indonesian mobile phone company and stole nearly 1.8 million encryption keys used to protect communications.[61] The same document also states that GCHQ was preparing similar SIM card theft operations against one of Gemalto's competitors, Germany-based SIM card giants Giesecke and Devrient.[62]

https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf [Accessed 1 October 2015]

[59] Begley, J. and Scahill, J. (19 February 2015) The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle, *The Intercept* [Online]. Available from: https://theintercept.com/2015/02/19/great-sim-heist/ [Accessed 1 October 2015]

[60] Ibid

[61] Poitras, L. and Risen, J. (15 February 2014) Spying by N.S.A. Ally Entangled U.S. Law Firm, *The New York Times* [Online]. Available from: http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=0&mtrref=undefined [Accessed 1 October 2015]

[62] Begley, J. and Scahill, J. (19 February 2015) The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle, *The Intercept* [Online]. Available from: https://theintercept.com/2015/02/19/great-sim-heist/ [Accessed 1 October 2015]

57. Another attack, this time against an unnamed telephone company, allowed Five Eyes agencies to obtain bulk historical phone billing records, which include the time, date and the location of every phone call made on that network.[63]

Other CNE capabilities

58. One note in a leaked copy of an internal NSA/GCHQ message board highlighted just a few capabilities available when CNE is used against network routers:

> *"You could add credentials, allowing yourself to log in any time you choose.*
> *You could add/change routing rules*
> *You could set up a packet capture capability [...]*
> *You could weaken any VPN encryption capabilities on the router, forcing it to create easily decryptable tunnels*
> *You could install a dorked version of the Operating System with whatever functionality you want pre-built in"* [64]

59. By replacing the router's operating system with a "dorked" or altered version, there would be no need to deploy malware again to obtain additional access, as the very operating system of the router would be under your control until it was updated or the malware discovered.

60. While controlling or extracting information from computers and networks is intrusive, intelligence agencies can also do more. To block access to certain websites, they can deploy QUANTUMSKY.[65] To prevent someone from downloading a certain file from the internet, then they can use QUANTUMCOPPER to corrupt a target's file downloads. [66]

[63] Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/27/20150117-spiegel-supply-chain_interdiction_-_stealthy_techniques_can_crack_some_of_sigints_hardest_targets.pdf [Accessed 28 September 2015]

[64] Five Eyes Hacking Large Routers (12 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140312-intercept-five_eyes_hacking_large_routers.pdf [Accessed 28 September 2015]

[65] Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 28 September 2015]

[66] Ibid

How malware is deployed

61. CNE is most often carried out by remotely accessing the target device. One NSA document explains that "to maximise agility and minimize risk and cost, a targeted system is usually subverted remotely, via existing tools/implants and infrastructure. When remote access is not possible, field operations are undertaken to physically place hardware implants or software modifications into or near targeted systems."[67]

62. Historically, one of the primary ways GCHQ would send out malware was in bulk, as spam email. It appears that GCHQ was responsible for at least some of the spam email that we all receive. This "bulk spam mission" however was reportedly slowly becoming less viable, resulting in the success rate of infecting a computer becoming less than 1%.[68]

63. Currently, GCHQ appears to prefer a transmission system developed by the NSA codenamed QUANTUM. Indeed, one NSA document reveals "GCHQ uses technique [sic] for 80% of CNE access."[69] QUANTUM isn't a new technique; some of its strains, like QUANTUMINSERT, were first created by the NSA in 2005, or QUANTUMSKY in 2004.[70]

64. QUANTUM consists of a variety of methods that allow intelligence agents to take control of target devices. One QUANTUM variation works by "shooting" malware directly into internet traffic that flows through TEMPORA or similar mass surveillance systems. As TEMPORA or similar systems collect and process communications in bulk, the keyword searching conducted under that program can be repurposed for the deployment of CNE too. Based on keywords

[67] NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf [Accessed 1 October 2015]

[68] NSA Phishing Tactics and Man in the Middle Attacks (12 March 2014) [Online]. Available from: https://www.eff.org/files/2014/03/12/20140312-intercept-nsa_phishing_tactics_and_man_in_the_middle_attacks.pdf [Accessed 1 October 2015]

[69] Multiple Methods of Quantum (12 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140312-intercept-multiple_methods_of_quantum.pdf [Accessed 1 October 2015]

[70] Ibid

within emails collected, QUANTUMTHEORY can be activated, injecting, or "shooting", malware into the communication in real time in an attempt to exploit the recipient of the email.[71]

65. One base in North Yorkshire, RAF Menwith Hill, has been critical in the deployment of QUANTUM attacks. A document shared with the Five Eyes alliance refers to RAF Menwith Hill as being an early tester of QUANTUM when targeting in particular, Yahoo and Hotmail email accounts. Indeed, for a period of time the NSA was unable to deploy QUANTUM to target users of Google services from any other location than the UK. [72]

66. Another deployment of QUANTUM, codenamed QUANTUMHAND, works by waiting until the target attempts to log into Facebook, at which point GCHQ intercepts the request to log in. Then GCHQ, not Facebook, responds to the request by sending back concealed malware which tricks the victim's computer into thinking the communication is being sent from the genuine Facebook.[73]

67. Another option for interfering with a target device is supply chain exploitation, which is discussed in further detail in the paragraphs 92 to 101 of this statement.

