PRIVACY INTERNATIONAL AND OPEN RIGHTS GROUP'S SUBMISSION IN RESPONSE TO THE CONSULTATION ON THE DRAFT EQUIPMENT INTERFERENCE CODE OF PRACTICE

20 MARCH 2015

Submitted to: RIPA@homeoffice.x.gsi.gov.uk

I. Introduction

Hacking, also known as computer network exploitation (CNE), is an extremely intrusive form of surveillance. It can yield information sufficient to build a total profile of a person, from his daily movements to his most intimate thoughts. It is potentially far more probing than techniques traditionally classified under the Regulation of Investigatory Powers Act (RIPA) as "intrusive surveillance". It is also rapidly becoming the intelligence services' tool of choice.

The UK has been deploying CNE for over a decade, yet the release of the draft Equipment Interference Code of Practice (EI Code) is the first time the UK intelligence services have sought public authorisation for their activities. Indeed, it is the first time the intelligence services have publicly acknowledged they engage in CNE. For that reason, this consultation regarding the draft EI Code is extremely important. Privacy International and Open Rights Group appreciate this opportunity to weigh in on whether CNE is an appropriate surveillance technique and, if it is used, the controls, safeguards and oversight that must be applied.

Unfortunately, the draft EI Code is too little, too late. The serious concerns raised by state hacking, which include intruding upon privacy in new and extremely invasive ways, undermining the security of the entire internet, and setting a precedent for other spy agencies around the world, require that the UK intelligence agencies' CNE operations be closely controlled, if they are permitted at all. Privacy International and Open Rights Group believe that the draft EI Code is not the proper way to address state-sponsored CNE. Hacking powers should be fully debated and, if approved, enshrined in primary legislation, as communications interception has been in RIPA. A six-week consultation on a draft Code is insufficient. This is especially true in light of the Intelligence and Security Committee's report calling for a complete statutory reworking of the UK's byzantine system of regulating surveillance.

While maintaining their objection to the process, Privacy International and Open Rights Group take this opportunity to assist the Secretary of State and Parliament as they consider the draft Code. First, we describe the technology underlying CNE, and its ability to enable the State to reach into every aspect of an individual's life, while also undermining the security of both any computer targeted and the internet as a whole. Given these concerns, we seriously question whether CNE should ever be deployed by the intelligence services. In the case that CNE is authorised, in the second part of this submission we put

forth a set of policies we think any CNE operation must abide by in order to help lessen the intrusion on privacy and security. We then critique the draft EI Code, which in its current form grants the intelligence services far too much leeway to hack anyone in the world with minimal authorisation, few safeguards and limited oversight. Both substantively and procedurally, therefore, the draft EI Code is deficient.

II. Computer Network Exploitation Is Far More Intrusive than Any Single Surveillance Technique Currently Deployed by the Intelligence Services

We begin this submission with a detailed explanation of the type of activities the term "Equipment Interference" may encompass. Due to their unprecedented intrusive nature, the use of these techniques raises serious privacy concerns that cannot be fully understood without knowledge of the mechanisms and scope of CNE.

The draft EI Code says very little about what is meant by the term "Equipment Interference." The Glossary definition provided focuses not on the technical capabilities of the intelligences services, but merely their broad mandate to use those capabilities to:
"a) obtain information from the equipment in pursuit of intelligence requirements;
b) obtain information concerning the ownership, nature and use of the equipment with a view to meeting intelligence requirements;
c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b); and
d) enable and facilitate surveillance activity by means of the equipment."
(Section 10, Glossary)

The interference may be with any "equipment producing electromagnetic, acoustic and other emissions, or information derived from or related to such equipment."

This definition raises more questions than it answers. What "equipment" may be targeted? What information can be obtained from targeted equipment, or when the intelligence services "enable and facilitate surveillance activity by means of the equipment"? How is that information obtained? What harm may be done when the intelligence services "locate and examine, remove, modify or substitute equipment hardware or software"?

Privacy International and Open Rights Group attempt to answer these questions below. In short, the type of equipment that can be targeted is vast, ranging from personal computers and mobile phones to wifi-enabled televisions, smart meters and energy grids, and communications network infrastructure. The information that may be obtained from these devices is potentially limitless. And it is most often acquired through the use of malicious code that can damage not only the target devices, but threaten the security of any network on which it resides,

including the entire internet. In promulgating this draft Code, the ministers are displaying a troubling lack of candour by failing to acknowledge how intrusive equipment interference can be and the risks it poses to the security of our devices and communications infrastructure.

