ERA Forum (2020) 20:423–438
https://doi.org/10.1007/s12027-019-00571-z

ARTICLE

Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice

Steven David Brown[1]

Published online: 6 August 2019

Abstract Law enforcement use of hacking techniques has become well-established and is an inevitable consequence not only of endemic anonymization used by computer-based criminals, but also of the increasing dominance of cloud-based computing models that challenge traditional notions of jurisdiction. Whilst recognising the many and legitimate concerns of privacy watchdogs this article explores how and why law enforcement uses malware to target criminals who would otherwise operate with virtual impunity.

Keywords Hacking · Law enforcement · Electronic evidence · N.I.T.s · Cyber

Criminal justice has always recognised exceptions for law enforcement when it comes to actions that would otherwise be regarded as criminal. Given the right set of circumstances, officers may carry and use weapons, offer to sell narcotics, physically restrain and detain members of the public, seize property etc, all in support of the 'greater good'. These exceptions have evolved over centuries along with suitable safeguards and (in many countries) a generally robust system of judicial oversight. They reflect the fact that, in maintaining law and order and in protecting the public, sometimes, the application of coercive and intrusive acts against individuals and in private spaces may be necessary and in the public interest.

Consider, for instance, what happens during the execution of a typical search warrant in the 'real' physical world: Having convinced the appropriate authority of the legal formalities and of a reasonable suspicion, usually substantiated on oath, that

✉ S.D. Brown
writeinzeit@gmail.com

[1] Barrister, CFE, Vienna, Austria

evidence of a crime will be found on a premises,[1] the designated officers attend the stated location. In effecting entry, the search team may legitimately resort to force which may involve causing damage. Once inside, and usually against the remonstrations of the occupiers, they will proceed to rifle through the cupboards and drawers looking for items listed in the warrant. As they do so they are very likely to come across intimate articles and confidential correspondence, even privileged material, but, if such items resemble those mentioned in the warrant, the search team must nevertheless inspect them to ensure they have no evidential value, are not being used to conceal evidence, and/or are, indeed, covered by 'privilege'. More than that, the searching officers may well be intruding into a shared living space and be sifting through property that belongs to third parties who also reside there and whom are not suspected of any wrongdoing. Their property also has to be viewed and reviewed in order to be excluded. Once seen, any confidential matter cannot be forgotten and, should that extra, unrelated material be indicative of other offences, further enquiries will ensue.

One traditional element of any lawful search warrant is that the premises must be clearly and specifically identified. Unfortunately, when it comes to investigations into computer-based crime the challenges involved in attributing criminal activity to an individual, let alone a physical location, can be a very real impediment.[2]

The usual first step in identifying a suspect through cyberspace is to trace the Internet Protocol (IP) Address involved.[3] Unfortunately, there are multiple, well-honed techniques by which a criminal can mask his or her true IP address or implicate the IP address belonging to someone else.[4] These include the use of public wifi access points, fake email and social media accounts and zombie[5] devices as well as techniques of 'anonymization' such as the use of proxy servers, virtual private networks (VPNs) and specialist software packages such as the Invisible Internet Project (I2P) or The Onion Router (Tor). Indeed, the effectiveness of VPNs in this regard has led to their prohibition in Belarus, Iraq, North Korea and Turkmenistan and to the introduction of special control measures in China, Iran, Oman, Russia, Turkey and the UAE.[6] In addition to these user-initiated concealment strategies, the creation of Carrier-Grade NAT[7] networks by Internet Service Providers (ISPs) can also have the unintended consequence of obfuscating an attacker's location. Singularly, or in com-

[1] Of course, these formalities vary from country to country.

[2] *UNODC*, [48], p. 169.

[3] An Internet Protocol (or IP) address is required for every device connected to the Internet and indicates the country of origin and the service provider involved. The service provider can then be approached to identify who was using that IP address at the relevant time.

[4] This phenomenon is sometimes referred to as 'Going Dark' in that law enforcement is increasingly blinded and placed 'in the dark' by encryption and anonymization. See *FBI* [24].