68. Five Eyes agencies have also deployed malware to visitors of online forums. [74] One attack, carried out by the Equation Group which has been linked to the Five Eyes, sent malware to everyone who logged-into a series of web discussion forums. The security company Kaspersky published a detailed description of the operation.[75] They explained that the malware was sometimes deployed via advertisements on popular web forums used in the Middle East. Everyone who

[71] MHS Leverages XKS for QUANTUM (12 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140312-intercept-mhs_leverages_xkeyscore_for_quantum.pdf [Accessed 28 September 2015)

[72] QUANTUMTHEORY Hacking Tactics (12 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140312-intercept-the_nsa_and_gchqs_quantumtheory_hacking_tactics.pdf [Accessed 1 October 2015]

[73] Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 1 October 2015]

[74] Kaspersky Lab (February 2015) Equation Group: Questions and Answers [Online]. Available from: https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf [Accessed 1 October 2015]

[75] Ibid

visited the compromised forum could be infected, although the operation was partially geographically limited. Visitors to the forum from certain countries, including Jordan, Turkey and Egypt, would not be targeted. Once deployed, the malware infects the computer and installs a validator, named DOUBLEFANTASY, which monitors the computer for a period, reporting back to the person controlling it for further instructions. Those instructions may be either to obtain whatever information is desired from the computer, or if the device is not of interest, the operation may be terminated.[76]

69. Another method of deploying malware is known as a "watering hole" attack. Such attacks are usually accomplished by installing custom code on a website that will infect with malware any device that visits that website. For example, the US Federal Bureau of Investigation (FBI) has admitted to deploying such an attack on the servers of the service Freedom Hosting. Each server was turned into a watering hole, and subsequently infected with malware any device that visited the server whether or not that device was of interest to the FBI.[77]

Additional harmful consequences of CNE

70. CNE by its nature exploits weaknesses in software and hardware that is often used by millions of people. One US intelligence official analogised using CNE to a situation in which "[y]ou pry open the window somewhere and leave it so when you come back the owner doesn't know it's unlocked, but you can get back in when you want to."[78]

71. An internal document reveals GCHQ's desire for the ability to "exploit any phone, anywhere, any time."[79] This goal creates perverse incentives, which may

[76] Ibid

[77] Poulsen, K. (13 September 2013) FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, *Wired* [Online]. Available from: http://www.wired.com/2013/09/freedom-hosting-fbi/ [Accessed 1 October 2015)

[78] Gellman, B. and Nakashima, E. (30 August 2013) U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html [Accessed 28 September 2015]

[79] Borger, J. and Hopkins, N. (1 August 2013) Exclusive: NSA pays £100m in secret funding for GCHQ, *The Guardian* [Online]. Available from: http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden [Accessed 1 October 2015]

lead to sacrificing the security of the communications that we all rely on for banking, commerce and other everyday transactions in the name of access for intelligence agencies.

72. As I will describe below, GCHQ and NSA are stockpiling software vulnerabilities, known as zero days. They are also overtly and covertly weakening the security of some hardware and software at its source, influencing security decisions made at technical standards bodies to suit their goals, and undermining trust in critical systems that people around the world rely on for security.

Stockpiling of zero days

73. GCHQ and the Five Eyes use a variety of methods to exploit hardware and software. Many of those methods rely on the use of a vulnerability – a pre-existing error, often called a "bug", in hardware or software that allows it to be used in a manner that was not intended or anticipated.

74. In the normal course, when researchers and others discover vulnerabilities, they report the vulnerability to the company responsible for the security of the equipment affected. If GCHQ or the Five Eyes discover a vulnerability, however, they have an incentive not to reveal it in order to use it offensively as part of a CNE attack, or to stockpile it for future use. An NSA classification guide states that "technical details concerning specific software vulnerabilities, when not publically known, and [that] are exploited for CNE activities" hold a minimum classification of TOP SECRET.[80]

75. Zero day vulnerabilities get their name from the fact that, when identified, the computer user has had "zero days" to fix them before attackers can exploit the vulnerability.

[80] NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf [Accessed 1 October 2015]

76. US intelligence officials have acknowledged that governments have become some of the biggest developers and purchasers of information identifying zero days.[81] One NSA budget shows the agency in 2013 set aside $25.1 million for investment in "resources to maintain and expand the Nation's CNE capability by additional covert purchases of software vulnerabilities in support of CNE."[82]

77. Almost all technology companies have schemes to purchase zero days affecting their systems, with many offering large sums to security researchers who find the vulnerabilities and bring them to the company to fix. While most companies are providing thousands, or even tens of thousands of dollars for particularly important vulnerabilities, the largest publicly acknowledged payment ever made was $100,000 for a whole class of vulnerabilities affecting Microsoft's operation system Windows.[83]

78. Payments offered by governments for vulnerabilities dwarf those given by the companies in both size and scale. The price of zero days is therefore rising, with one security firm that regularly sells zero days to governments now offering $1 million for a vulnerability that would allow an attacker to break into an iPhone or iPad running Apple's newly released iOS 9.[84]

79. By purchasing zero days, and using them offensively as part of attacks, GCHQ and the NSA are preventing preventing potentially millions of individuals and companies from being protected.

80. This perverse situation has drawn criticism in the US, from the President's own Review Group on Intelligence and Communications Technologies. When

[81] Sanger, D. (12 April 2014) Obama Lets NSA Exploit Some Internet Flaws, Officials Say, *The New York Times* [Online]. Available from: http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html?_r=1 [Accessed 1 October 2015]
[82] NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf [Accessed 1 October 2015]
[83] Bort, J. (9 October 2013) Microsoft Paid This Man $100,000 For Finding A Big Security Flaw In Windows 8.1, *Business Insider* [Online]. Available from: http://www.businessinsider.com/microsoft-pays-100k-for-windows-8-flaw-2013-10?IR=T [Accessed 1 October 2015]
84 Greenberg, A. (21 September 2015) Spy Agency Contractor Puts Out a $1M Bounty for an iPhone Hack, *Wired* [Online]. Available from: http://www.wired.com/2015/09/spy-agency-contractor-puts-1m-bounty-iphone-hack/ [Accessed 1 October 2015]

considering the zero day problem, they recommended that "[i]n almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities — 'patching' them — strengthens the security of US Government, critical infrastructure, and other computer systems."[85]

Affirmatively weakening security protections

81. Not satisfied with being able to outspend any competition in the market for vulnerabilities, GCHQ and the NSA have also undertaken to shape the technology marketplace and weaken the development of security technology to suit the agencies' goals.