A. What "equipment" may be targeted?

Using the term "equipment" to describe the subjects of the intelligence services' CNE activities makes those targets sound relatively benign. The equipment at issue, however, encompasses almost all of the devices we use everyday. Most obviously, through this draft Code the intelligence services are seeking permission to hack into desktop computers, laptop computers, tablets and mobile phones.[1] These "equipment" alone contain vast amounts of information about every aspect of their users' lives.

Additionally, any device that is connected to a modern network (and even some that are not, see section II.C.) is fair game under the draft Code. Such devices now include televisions, refrigerators, baby monitors, smart meters, smart Barbies and a myriad of others. By allowing the intelligence services to access these devices, the Code grants the services a window into the most intimate moments of our lives. For instance, smart fridges can reveal when and what we eat and smart televisions can record our activities.

Network exploitation does not stop at individual machines. It can include the network infrastructure itself, such as the routers that direct network traffic and the computers that control network security.[2] Exploiting infrastructure potentially gives the intelligence services access to millions of devices and masses of communications.

B. What information can be obtained from target equipment, or when the intelligence services "enable and facilitate surveillance activity by means of the equipment"?

Equipment interference has the potential to be far more intrusive than any current surveillance technique, including the interception of communications. CNE allows the intelligence services to engage in a wide range of activities. At one end of the spectrum is the ability to collect identifying information from networked devices, such as laptops and mobile phones, which may include names and IP addresses, but may also reveal sensitive profile information supplied by a user in registering a device, such as his location, age, gender, marital status, income, ethnicity, sexual orientation, education and family.

---

1 Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework* (hereafter "ISC Report"), at 14 n.13 (listing that devices that may be targeted, including "computers, servers, routers, laptops, mobile phones and other devices").

2 Ibid.

Once they gain access to a device, there is no technical barrier preventing the intelligence services from obtaining far more information.[3] The intelligence agent has total control over the targeted device, as if he were its (very technically sophisticated) owner. As a British company that sells equipment interference technology boasts, CNE technologies "give full access to stored information with the ability to take control of target system's functions to the point of capturing encrypted data and communications."[4] The intelligence agent can access any stored data, including documents, emails, diaries, contacts, photographs, internet messaging chat logs, and location records on mobile equipment. He can see anything typed into the device, including login details and passwords, internet browsing histories, and draft documents and communications the user never intended to share. He can recover files that have been deleted. He can control any functionality, including surreptitiously turning on the microphone, webcam and GPS-based locator technology. He can even re-write the code that controls the device, adding new capabilities and erasing any trace of his intrusion.[5]

As has been recently revealed, this intrusion can be multiplied when the intelligence services choose to target devices that are associated with communications networks. By hacking Belgacom, a Belgian telecommunications group, GCHQ might gain access not only to Belgacom's machines, but to those of all its users.[6] By hacking Gemalto, a manufacturer of SIM cards and next-generation credit cards, the intelligence services can obtain the keys to much of the world's encrypted mobile phone communications.[7] Energy networks, private networks of banks and many others might also be targets. CNE can even facilitate mass surveillance if components of the internet backbone are infiltrated, such as landing stations for the undersea cables that carry our communications between continents.

---

3 For a description of just some of the intelligence services' capabilities, please see Ryan Gallagher and Glenn Greenwald, "How the NSA Plans to Infect 'Millions' of Computers with Malware," *The Intercept* (12 March 2014), available at https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers- malware/

4 FinFisher, "Governmental IT Intrusion and Remote Monitoring Solutions," available at https://www.documentcloud.org/documents/408444-finfisher-product-portfolio-english-gamma-2011.html

5 James Ball, "Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data," *The Guardian* (28 January 2014), available at http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data

6 "Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm," *Der Spiegel* (20 September 2013), available at http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

7 Jeremy Scahill and Josh Begley, "The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle," *The Intercept* (19 February 2015), available at https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

It is for these reasons that one of the few courts to address the surveillance use of CNE, the German Supreme Court, declared CNE to be much more intrusive than traditional forms of communications interception.[8] Indeed, if the interception of communications is the modern equivalent of wire- tapping, then CNE is the modern equivalent of entering someone's house, searching through his filing cabinets, diaries and correspondence, and planting devices to permit constant surveillance in future, and, if mobile devices are involved, obtaining historical information including every location he visited in the past year.[9] The only differences are the ease and speed with which it can be done, the ease of concealing that it has been or is being done, and the fact that, if a mobile device has been infected, the ongoing surveillance will capture the affected individuals wherever they are.