[5] A 'zombie' is a computer device that has been compromised by malware so that it is under the remote control of another and can be used to perform tasks without the owner being aware.

[6] *Mason* [35].

[7] A Carrier-Grade Network Address Translation is a network management response to the limited number of IPv4 addresses available. In a Carrier-Grade NAT one IPv4 address is configured by the Internet Service Provider to apply, in some cases, to hundreds of users. See *Europol* [21].

bination, such techniques mean attributing nefarious activity through an IP address to a device and then to a suspect user can be somewhat problematic. Indeed, this situation has been described as generating, 'an asymmetry between investigators' ability to track unlawful activity and criminals' capacity to commit crimes on the dark web.'[8] In other words, with a minimum of technical knowledge, any computer-based criminal can become to all intents and purposes unidentifiable.

When confronted with such an obstacle, criminal justice faces a stark binary choice: either to shelve the investigation or to adopt the controversial strategy of employing the same techniques as a cybercriminal (i.e. to 'hack back'). Unsurprisingly, where criminality has been sufficiently serious, the practise has been long established for law enforcement to use hacking methodologies including those which have come to be known as, 'Network Investigative Techniques' (N.I.T.s). The very prospect that emanations of the state can access the kind of intimate and confidential data shared and stored electronically by its citizenry is uncomfortable to say the least. It must be recognised that some countries are rather less benevolent than others and the concomitant risks to freedom and individual rights are high, however, we must also recognise that the technology not only exists, but is also easy to obtain and deploy. Its availability is independent and irrespective of political, diplomatic or human rights sensibilities. The abuse of such techniques is only prevented where there exists a prevailing culture of procedural restriction and an equitably applied rule of law (which, regrettably, does not constrain every state). Nevertheless, it is demonstrably the case that, going back some years, a number of very serious crimes would not have been solved and many highly dangerous criminals would not have been brought to justice had it not been for the law enforcement use and deployment of malicious software ('malware').[9]

For obvious reasons, government use of malware has tended to remain, if not deliberately kept, under the radar of public perception and is exposed only intermittently, however, as a law enforcement strategy, the potential for using hacking techniques against serious criminals was soon recognised. As early as 1998, in the Scarfo case, the FBI surreptitiously installed a malware program called KLS[10] on a mobster's computer in order to record the password (i.e. encryption key) used by him to encrypt certain incriminating files.[11] The FBI also successfully used similar software in the seminal case of Ivanov and Gorshkov to obtain login credentials and then to access the suspects' server in Chelyabinsk, Russia without making a mutual legal assistance (MLA) request.[12] The use of this malware was successfully defended in the US courts,[13] but resulted in a Russian arrest warrant being issued for the FBI Special Agent who used the login credentials to gain unauthorised access to the server in

[8] *Ghappour* [25] p. 2.

[9] One definition for malware is: "... software that is specifically designed to gain access to or damage a computer, usually without the knowledge of the owner." *Norton* [37].

[10] KLS stands for 'Key Logger System'.

[11] The affidavit of Supervisory Special Agent Murch gives a very clear and highly cogent description of this software and its application. *Murch* [36].

[12] *Lemos* [33].

[13] *Brunker* [7].

Russia to search for and download evidence.[14] This latter case highlights an interesting legal point regarding cross border access of data. Gorshkov's lawyer challenged the admissibility of the evidence obtained from the 'illegal' search in Russia, but the Judge held that the usual U.S. Fourth Amendment rights to protection against unwarranted searches did not apply to 'the property of non-residents that is located outside of the United States' and that since no one's 'possessory interest' had been affected, there had not technically been a 'search'. The information was still intact and available for access on the server in Russia and the act of retrieving the data did not preclude others' access to it. Indeed, the capturing of the data was, in the view of the court, a justified precaution to prevent its destruction while the FBI subsequently obtained a warrant to examine the data.[15] This distinction of absence of protection for non-US citizens or residents in a foreign jurisdiction appears also to have operated on the U.S. Drug Enforcement Administration (DEA) in justifying its business case for the $927,000 purchase of commercial malware in 2012:

> In 2012, having encountered evidence collection challenges in a number of foreign investigations, and without the resources to internally develop its own technical solutions, DEA sought to lawfully acquire a commercially-available tool that would allow for remote, overseas deployment of communications monitoring software on foreign-based devices used by foreign-based drug traffickers and money launderers.[16]

The fact that the DEA malware was not intended for use against targets within the USA is repeatedly underlined and demonstrates the intended extra-territorial application of this tool. We do not know whether its deployment was contingent on some form of mutual legal assistance, but the DEA's explanation was clearly drafted to avoid unhelpful and inconvenient legal questions concerning the US Fourth Amendment protection and 'unreasonable' search and seizure.

Understandably, the use of law enforcement malware has been particularly prominent in the investigation of online anonymous criminal communities, the members of which remain hidden behind freely available 'anonymizing' tools such as The Onion Router (Tor).[17] In the well-known Playpen case (the FBI's 'Operation Pacifier'), a prominent paedophile website was taken over and run by the FBI for 12 days from 20 February–4 March 2015 using a government server. This was, of course, a highly risky venture in and of itself, but by transmitting malware to those who visited the Playpen site, the FBI was able to acquire the true IP addresses of more than 8,000 alleged paedophiles in 120 countries.[18] The 'Network Investigative Technique' used in this operation had been authorised by court order and its function was described to the court in this way:

[14] *Leyden* [34].

[15] *Schroeder* [43] p. 179.

[16] The DEA cut short its use of this 'tool' in 2015. *DoJ* [19].

[17] It is important to note that the use of Tor is not of itself indicative of criminal intent. Indeed, it was invented by the US Naval laboratory for laudable reasons and supports many legitimate uses. Further information can be found here: www.torproject.org.

[18] *Cox* [16].

> An NIT consists of four main components: (1) a generator, (2) an exploit, (3) a payload, and (4) a logging server. A generator runs on the "hidden service" (e.g. Playpen) and produces a unique identification (ID) number that is associated with each user of the dark web site. The generator then transmits that unique ID, along with the exploit and payload, to each user's own computer. Once on a user's computer, the exploit takes control of the Tor browser (i.e. hacks) and executes the payload.[19]

It other words, it functioned exactly like any other malicious software except for the ultimate purpose to which it was put. The operation netted 350 arrests in the USA (548 internationally) on the basis of a single domestic warrant.[20] But, under the Federal Rules of Search and Seizure in force in 2015, such a warrant was only valid in the administrative area of the issuing court.[21] Given the online anonymity of Playpen's customers, investigators could honestly, if perhaps disingenuously, state that they did not know of any extraterritorial effect, but, as a matter of law as well as of privacy, this use of Network Investigative Techniques has, of course, been vigorously challenged.[22] In at least three of the resulting U.S. prosecutions, the presiding judges have disallowed evidence on the grounds that the Rule 41 warrant was insufficient and that the N.I.T. therefore constituted an illegal search.[23] Nevertheless, having obtained the IP addresses of foreign-based suspects, the FBI then exercised a clear and successful engagement of international cooperation partners leading to the apprehension of a large number of a particularly heinous brand of criminal. When used against paedophiles, ignoring the spirit of legal procedure certainly carries considerable sympathy and will invest proceedings with a predisposition towards approval, but should it?