82. The NSA's SIGINT strategy sets out its goals for 2012, which include "[i]nfluenc[ing] the global commercial encryption market through commercial relationships, HUMINT, and second and third party partners."[86] Another briefing document sets out how the NSA wants to "[s]hape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities."[87]

83. These overt and covert efforts to weaken, and make "exploitable", commonly used technologies undermine computer security for all. Strong encryption is essential for information assurance, data protection, and cyber security, as well as being a critical underpinning for online commerce and international banking.

84. Despite this, a 2010 GCHQ document states, "[f]or the past decade, NSA has lead [sic] an aggressive, multi-pronged effort to break widely used internet

[85] President's Review Group on Intelligence and Communications Technologies (12 December 2013) Liberty And Security in a Changing World [Online]. Available from: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [Accessed 1 October 2015]

[86] SIGINT Strategy (22 November 2013) [Online]. Available from: https://www.eff.org/files/2013/11/25/20131123-nyt-sigint_strategy_feb_2012.pdf [Accessed 1 October 2015]

[87] The New York Times (5 September 2015) Secret Documents Reveal N.S.A. Campaign Against Encryption [Online]. Available from: http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html [Accessed 1 October 2015]

encryption technologies."[88] The program "actively engages US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs" including "inserting vulnerabilities into commercial encryption systems."[89]

85. Another briefing document explains that in 2013, the NSA will “[c]omplete enabling for [redacted] encryption chips used in Virtual Private Networks and Web encryption devices” [90] meaning that either by working with the manufacturers of the chips to insert back doors or by exploiting a security flaw in the chips' design, the NSA will be able to break the encryption.[91]

86. Virtual Private Networks (VPNs) are important tools that allow individuals and organisations to keep data secure as it is transmitted over the internet. Many businesses use dedicated hardware to encrypt traffic before it is sent using a VPN. Indeed, the guidance provided by the UK Cabinet Office recommends that businesses ensure “device and information exchanges are protected by an appropriately configured VPN.”[92] By undermining VPNs, the NSA not only makes them vulnerable to exploitation for intelligence agencies, but also by other actors who might discover the weaknesses and exploit them.

87. Certain companies appear to be working with the NSA/GCHQ to ensure their products are “exploitable.” Little is known about which companies are likely to be involved, but one document from the NSA explains that “documents that contain information that implies that commercial companies cooperate with NSA or Second Party partners to render their products exploitable” are to be classified TOP SECRET. Indeed the document goes on to say “exposure of any

[88] Ball, J., Borger, J. and Greenwald, G. (6 September 2013) Revealed: how US and UK spy agencies defeat internet privacy and security, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [Accessed 1 October 2015]

[89] Ibid

[90] The New York Times (5 September 2015) Secret Documents Reveal N.S.A. Campaign Against Encryption [Online]. Available from: http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html [Accessed 1 October 2015]

[91] Ibid

[92] United Kingdom Cabinet Office, Department of Business Innovation and Skills (16 January 2015) 10 Steps: Home and Mobile Working [Online]. Available from: https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-home-and-mobile-working--11 [Accessed 1 October 2015]

company’s commercial cryptanalytic relationship with [NSA] even for a company no longer in existence, will damage [NSA’s] credibility with current companies who are approached for assistance.”[93]

88. GCHQ has also contributed to the effort to weaken encryption by establishing a HUMINT Operations Team (HOT). HUMINT, short for "human intelligence", refers to information gleaned directly from human sources or undercover agents. This GCHQ team was, according to an internal document, "responsible for identifying, recruiting and running covert agents in the global telecommunications industry."[94]

Influencing technical standards

89. Technical standards are essential for the compatibility and interoperability of technologies as they are developed, produced and used globally.

90. The NSA has internally stated a goal to “influence policies, standards and specifications for commercial public key technologies.”[95] This is not necessarily sinister in and of itself, as it would be expected that the leading US cryptologic agency would be involved in cryptography standards. However, what is concerning is the fact this statement is made within the context of a document setting out the NSA’s signals intelligence (SIGINT) enabling goals, aimed at allowing the NSA to ensure commercial systems are “exploitable through SIGINT collection.”[96]

91. The NSA has implemented this strategy in at least one instance involving the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC-DRBG) algorithm, which is used to generate random numbers. Random number

[93] Classification Guide for SIGINT Material, 1945-1967 (18 June 2014) [Online]. Available from: https://www.eff.org/files/2014/06/23/guidelines_for_the_classification_of_nsa_sigint_details_1945-1967.pdf [Accessed 1 October 2015]

[94] Ball, J., Borger, J. and Greenwald, G. (6 September 2013) Revealed: how US and UK spy agencies defeat internet privacy and security, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [Accessed 1 October 2015]

[95] Computer Network Operations - SIGINT Enabling (5 September 2013) [Online]. Available from: https://www.eff.org/files/2014/04/09/20130905-guard-sigint_enabling.pdf [Accessed 1 October 2015]