C. How is the information obtained?

The intelligence services can use a number of creative and ever-evolving methods to obtain the information outlined above. Most involve the deployment of malware, 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.

A few of the most common methods for deploying malware include social engineering, "watering hole" attacks, "man in the middle" attacks, and surreptitious entry.

Social engineering involves sending an email or other message to the target that contains a link or attachment infected with malware. In order to trick the target into clicking on the link or attachment, the agent sending the email usually impersonates a person or organisation with which the target is familiar. Such impersonation can raise serious public concerns, especially when the agencies impersonate well-known and trusted third parties. This method, while prevalent, is becoming relatively well known since it is often used by scammers and others who attempt to take over devices for criminal purposes. Due to public education campaigns, more people are now aware of and may not be taken in by social engineering.

A **"watering hole" attack** facilitates the deployment of malware without any affirmative act on the part of the target. It is usually accomplished by installing custom code on a website that will infect with malware any device that visits that website. Systems are available for purchase that can allow for such infections

---

[8] Zitierung: BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 267), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

[9] The US Supreme Court agrees that access to content on a mobile phone is analogous to "the most exhaustive search of a house." *Riley v California*, 134 S. Ct. 2473, 2489-91 (U.S. 2014).

across a whole country's network.[10] Of course, that means that anyone who visits the website, whether a target or not, may be infected, significantly increasing the impact on suspicionless parties. For this reason, use of watering holes should rarely, if ever, be permitted.

A **"man in the middle" attack** similarly 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 his response, the agent will send back malware instead of, or sometimes in addition to, the requested content. "Man in the middle" attacks may appear as updates to common plug-ins like Adobe Flash Player[11] or to web browsers, such as Firefox.[12] Other forms of infection occur as a target downloads a file from the web.[13] Technology is in development that would allow man-in-the-middle-style attacks to be conducted on a mass scale through automated implants.[14]

Once malware is deployed, the intelligence services may even involve suspicionless third parties in the extraction of information from targets. Sometimes called "data mules",[15] third party equipment can be used as an intermediate step in obtaining data from target devices. This helps the agencies cover their tracks, but could result in the innocent third party being suspected of wrongdoing.

Finally, even devices that are not connected to the internet may be subject to attack if the intelligence agencies can otherwise gain access to them through **surreptitious entry.** This may include breaking and entering into homes or offices, then infecting the target device by, for instance, installing malware contained on a USB stick.

---

10 FinFisher, "Remote Monitoring & Infection Solutions," available at https://www.documentcloud.org/documents/810313-757-gamma-group-brochure-product-description.html

11 Ibid.

12 Alex Fowler, "Protecting our brand from a global spyware provider," The Mozilla Blog (30 April 2013), available at https://prod01-cdn03.cdn.firstlook.org/wp-uploads/sites/1/2014/03/turbine-large.jpg

13 FinFly LAN, https://www.documentcloud.org/documents/408439-04-finfly-lan.html

14 "Industrial-Scale Exploitation," *The Intercept* (12 March 2014), available at https://firstlook.org/theintercept/document/2014/03/12/industrial-scale-exploitation/

15 Jacob Appelbaum et al., "The Digital Arms Race: NSA Preps America for Future Battle," *Der Spiegel* (17 Jan. 2015), available at http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409-2.html

D. What harm is done when the intelligence services "locate and examine, remove, modify or substitute equipment hardware or software"?

CNE is not only extremely intrusive, but also has the potential to undermine the security of the target device and the internet as a whole. Fundamentally, malware and other CNE methods are designed to allow an unauthorised person to control another's computer. The security hole created can be exploited by *anyone* with the relevant technical expertise. Passwords, encryption keys and personal files can be collected and copied, either to further other intelligence aims or for a criminal purpose, depending on who has found the vulnerability in the target's system. CNE is the modern equivalent of breaking into a residence, and leaving the locks broken or damaged afterwards.

Furthermore, computer systems are complex and unpredictable. And malware is often not fully vetted to determine its effects on the system.[16] Its installation alone may cause damage, such as the destruction of property or data on the computer, including draft documents or family photos. Intentional alteration is also possible, raising serious concerns regarding the integrity of evidence obtained from the target device. Covert modifications of the system and the planting of data and network logs could lead to misrepresentations of activity and perversions of justice.