[96] Ibid

generation is used throughout security systems to create secure keys and for authentication. If the numbers generated are not random but can be predicted, the encryption system itself will be compromised. Dual_EC-DRBG was a standard promulgated by a number of US and international standards bodies. In 2013, however, the New York Times reported that documents in their possession "appear to confirm" that the NSA had inserted a “backdoor” into Dual_EC-DRBG to allow the NSA to decrypt material that used the algorithm.[97] The US body responsible for the standard subsequently withdrew it and recommended “current users of Dual_EC-DRBG transition to one of the three remaining approved algorithms as quickly as possible."[98]

“Supply chain enabling, exploitation and intervention”

92. In some circumstances, documents show the NSA has undertaken what it calls “supply chain enabling, exploitation, or intervention operations” including “[h]ardware implant enabling, exploitation or operations.”[99]

93. One NSA staffer explains the hardware implant enabling process in full: “Here’s how it works: shipments of computer network devices (servers, routers, etc,) being delivered to our targets throughout the world are intercepted. Next, they are redirected to a secret location where Tailored Access Operations/Access Operations (AO-S326) employees, with the support of the Remote Operations Center (S321), enable the installation of beacon implants directly into our targets’ electronic devices. These devices are then re-packaged and placed back into transit to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.”[100]

[97] The New York Times (5 September 2015) Secret Documents Reveal N.S.A. Campaign Against Encryption [Online]. Available from: http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html [Accessed 1 October 2015]

[98] United States Department of Commerce, National Institute of Standards and Technology (21 April 2014) NIST Removes Cryptography Algorithm from Random Number Generator Recommendations, *NIST Tech Beat* [Online]. Available from: http://www.nist.gov/itl/csd/sp800-90-042114.cfm

[99] Computer Network Exploitation Classification Guide / 2-59 [Online]. Available from: http://www.spiegel.de/media/media-35656.pdf [Accessed 2 October 2015]

[100] Gallagher, S. (14 May 2014) Photos of an NSA “upgrade” factory show Cisco router getting implant, *Ars Technica* [Online]. Available from: http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/ [Accessed 1 October 2015]

94. Interfering with the network hardware supply chain in this way allows the NSA to place controlled backdoors in the "internet backbone"[101] and gain access to communications networks, providing potential access to a whole country's core communication infrastructure used by millions of people.[102] Details of what can could achieved is set out in the earlier 'what malware can do against a server, or network' section of this statement.

95. The document that revealed the NSA's supply chain operations was accompanied by a photograph showing NSA staff unsealing, opening, altering, repackaging, and resealing routing equipment belonging to the US company Cisco.[103] In response to this photograph, Cisco wrote to President Obama explaining that "we simply cannot operate this way, our customers trust us to be able to deliver to their doorsteps products that meet the highest standards of integrity and security."[104] Cisco also began shipping equipment to fake addresses in an effort to avoid NSA interdiction.[105]

96. Orders for Cisco products fell 18% in the months after the revelation[106] and some estimates suggest US technology companies may lose as much as $35 billion in revenue as a result of recent revelations regarding intelligence agency activities.[107]

97. Documents obtained by Edward Snowden reveal another form of supply chain exploitation, this time targeted at the development of applications ("apps") for

[101] Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/27/20150117-spiegel-supply-chain_interdiction_-_stealthy_techniques_can_crack_some_of_sigints_hardest_targets.pdf [Accessed 28 September 2015]
[102] Ibid
[103] Ibid
[104] Chambers, J.T (15 May 2014) Letter to President Obama [Online]. Available from: http://www.docstoc.com/docs/170154030/Cisco-Chambers-to-POTUS-2014_05_15pdf [Accessed 1 October 2015]
[105] Pauli, D. (18 March 2015) Cisco posts kit to empty houses to dodge NSA chop shops, *The Register* [Online]. Available from: http://www.theregister.co.uk/2015/03/18/want_to_dodge_nsa_supply_chain_taps_ask_cisco_for_a_dead_drop/ [Accessed 1 October 2015]
[106] Gaouette, N. (26 November 2013) NSA Spying Risks $35 Billion in U.S. Technology Sales, *Bloomberg Business* [Online]. Available from: http://www.bloomberg.com/news/articles/2013-11-26/nsa-spying-risks-35-billion-in-u-s-technology-sales [Accessed 1 October 2015]
[107] Whittaker, Z. (9 June 2015) US tech giants to "far exceed" $35 billion loss in NSA fallout, *ZDNet* [Online]. Available from: http://www.zdnet.com/article/us-tech-companies-to-far-exceed-35-billion-loss-in-nsa-fallout/ [Accessed 1 October 2015]

Apple's iPhone. Researchers at the CIA created a modified version of Apple's software development tool, Xcode, which is used to make apps for the iPhone. The documents explain how if the modified version of Xcode could be surreptitiously distributed to certain developers, then any subsequent apps created by those developers would be built with backdoors already within them.[108] Depending on which developers used the modified Xcode, and how many used their apps, millions of people could be affected. The documents do not say whether the operation was deployed.

98. In China, security researchers recently discovered a modified version of Apple's Xcode software, dubbed XcodeGhost, had been distributed in exactly this way and used by a number of prominent Chinese developers.

99. While it is not known who is responsible for releasing the modified version of Xcode, and there is some scepticism as to whether US authorities carried out the attack due to sloppy code being used in the malware, the damage caused by XcodeGhost is significant. More than 4000 apps were created with the modified XCode.[109] Apps created with XcodeGhost were reportedly able to obtain usernames and passwords, infect other apps, redirect visits to websites, and steal iCloud passwords and upload them to the attacker's servers without the victim's knowledge.[110]

100. The infected apps include those used for instant messaging, banking, maps, stock trading, and games. Among the more well-known apps are the instant messager app WeChat; Didi Chuxing - the most popular taxi app in China; and

[108] Lee, M. (22 September 2015) Apple's App Store got infected with the same type of malware the CIA developed, *The Intercept* [Online]. Available from: https://theintercept.com/2015/09/22/apples-app-store-infected-type-malware-cia-developed/ [Accessed 1 October 2015]

[109] Pauli, D. (25 September 2015) XcodeGhost-infected apps open gates to malware hijacking, *The Register* [Online]. Available from: http://www.theregister.co.uk/2015/09/25/xcodeghost_mitm_palo_alto/ [Accessed 1 October 2015]

[110] Khandelwal, S. (23 September 2015) Apple's Biggest Hack Ever: 4000 Malicious iOS Store Apps Linked to CIA?, *The Hacker News* [Online]. Available from: http://thehackernews.com/2015/09/ios-malware-cyber-attack.html [Accessed 1 October 2015]

Railway 12306 - the only official app used for purchasing train tickets in China.[111] Millions of people will have been affected.

101. Apple have removed the infected apps from the App Store and published instructions for developers to help them identify if they have been infected.[112] Some have described the operation as Apple's biggest ever hack.[113]

Faking software updates

102. Updating the software on your mobile phone or computer with the latest security patches is an essential practice for individuals and businesses seeking protect themselves against cyber attacks. While these security updates are pushed to computers automatically, they often require action on behalf of the user to be installed, which many users fail to do. Governments around the world are encouraging the download and installation of software updates as a critical cyber security measure. One UK Home Office cyber security education campaign explains, "Software updates contain vital security upgrades which help protect your device from viruses and hackers [..,] While it's easy to hit 'cancel' and go back to what you're doing, the few minutes it takes to download and install the software updates could save you an enormous amount of time and trouble in the long run."[114]

103. The Five Eyes are exploiting the trust users place in these updates by deploying fake software updates that install malware.

104. The most prominent example of this practice comes from a high profile malware attack, called Flame, reported by the Washington Post to have been

[111] Xiao, C. (18 September 2015) Malware XcodeGhost Infects 39 iOS Apps, Including WeChat, Affecting Hundreds of Millions of Users [Online]. Available from: http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/ [Accessed 1 October 2015]

[112] Apple (22 September 2015) Validating Your Version of Xcode [Online]. Available from: https://developer.apple.com/news/?id=09222015a [Accessed 1 October 2015]

[113] Khandelwal, S. (23 September 2015) Apple's Biggest Hack Ever: 4000 Malicious iOS Store Apps Linked to CIA?, *The Hacker News* [Online]. Available from: http://thehackernews.com/2015/09/ios-malware-cyber-attack.html [Accessed 1 October 2015]

[114] HM Government, Installing software updates [Online]. Available from: https://www.cyberstreetwise.com/software-updates [Accessed 1 October 2015]

jointly developed by the Five Eyes,[115] a fact confirmed by subsequent Snowden documents.[116] Over the course of six years, security researchers estimate Flame targeted more than 1,000 computers around the world, mostly in the Middle East.[117]

105. Flame was designed to spread from one infected computer to other machines on the same network. When uninfected computers update themselves, Flame intercepts the request to the Microsoft Update server and instead delivers malware to the machine that is signed with a fake Microsoft certificate.[118]

106. At the time Flame was deployed, about 900 million Windows computers trusted and relied on security updates from Microsoft Update.[119] Once Flame was discovered, the Microsoft certification process was rebuilt, the delivery mechanism for Windows updates was re-architected and a patch was sent out via Microsoft Update in an emergency security package, ten days earlier than the next planned update. Security companies described the loss of trust and confidence in the software update process as "the nightmare scenario."[120]

107. In a recently leaked policy document, the White House admitted and agreed that exploiting companies automatic software update procedures could "call into question the trustworthiness of established software update channels" and might

[115] Miller, G. et al (19 June 2012) U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html [Accessed 1 October 2015]

[116] Visit Precis: Lobban (30 April 2014) [Online]. Available from: https://www.eff.org/files/2014/04/30/20140430-intercept-gchq_visit.pdf [Accessed 1 October 2015]

[117] Zetter, K. (2 October 2015) Did the NSA and the UK's Spy Agency Launch a Joint Cyberattack on Iran?, *Wired* [Online]. Available from: http://www.wired.com/2015/02/uks-spy-agency-partner-nsa-cyberattacks-iran/ [Accessed 1 October 2015]

[118] Zetter, K. (6 April 2014) Flame Hijacks Microsoft Update to Spread Malware Disguised As Legit Code, *Wired* [Online]. Available from: http://www.wired.com/2012/06/flame-microsoft-certificate/ [Accessed 1 October 2015]

[119] Microsoft Update and The Nightmare Scenario (4 June 2012) F-Secure Blog [Online]. Available from: https://www.f-secure.com/weblog/archives/00002377.html [Accessed 1 October 2015]

[120] Keizer, G. (7 June 2012) Microsoft's reaction to Flame shows seriousness of 'Holy Grail' hack, *Computer World* [Online]. Available from: http://www.computerworld.com/article/2504108/cybercrime-hacking/microsoft-s-reaction-to-flame-shows-seriousness-of--holy-grail--hack.html [Accessed 1 October 2015]

lead some users to opt out of updates, "rendering their devices significantly less secure as time passed and vulnerabilities were discovered but not patched."[121]

CNE technical failures

108. Unlike more traditional SIGINT collection techniques that acquire communications passively, the active intervention of CNE is fraught with difficulties.