The integrity of every network, including the entire internet, is at issue. When the intelligence services release malware, they rarely will be able fully to control its distribution. For instance, the malware the US government used to infect Iranian nuclear facilities, Stuxnet, was later found on computers at the corporation Chevron.[17] If a watering hole is deployed, the government cannot dictate who lands on the infected website. A link to a fake news story, directly emailed to a target, might be forwarded on to others or posted on social media. A server that is the subject of a man in the middle attack could host multiple websites, exposing all those website users to exploitation.

If a network communications hub is targeted, that security vulnerability will expose all network users. Or the attack might shut down the network entirely, such as occurred when the US attacked communications infrastructure in Syria.[18] Accordingly, CNE may lead to significant economic losses for network administrators and users and create backdoors for outside access to all personal information contained within the network.

---

16 Chaos Computer Club, "Chaos Computer Club analyzes government malware" (October 8, 2011), available at: https://www.ccc.de/en/updates/2011/staatstrojaner

17 Rachel King, "Stuxnet Infected Chevron's IT Network," *Wall St. J.* (8 November 2012), available at http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/.

18 Spencer Ackerman, "Snowden: NSA accidentally caused Syria's Internet blackout in 2012," *The Guardian* (August 13, 2014), available at: http://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet- outage-civil-war

Perversely, government use of CNE fuels a commercial market for security vulnerabilities known as "zero-day" exploits. Zero-days are vulnerabilities in computer software which have yet to be detected by the software manufacturer or designer. Zero-days are thus very valuable for intelligence services and criminals alike, as there is no defence against them.

Far from trying to stem the trade in these vulnerabilities, governments are often the highest bidders for them.[19] After buying zero-days, governments are reluctant to reveal them to software makers because the hole might then be repaired, curtailing government access. Governments thereby risk developing interests adverse to their own citizens' and businesses' security, which is undermined by the continued existence of zero-day exploits. Each time the intelligence services use a zero-day exploit, they are also risking its discovery by criminals and other intelligence services who might use it against British citizens.[20] While the ISC reports that GCHQ reveals some zero-day exploits to manufacturers, it fails to state how fast they are turned over or confirm that all such vulnerabilities are reported.[21]

III. If Permitted at All, Computer Network Exploitation by the Intelligence Services Should Only Be Allowed In the Most Limited of Circumstances With the Highest Safeguards In Place

The intelligence services' mandate is to protect our security, not undermine it. As the ISC recently reported, in addition to its intelligence gathering functions, GCHQ has an "'Information Assurance' role, providing government, industry and the public with advice and guidance to protect their IT systems and use the internet safely."[22] The preceding section demonstrates CNE often has the opposite effect, threatening the security of target devices and the internet as a whole.

---

19 Nicole Perlroth and David E. Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code," *N.Y. Times* (13 July 2013), available at http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html ("But increasingly the businesses are being outbid by countries with the goal of exploiting the flaws in pursuit of the kind of success. . . that the United States and Israel achieved. . ."); Joseph Menn, "Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback," *Reuters* (10 May 2013), available at http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510 ("Even as the U.S. government confronts rival powers over widespread Internet espionage, it has become the biggest buyer in a burgeoning gray market where hackers and security firms sell tools for breaking into computers.").

20 Sean Gallagher, "NSA secretly hijacked existing malware to spy on N. Korea, others," *ArsTechnica* (19 January 2015), available at http://arstechnica.com/information-technology/2015/01/nsa-secretly-hijacked-existing-malware-to-spy-on-n-korea-others/

21 ISC Report, at 69 (paragraph 183).

22 ISC Report, at 68 (paragraph 182).

Whether CNE is ever justifiably deployed, therefore, is still an open question. It is very difficult to balance the desire for a new, very powerful surveillance tool with the likelihood of sabotaging the security of our business and personal communications. The privacy intrusion involved further complicates the matter, as CNE reaches further into our lives and thoughts than any heretofore known form of surveillance.

For these reasons, Privacy International and Open Rights Group urge the Secretary of State and Parliament to very seriously consider if CNE can ever be safely and proportionately used. As the UN Special Rapporteur on freedom of expression has declared, "[f]rom a human rights perspective, the use of such technologies is extremely disturbing."[23] Even if it is to be used, CNE should only be deployed in the most compelling and narrowly-defined circumstances, with the greatest oversight and safeguards. The following set of principles, if adopted, would help ensure that CNE is used only infrequently when most needed and justified. Unfortunately, the draft EI Code does not come close to fulfilling these requirements.