109. Occasionally, unintended consequences occur when targeting large scale, core communications infrastructure with CNE. In 2012, it was reported that 92% of the communications networks providing internet connectivity for Syria suddenly were knocked offline.[122] At the time, this disruption was widely assumed to have been caused by the Syrian government in order to destabilise opposition groups, and was criticised by world leaders.

110. According to Edward Snowden, the NSA, not the Syrian government, caused the disruption. The NSA had been attempting to use CNE to conduct surveillance on the Syrian network when something went wrong with the operation "and the [targeted] router was bricked instead—rendered totally inoperable. […] The failure of this router caused Syria to suddenly lose all connection to the internet – although the public didn't know that the US government was responsible."[123]

111. Other documents show that the Syria incident is not a one off occurrence. One NSA document refers to a time when all its malware deployments against a

[121] Obama administration draft paper on technical options for the encryption debate (September 2013) [Online]. Available from: http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/ [Accessed 1 October 2015]

[122] Shachtman, N. (29 November 2012) Syria Has Just Been Taken Offline, *Wired* [Online]. Available from: http://www.wired.com/2012/11/syria-offline/ [Accessed 1 October 2015]

[123] Ackerman, S. (13 August 2014) Snowden: NSA accidentally caused Syria's internet blackout in 2012, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war [Accessed 1 October 2015]

certain type of Cisco router began "experiencing a software bug that causes [the routers] to intermittently drop out."[124]

112. On other occasions, poor procedures inside Five Eyes agencies mean that structures set up to deploy CNE capability for missions are not properly decommissioned, leaving loose ends causing damage far beyond the time period of the operation.

113. For instance, security researchers were only able to discover the Five Eyes Equation Group malware, described above in paragraph 68, because of mistakes made by the agencies. The NSA's registration of some of the web domains used by servers in the NSA command and control structure of the Equation Group malware expired, yet the servers were still operating on auto-pilot allowing researchers to register 20 out of the 300 web domains that appeared to be in use, and acquire information about the victims of the malware attack via those domains.[125]

114. Further, some NSA CNE attacks, such as Stuxnet, whose target was Iranian nuclear facilities, have inadvertently spread. Stuxnet eventually appeared on the company Chevron's computer network. The CIO of Chevron put it plainly: "We're finding it in our systems and so are other companies [. . .] [s]o now we have to deal with this." [126]

Inability to remove CNE malware

115. It also appears to be hard to remove malware from computer systems once it has been deployed. For example, when researchers took over the web domains related to the Five Eyes Equation Group malware, as described above in

[124] NSA Report: Update Software on all Cisco ONS Nodes [Online]. Available from: https://search.edwardsnowden.com/docs/UpdatesoftwareonallCiscoONSnodes [Accessed 2 October 2015]

[125] Goodin, D. (16 February 2015) How "omnipotent" hackers tied to NSA hid for 14 years—and were found at last, *Ars Technica* [Online]. Available from: http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/ [Accessed 1 October 2015]

[126] King, R. (9 November 2012) Virus Aimed at Iran Infected Chevron Network, *The Wall Street Journal*. Available from: http://www.wsj.com/articles/SB10001424127887324894104578107223667421796 [Accessed 1 October 2015]

paragraph 68, they found that despite the fact that the CNE attack occurred over 12 years ago, victim computers around the world were still infected with the malware, with dozens of them continuing to report in from Russia, Iran, China, and India.[127]

116. This problem is likely to get worse as the complexity of the malware being deployed by Five Eyes agencies increases. It is already a stated goal of the NSA to be able to "[d]evelop and deliver capabilities that will allow endpoint implants to persist in target computers/servers through technology upgrades," with an emphasis "on developing persistent solutions that incorporate stealth techniques."[128]

Targets not of national security interest

117. With the convergence of communications technologies, the devices, networks, and platforms that are used by the suspicionless public are the same ones that suffer as GCHQ undertakes CNE attacks, not against national security targets, but against law abiding companies, their staff, researchers, and system administrators, who have only one thing in common with each other – they are a "means to an end."[129]

Targeting companies to enable CNE missions

118. This statement has already described a number of operations undertaken by the Five Eyes agencies against companies that are not engaging in any wrongdoing and are not considered a national security threat. Whether it is the targeting of European telecommunications companies like Deutsche Telekom AG,[130]

[127] Goodin, D. (16 February 2015) How "omnipotent" hackers tied to NSA hid for 14 years—and were found at last, *Ars Technica* [Online]. Available from: http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/ [Accessed 1 October 2015]

[128] NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf [Accessed 1 October 2015]

[129] Targeting System Administrator Accounts to Access Networks (20 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140320-intercept-targeting_system_administrator_accounts.pdf [Accessed 28 September 2015]

[130] Grothoff, C. et al (14 September 2014) Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies, *The Intercept* [Online]. Available from: https://firstlook.org/theintercept/2014/09/14/nsa-stellar/ [Accessed 1 October 2015]

Netcologne,[131] and Belgacom[132]; Satellite operators like Stellar, Cetel, and IABG,[133] or companies that facilitate encryption for mobile phones like Gemalto,[134] Giesecke and Devrient,[135] there now appears to be a class of companies, often with thousands of employees, and potentially millions of customers, whose involvement in technology means that the Five Eyes intelligence agencies consider them fair game for targeting.

119. When discussing the rationale for targeting one telecommunications company, NSA documents explain that many of its targets communicate using the company's products; "[w]e want to make sure that we know how to exploit these products [. . .] [to] gain access to networks of interest."[136]

120. GCHQ and the NSA have also monitored researchers at anti-virus companies. One NSA slideshow references a program codenamed CAMBERDADA under which malware apparently was sent to various anti-virus companies. The slideshow also lists 23 anti-virus companies from all over the world, stating just two words - "More Targets!"[137]

Targeting suspicionless people with CNE as a means to an end

121. In addition to companies, GCHQ apparently targets entirely suspicionless people, who are not a national security threat, nor are suspected of having committed any crime.