* * * * *

The following principles are based, in part, on those set forth in the International Principles on the Application of Human Rights to Communications Surveillance,[24] which have been signed by hundreds of human rights organisations from around the world. Based on national and international legal norms, the Principles set a threshold for intelligence services to meet in order to guarantee their activities are necessary and proportionate – as required by European Convention on Human Rights as incorporated into the Human Rights Act of 1998.

First, a CNE operation shall not be undertaken unless there is a high degree of probability that a serious crime[25] or specific threat to a national security[26] has

---

23 *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, UN General Assembly, A/HRC/23/40, at paragraph 62, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

24 *International Principles on the Application of Human Rights to Communications Surveillance*, available at https://en.necessaryandproportionate.org

25 The definition of a serious crime should be a narrow one. Section 4.4 of the draft Code appears to be an attempt to define serious crimes in the context of the internal use of equipment interference. Yet even that definition is not narrow enough. It could capture broad swaths of crimes through its apparent inclusion of conspiracy, or "conduct by a large number of persons in pursuit of a common purpose", and by setting the bar based on the length of the sentence imposed not the nature of the crime.

been or will be carried out. This prohibits the intelligence services from engaging in fishing expeditions or from targeting people or devices that do not have a direct connection to an identified threat or serious crime. Those not suspected of criminal involvement or considered a threat to national security should not be targeted under any circumstances, even if doing so may be more expedient.

The draft EI Code completely fails to incorporate this policy. Far from protecting suspicionless individuals or devices from invasive surveillance, the draft Code sanctions it. Most troubling, section 2.12 of the Code explicitly permits intrusion into devices that are "not intelligence targets in their own right" so long as the intrusion is treated as "intended". This provision seems to give the intelligence services free reign to target whomever they like, so long as they can make a tenuous connection to a statutory purpose. Under section 2.12, they can deliberately target a person they know is innocent of any wrongdoing. Indeed, the application for a section 5 warrant need only provide the "details of any offence suspected or committed *where relevant*" (Section 4.6, emphasis added). And the identity of the individual who owns or possesses the target equipment need only be specified "where known" (Section 4.6). Together, these provisions make clear that a connection to a serious crime or specific threat is purely optional. The intelligence services are being given leave to go on a fishing expedition likely to impact many unknown people about whom the services possess no suspicion.

Granting the intelligence services such a broad scope is neither necessary nor proportionate. Indeed, one of the few judges in the world to address deployment of CNE for surveillance purposes refused to issue a warrant on the basis that suspicionless individuals might be caught up in the intrusive search.[27] The German Supreme Court similarly refused to permit CNE unless a very strong connection to a predominantly important legal interest – a threat to life, limb, freedom or the continued existence of the state – could be concretely demonstrated.[28] By ignoring such precedent, the UK risks not only violating the human rights of its targets, but also establishing one of the most permissive surveillance regimes in the world – no doubt inspiring other countries to be similarly lax in their policies. Indeed, it appears that at least one country, Bahrain, has already been utilising CNE against human rights activists located on

---

[26] National security should also be interpreted narrowly, for instance as described in the Siracusa Principles, available at http://www1.umn.edu/humanrts/instree/siracusaprinciples.html

[27] *See In Re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 758-61 (S.D. Tex. 2013).

[28] Zitierung: BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 267), available at http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

British soil.[29] The draft Code sanctions such behaviour, putting the privacy of all of us at risk.

Second, a warrant for CNE shall not issue unless there is a high degree of probability that evidence relevant and material to a serious crime or specific threat to a national security would be obtained by accessing the equipment identified. Similar to the first policy, this requirement is designed to prevent the intelligence services from invading devices that are unlikely to contain useful information. Indiscriminate deployment of CNE is prohibited.