[131] Ibid

[132] Gallagher, R. (13 December 2014) Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco, *The Intercept* [Online]. Available from: https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story/ [Accessed 1 October 2015]

[133] Grothoff, C. et al (14 September 2014) Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies, *The Intercept* [Online]. Available from: https://firstlook.org/theintercept/2014/09/14/nsa-stellar/ [Accessed 1 October 2015]

[134] Begley, J. and Scahill, J. (19 February 2015) The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle, *The Intercept* [Online]. Available from: https://theintercept.com/2015/02/19/great-sim-heist/ [Accessed 1 October 2015]

[135] Ibid

[136] Perlroth, N. and Sangder, D.E. (22 March 2014) N.S.A. Breached Chinese Servers Seen as Security Threat, *The New York Times* [Online]. Available from: http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=1 [Accessed 2 October 2015]

[137] Fishman, A. and Marquis-Bore, M. (22 June 2015) Popular Security Software Came Under Relentless NSA And GCHQ Attacks [Online], *The Intercept*. Available from: https://firstlook.org/theintercept/2015/06/22/nsa-gchq-targeted-kaspersky/ [Accessed 28 September 2015]

122. In one post to an NSA internal message board, an NSA staffer described deploying CNE against systems administrators (individuals who run and maintain internal computer networks). By hacking a system administrator's computer, the agency can gain covert access to communications that are processed by his or her company whether that is a telecommunications company, an internet service provider or any other company. In noting why system administrators are targeted, the staffer explains that it makes it easier to gain access to the communications of any "government official that happens to be using the network some admin takes care of."[138]

123. The post – entitled "I hunt sys admins" – makes clear that there is a continuous effort to target such individuals, and that intrusive surveillance is acknowledged as not just something to be deployed against terrorists or other national security threats. "Sys admins are a means to an end," the NSA staffer writes. [139]

124. The NSA staffer explains how, in many circumstances, targeting the system administrator is his or her first port of call; "many times, as soon as I see a target show up on a new network, one of my first goals is, can we get CNE access to the admins on that network, in order to get access to the infrastructure that target is using?"[140]

125. Both CNE, and other SIGINT capabilities such as interception, are used in tandem to attack system administrators. The post continues, "all of this boils down to getting an admin's webmail/facebook account in order to QUANTUM it and get CNE access to their box [computer]."[141]

126. Der Spiegel describes how one computer expert working for a data storage company was heavily targeted: "[a] complex graph of his digital life depicts the man's name in red crosshairs and lists his work computers and those he uses

[138] Targeting System Administrator Accounts to Access Networks (20 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140320-intercept-targeting_system_administrator_accounts.pdf [Accessed 28 September 2015]

[139] Ibid

[140] Ibid

[141] Ibid

privately ('suspected tablet PC'). His Skype username is listed, as are his Gmail account and his profile on a social networking site. […] In short, GCHQ knew everything about the man's digital life." [142]

127. In another operation, codenamed AURORAGOLD, the NSA specifically monitored the content of messages sent and received by more than 1,200 email accounts belonging to individuals not considered a national security threat, nor suspected of any criminal wrongdoing, but who were associated with major mobile phone network operators. By intercepting confidential company planning papers, AURORAGOLD helped the NSA deploy CNE against telecommunications companies.[143]

128. GCHQ similarly attacks telecommunications companies by vacuuming up "a large number of unrelated items" from the private communications of targeted employees.[144]

129. Suspicionless people other than system administrators are also targeted. One Belgian computer science professor, Jean Jacques Quisquater, had his personal computer targeted and infected with Regin, malware now confirmed to have be developed by GCHQ and NSA. According to Quisquater, he is aware of other computer science professors have also been targeted by the same attackers.[145] His scientific research is focussed on devising methods for security and cryptography which he publishes in conferences, journals, patents and standards. When he was asked why he felt he was targeted, Quisquater told newspapers, "[m]aybe cryptography research is under surveillance, maybe some

[142] Spiegel staff (11 November 2013) Quantum Spying: GCHQ Used Fake LinkedIn Pages to Target Engineers, *Der Spiegel* [Online]. Available from: http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html [Accessed 2 October 2015]

[143] Gallagher, R. (4 December 2014) Operation AURORAGOLD: How the NSA Hacks Cellphone Networks Worldwide, *The Intercept* [Online]. Available from: https://theintercept.com/2014/12/04/nsa-auroragold-hack-cellphones/ [Accessed 2 October 2015]

[144] Nakashima, E. (19 February 2015) NSA, Britain's GCHQ allegedly seized encryption keys for millions of phones, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/world/national-security/nsa-britains-gchq-allegedly-seized-encryption-keys-for-millions-of-phones/2015/02/19/369cc8b0-b883-11e4-9423-f3d0a1ec335c_story.html [Accessed 2 October 2015]

[145] Constantin, L. (3 February 2014) Prominent cryptographers targeted by malware attacks, *PCWorld* [Online]. Available from: http://www.pcworld.com/article/2093700/prominent-cryptographer-victim-of-malware-attack-related-to-belgacom-breach.html [Accessed 2 October 2015]

people hope I have some interesting information or contacts or maybe there's another goal we'll never know."[146]

Using suspicionless people as "data mules" for CNE

130. When attacking a computer, the infection with malware is only the first stage. The next stage is collecting and transmitting back information from that computer, whether that is documents, account credentials for other computer systems, or audio recorded using the computer's microphone. This is known as exfiltration.

131. In order to hide this exfiltration trail, intelligence agencies of the Five Eyes have justified even greater intrusion on suspicionless people in order to mask the fact they deployed CNE in the first place. These suspicionless individuals are described as "unwitting data mules" in one NSA presentation.[147] Their purpose, the presentation explains, is to act as middlemen, with the malware forcing their computers to act as a go-between for the NSA and the target of the attack. This is done in multiple stages, with sophisticated operations requiring the "need to transfer data and commands over two or more hops," causing a growing web of suspicionless computers to be caught up in the operation.

132. Research by one anti-virus company, Kaspersky, into a sophisticated piece of malware named Regin, which is widely believed to be the work of intelligence agencies of the Five Eyes, highlighted one such technique, explaining how one attack ended up affecting individuals and their computers from three other organisations. In one country 'X', multiple different groups were hacked, including the president's office, a research centre, an educational institution network and a bank. These victims were spread across the country but all interconnected to each other. Each of them had been attacked and infected with versions of the Regin malware, and was then instructed to communicate and pass information with the others. In this way, a peer-to-peer network was

[146] Ibid

[147] Appelbaum, J. et al. (17 January 2015) The Digital Arms Race: NSA Preps America for Future Battle. Spiegel Online [Online]. Available from: http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409-2.html [Accessed 2 October 2015]

created, allowing the Five Eye attackers to issue commands to the malware targeting the president's office via the bank's network, with the exfiltrated information passing back via the same route. [148]

133. According to Kaspersky, it is not likely the research centre, educational institution, or the bank were the true targets of the attack, but instead they were used as cover to ensure the desired infiltration of the president's office stayed in place.

Increasing the likelihood of suspicionless people being attacked by CNE

134. As individuals and institutions are now being used as middlemen for the exfiltration of data, the likelihood that other foreign intelligence, or criminal actors will target these "unwitting data mules" also increases. [149]

135. One NSA document sets out such a scenario. In a CNE attack against one country (country A), they discovered another country (country B) also had malware running on the same computers the NSA was targeting in country A. The NSA withdrew from targeting the original country A machines, and instead followed the trace back to see who country B were using as an "exfil point" outside the country and instead deployed malware against this suspicionless target, obtaining a copy of everything that country B was getting from the computer in country A. This is known as Fourth Party collection.[150]

The scale of CNE deployments

136. CNE was once a rarely used capability. This did not stay the case for long. By 2003, the use of CNE had risen dramatically, and with a few hundred NSA staff

[148] Kaspersky Lab's Global Research & Analysis Team (24 November 2014) Regin: nation-state ownage of GSM networks [Online]. Available from: https://securelist.com/blog/research/67741/regin-nation-state-ownage-of-gsm-networks/ [Accessed 1 October 2015]

[149] Fifth Party Access (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-fifth_party_access_-_when_the_targeted_fourth_party_has_someone_under_surveillance_who_puts_others_under_surveillance.pdf [Accessed 1 October 2015]

[150] Ibid

conducting on average 20-25 CNE operations a day, rising again to 100 CNE operations a day by the end of 2005.[151]

137. Since then the Five Eyes have "aggressively scaled"[152] their hacking initiatives, in the past decade computerizing some processes previously handled by humans. One key system codenamed TURBINE now "allow[s] the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually."

138. Another document confirms the scale of the ambition, stating TURBINE's goal is to "increase the current capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CNA) implants to potentially millions of implants."[153] Developed as part of the Tailored Access Operations unit, the TURBINE system is described in leaked documents as an "intelligent command and control capability" that enables "industrial-scale exploitation."[154]

139. It is unclear how many devices the Five Eyes have interfered with over the years, but some figures are available. Under one NSA program codenamed GENIE, the goal for the end of 2013 was to "increase the number of Endpoint Points-of Presence worldwide to a range of 85,000-96,000"[155] and the number of "Endpoint active accesses to 9,000-10,000."[156] Elsewhere the Washington Post reported on the LinkedIn profile of one NSA staffer, whose profile

[151] Expansion of the Remote Operations Center (ROC) on Endpoint Operations (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/23/20150117-speigel-document_about_the_expansion_of_the_remote_operations_center_roc_on_endpoint_operations.pdf [Accessed 2 October 2015]

[152] Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 28 September 2015]

[153] Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 28 September 2015]

[154] Ibid

[155] NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf [Accessed 1 October 2015]

[156] Ibid

included the fact that the 14 personnel under his command had undertaken over 54,000 CNE operations.[157]

140. In other areas, even small research teams are working out whether they can deploy CNE in bulk, forcing computers to secretly stamp unique identifiers into every internet packet that leaves that machine. These plans to conduct “large scale staining of machines” have already being deployed.[158] Activities like this, that utilize the bulk capabilities of both SIGINT and CNE will likely increase, as one leaked document explains “this is great example of CNE effects enabling passive SIGINT and then this in turn enabling CNE and will hopefully lead the way for future joint projects.”[159]

141. Other malware tools such as SECONDDATE can be used both for tailored “surgical” attacks and to launch bulk malware attacks against computers. According to a 2012 presentation, the tactic has “mass exploitation potential for clients passing through network choke points.”[160]

Eric

Eric King
5th October 2015

[157] Peterson, A. (29 August 2013) The NSA has its own team of elite hackers, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/ [Accessed 2 October 2015]

[158] Op MULLENIZE (4 October 2014) [Online]. Available from: https://www.eff.org/files/2013/11/25/20131004-wapo-gchq_mullenize.pdf [Accessed 2 October 2015]

[159] Ibid

[160] Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 28 September 2015]