Once again, the draft Code fails in this regard. In particular, section 7 allows the Secretary of State to authorise CNE in bulk in support of a "broad class of operations." Once the authorisation is issued, no further warrant need be sought nor specific evidence of wrongdoing provided. The intelligence services are free, subject to internal approval, to target any device, or many devices at once, so long as they are related to the approved class of operations and believed to be outside the British Islands. The potential breadth of the authorisation is compounded by the fact that the Secretary of State need only be satisfied the "nature and likely consequences of any acts done in reliance on the authorisation will be *reasonable*" (Section 7.8, emphasis added). Proportionality is not mentioned. The ISC recently revealed that, as of October 2014, GCHQ was conducting its overseas equipment interference under only five such class authorisations.[30]

As we have now discovered in other contexts, this purported distinction between internal and external, for the purposes of surveillance, is essentially meaningless. The ISC confirmed as much in its report.[31] The information of UK residents is often hosted on services that store their data abroad – such as most major internet service providers like Google, Facebook and Twitter. To the extent external communications networks are being hacked, they are also likely to be carrying UK residents' communications. And as we learned recently, the goal of external CNE operations may be to obtain encryption keys or other resources to allow the intelligence services more effectively to spy on those within the British Islands.

Furthermore, even if the agencies could limit their CNE operations so that they only affect those who are abroad, setting a lower privacy standard for the rest of the world is unjustifiable and discriminatory. In our modern, connected age, there is no rationale for providing any less electronic privacy protection to another countries' citizens. Indeed, by declaring it can indiscriminately hack any computer in the world, the UK is setting a very low bar for other countries'

---

29 Adriana Edmeades, "Bahraini Government, with Help from FinFisher, Tracks Activists Living In the UK," Privacy International (13 October 2014), available at https://www.privacyinternational.org/?q=node/460

30 ISC Report, at 88 (paragraph 234); see also ibid. at 65-66 (the ISC redacts the number of operations actually carried out under these broad authorisations)

31 ISC Report, at 40 (paragraph 108).

intelligence services, essentially inviting them to issue similar policies and attack UK citizens indiscriminately.

Third, any information accessed via CNE shall be confined to that which is relevant and material to the serious crime or specific threat to national security alleged. Much like the first and second policies, this requirement is designed to limit the negative privacy implications of CNE. Once an intelligence agent exploits a device, he has complete control over it and all the information it contains. He should not be allowed to trawl through the device looking for anything of interest. Any access should be explicitly circumscribed by the warrant issued, and oversight mechanisms should be in place to make sure those restrictions are honoured. Any immaterial information collected, despite these precautions, should not be retained, but immediately returned or destroyed. The EI Code is silent on these matters.

Complete control over a device also means the agent can alter or delete any of its contents. This capability raises serious concerns, especially regarding the admissibility of any evidence obtained from the compromised device. For that reason, there should be a strong prohibition on altering or deleting the contents of any target equipment. Furthermore, if evidence obtained via a CNE operation is introduced during a criminal proceeding, the government should provide disclosure regarding the operation so breaches of the chain of custody or alteration to data may be investigated, as appropriate. Again, there is no mention of these concerns in the draft Code.

Fourth, before a warrant for CNE is issued, the applicant must demonstrate that other less invasive techniques have been exhausted or would be futile, such that CNE is the least invasive option. Given that CNE is the most intrusive current form of surveillance, this requirement will rarely be satisfied. The draft EI Code makes some nods to this requirement, but does not go far enough. Whether the information sought could "reasonably be obtained by other less intrusive means" is part of the proportionality assessment for a section 5 warrant (Sections 2.6, 4.7). A section 7 authorisation is presumably subject to the same requirement, although that is not made explicit in the draft Code. Yet, given how intrusive CNE is, the Code should include a blanket prohibition on its use if another less intrusive surveillance method is available, even if less convenient.

Fifth, the intelligence services should not engage in CNE that is likely to make the device targeted, or communications systems generally, less secure. As discussed above, insecurity is often the inevitable result of CNE operations, whether they introduce malware into a specific device that can later be exploited by criminals or create a market for zero-day exploits or set loose malicious code that can infect many other machines. The use of self-replicating software implants is particularly troubling as these can find their way out of target systems and infect a much broader range of actors. The consequences of creating such insecurity, which include undermining the business and communications infrastructure on which the world now relies, generally far outweigh any benefit. For that reason, the intelligence services should strongly hesitate before employing CNE. This concern is nowhere reflected in the draft EI Code.

Sixth, given the extreme intrusiveness of CNE, and the other concerns we raise throughout this submission, its use should be subject to the highest levels of judicial authorisation. At minimum, no CNE operation (internal or external) should be undertaken without an authorising warrant that identifies the target and its connection to a serious crime or a specific threat to national security, declares there is a high probability evidence of the serious crime of specific threat to national security will be obtained, precisely and explicitly describes the method and extent of the proposed intrusion and the measures taken to minimise access to irrelevant and immaterial information, and declares that all less intrusive methods have been exhausted or would be futile. An independent judge should approve that warrant, and conduct periodic reviews of its continued efficacy. The warrant should not issue for a period of longer than one month, although it may be renewed on a monthly basis with sufficient cause, including an explanation of why the information sought has not yet been obtained. Finally, after an operation has concluded, the target should be notified of the intrusion, unless doing so would create an overriding, specific and articulable threat to national security.

The draft Code, once again, falls far short. While a warrant is required under section 5, none is needed for section 7 activities so long as there is authorisation in place for the broad class of operations. And, as discussed previously, even a section 5 warrant fails to require a strong nexus between the target and a serious crime or threat to national security. While regular reviews of section 5 warrants are mandated, no frequency is set for those reviews (Section 2.13). The warrant is renewable every six months, an extremely long period of time for the intelligence services to have total control over a target (Section 4.10).

Neither a section 5 warrant nor a section 7 authorisation is approved by an independent judicial authority. Section 3 of the draft Code emphasizes the troubling nature of this arrangement. It permits the intelligence services deliberately to target and use legally privileged and confidential information. While sharing that information with a prosecutor in a criminal matter is prohibited, the privileged communications of adverse parties may be accessible to the agencies in civil proceedings (Section 3.16). The draft Code prohibits the agencies from relying on such privileged information to gain a litigation advantage, but once privileged information is seen, it is almost impossible to put the genie back in the bottle. At the very least, an independent judge should approve such operations that could confer an unfair advantage on the intelligence services.

Seventh, in addition to strict authorisation protocols, CNE should be subject to stringent independent oversight. As required by the Intelligence Services Act of 1994 (ISA), the Intelligence Services Commissioner will oversee CNE activities. Currently, the Commissioner's reports are quite vague regarding the types of warrants issued and the extent of the privacy violations that result from reported "errors". For instance, in his 2013 report the Commissioner concluded that GCHQ was acting entirely within the law, despite allegations of illegality based on the Snowden revelations. Subsequently, the Investigatory Powers

Tribunal (IPT) has ruled that GCHQ's intelligence sharing with the US was unlawful prior to December 2014.[32] The disparity between the IPT's conclusion and the Commissioner's report is troubling. The Commissioner must engage in a more thorough and critical review of the intelligence services activities. This should include reporting not only on the total number of warrants issued under the ISA, but the types.

The recent ISC Report bolsters the conclusion that more oversight is needed. For instance, the ISC criticises the services for failing to keep adequate records of operational activity under their section 7 class authorisations.[33] Without such records, it's impossible for any independent body to oversee the intelligence services activities. Yet even the ISC Report does not go far enough. It critiques record-keeping without questioning the underlying policy that permits such broad authorisations in the first place.

If the UK is to sanction its intelligence services' use of CNE, much more effective oversight methods and bodies must be established. In particular, given the technical complexity of CNE, any oversight body must be technically competent in order effectively to assess the intrusion on privacy and the security risks created by such constantly evolving technology. As discussed above, those security risks fall into two distinct categories, risk to the device targeted and risks created by the development and fostering of these invasive technologies, such as the preservation of zero-days. While these risks need to be fully understood by the intelligence services, they also need to be subject to external oversight, as the agencies conflicting motivations may prevent them from accurately assessing the impact of the risk.

Eighth, CNE should not be used to circumvent other legal mechanisms for obtaining information. For instance, the broad provisions of section 7 might be construed as authorising the intelligence services to hack into servers containing communications and data being stored by major service providers like Google. There are already legal mechanisms in place, such as the Mutual Legal Assistance Treaties (MLATs), to obtain such information. Those processes should not be ignored or circumvented, even if they may be more cumbersome. To do so not only threatens privacy and the rule of law, but also risks doing violence to the principle of the sovereign equality of nations.

Ninth, any information obtained via CNE should be accessed only by authorised UK intelligence agencies, and used only for the purpose and duration for which authorisation was given. CNE should not routinely be shared with other agencies within the UK, or with other countries' intelligence agencies. Over the last several years, we have become increasingly aware that the intelligence services, especially GCHQ, are strongly intertwined with the US National Security Agency (NSA), and share data with a number of other countries including the other members of the Five Eyes Alliance: Australia, Canada and New Zealand. That

---

32 [2015] UKIPTrib 13_77-H, available at http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf

33 ISC Report, at 66.

sharing is particularly pervasive during alleged joint CNE operations.[34] This permissive sharing not only compounds the privacy violation, but further undermines purported safeguards provided for citizens by their own countries, as GCHQ may capture information from citizens of the countries with which it partners, then share that information with those very same countries.

For these reasons, intelligence sharing should be prohibited without substantial safeguards, narrow authorisations and effective oversight. The draft Code provides neither. It allows information gathered from CNE operations to be disclosed "outside the service," so long as the person obtaining the information needs to know it and has sufficient security clearance (Sections 6.6, 6.11). No oversight of such disclosure is specified, nor is an explanation provided as to how these secondary recipients will be forced to comply with any safeguards imposed. No prohibition is placed on sharing information collected about a person with his country of origin. Nor does the draft Code address how the UK intelligence services should treat information obtained by other countries via CNE then shared with the UK.[35]

Tenth, and finally, <u>any individual or entity that has been a target of CNE should be able to seek redress, including those from other countries who may have been targeted</u>. Without an effective redress mechanism, the intelligence services cannot be held to account if they abuse their power. Currently, redress for surveillance abuses is hard to obtain. The Investigatory Powers Tribunal rarely finds in favor of applicants.[36] The UK police have not been much better when it comes to abuses committed by other regimes against those present in the UK. Privacy International has assisted several targets of foreign surveillance to bring criminal complaints that have resulted, so far, in no charges filed.[37] Notification, as described in our sixth principle, will play an important role in allowing effective redress. The draft Code, however, does nothing to alleviate this issue as it does not even mention redress.

IV. Computer Network Exploitation Powers Should Be Presented In Primary Legislation for Full Consideration By Parliament, Not Rushed Through in a Draft Code

As the preceding discussion demonstrates, the UK intelligence services' use of CNE raises serious privacy and security concerns. The decision to sanction such activity should not be rushed. Adequate authorisations, safeguards and

---

34 *See, e.g.*, Jeremy Scahill and Josh Begley, "The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle," *The Intercept* (19 February 2015), available at https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

35 ISC Report, at 94 (recommending that intelligence sharing be governed by a clear and public legislative regime).

36 Investigatory Powers Tribunal, "Functions – Annual case statistics," available at http://www.ipt-uk.com/section.aspx?pageid=5

37 *See, e.g.*, "Privacy International Files Criminal Complaint on Behalf of Bahraini Activists Targeted by Spyware FinFisher," Privacy International (13 October 2014), available at https://www.privacyinternational.org/?q=node/451

oversight must be put in place. The draft Equipment Interference Code of Practice fails in this regard.

The draft Code also has serious international repercussions. It authorises indiscriminate hacking of foreign targets, opening up UK citizens to similar attacks from other countries. When such government CNE has been discovered, it has caused diplomatic crises.[38]

No detailed statutory authorisation for CNE currently exists. CNE powers are much more intrusive than any surveillance heretofore contemplated, including communications interception. If the RIPA is necessary for lawful interception of communications, it follows that CNE should also be regulated in primary legislation. The ISC has come to a similar conclusion, recommending a full overhaul of the statutory surveillance regime, which should include CNE activities if they are to be authorised.[39] Proposing to regulate such powers in a Code of Practice, which as secondary legislation receives much less parliamentary attention, is inappropriate. Hacking is the intelligence services' most intrusive and powerful tool yet. It must be taken seriously.

Thank you for your consideration of these comments. We are content to have this submission published and attributed to our organisations. If we may be of any additional assistance, we may be contacted as described below.

Caroline Wilson Palow
Legal Officer
Privacy International
62 Britton Street
London EC1M 5UY
Tel. 020 3422 4321
caroline@privacyinternational.org

Javier Ruiz Diaz
Policy Director
Open Rights Group
Free Word Centre
60 Farringdon Road
London EC1R 3GA
Tel. 020 7096 1079
javier@openrightsgroup.org

---

[38] Ryan Devereaux and Cora Currier, "European Lawmakers Demand Answers on Phone Key Theft," *The Intercept* (20 February 2015), available at https://firstlook.org/theintercept/2015/02/20/gemalto-heist-shocks-europe/

[39] ISC Report, at 67, 103. The Report also reveals that the intelligence services are developing decryption capabilities and otherwise attempting to read encrypted communications with only minimal authorisation and oversight. While not the subject of this draft Code, we believe such activities should also be addressed in any revision of the statutory surveillance regime.