In another investigation, the FBI is rumoured to have adopted an even more imaginative (though not publicly acknowledged) strategy. Operation Onymous targeted illicit market sites selling their wares on the Tor Network. When someone communicates using Tor, the message is wrapped in layers of encryption before being transmitted through a series or relay of random hubs or nodes.[24] As the message passes through each node, a layer or 'skin' of encryption is peeled away until the message exits the last node and passes to the recipient in clear text. Each node in the chain is isolated and does not know the origin of the message and the message itself is unreadable. For Operation Onymous it has been speculated that the FBI cracked the Tor Network and captured the illicit traffic by first setting up a number of their own Tor nodes and then using a denial-of-service (DoS) attack against other nodes in the network thereby forcing any messages to be relayed through FBI-controlled devices.[25] It has also been alleged that the FBI paid a 'bounty' of $1 million for the design of this

[19] This excerpt contains references not reproduced here. *Altvater* [2], p. 6.

[20] *FBI* [23].

[21] Rule 41 of the Federal on Search and Seizure has since been amended as we shall see presently. *Justia* [29].

[22] For a discussion of such concerns see *Rumold* [42].

[23] *Cox* [14] and [15], *Vitaris* [50].

[24] Nodes are computers volunteered by their owners to act as relays for Tor traffic.

[25] *Tor Blog* [47].

exploit which resulted in 17 arrests in 17 countries and dismantled up to 400 sites.[26] If this 'Onymous' technique was indeed executed as described, it must be supposed that many of the Tor nodes hit by the DoS attack were beyond the FBI's jurisdiction and belonged arguably to 'innocent' third parties. It is also likely that those using Tor for legitimate, non-criminal purposes at the same time were adversely affected and their data also captured.

The USA tends to feature prominently in discussions about law enforcement hacking. This is partly because law enforcement in the USA has been particularly active in this area, but also because the USA has an approach to the freedom of information which is liberal and far from universal. This should not, by any means, be taken as an indication that U.S. law enforcement is alone in adopting hacking strategies. As Kerr and Murphy (2017) have commented:

> ... every government is in the same boat, as every government is blocked from successfully investigating by the same technology.[27]

In Germany, in 2011, the Chaos Computer Club discovered that the German Government had been using Trojan malware since 2007 which provided a 'remote control capability' over the compromised target.[28] However, Germany did not pass specific legislation authorising the use of such a tool until 2016.[29] In the Netherlands, in 2014, it appears that the Hi-Tech Crime Team was able to neutralise a commercially marketed brand of malware called Blackshades by 'seizing the chance' to access the server on which it was hosted. Licences for the use of Blackshades software costing up to $100 had been on sale since 2010. Following this 'chance' access, 97 arrests in 16 countries ensued.[30] And in Australia, Taskforce Argos of the Queensland police, emulating the Playpen strategy, seized a Dark Web paedophile site called 'The Love Zone'.[31] During this operation police operated the website (which had 45,000 members) for 10 months, providing members of the community with a link to a malware-compromised file that routed encrypted web traffic outside of the Tor network in a similar manner to the FBI's Playpen Case. The owner of the site was eventually sentenced to 35 years imprisonment, but the total number of resulting arrests has been less easy to ascertain.[32]

In the UK, too, evidence of covert law enforcement hacking has been made public. Edward Snowden has revealed that, in 2011, GCHQ (the UK's signals intelligence agency) used a Distributed Denial of Service (DDoS) attack against the hacktivist collective, Anonymous, drawing the conclusion that: 'Online Covert Action techniques can aid cyber threat awareness.'[33] However, this led Anonymous member

[26] The number of sites taken down varies in different reports. *Greenberg* [26]; *Tor Blog* [46].

[27] *Kerr and Murphy* [30] p. 63.

[28] *Steifel* [44].

[29] The State Trojan has also been called 'Remote Communication Interception Software' by the German Federal Police (BKA). *Bundtzen* [8].

[30] *Oerlemans* [38].

[31] *Cox* [13].

[32] *Vitaris* [49].

[33] *BBC* [6].

Chris Weatherhead, who had been sentenced to 18 months imprisonment for running a server used by Anonymous in a DDoS attack, to observe ruefully how he received jail time for exactly the same activity launched by GCHQ against him.[34]

These are just a few, tangible examples of law enforcement hacking, but it is apparent that the practice is a widespread, if mostly intangible process that has spawned a commercial supply chain of significant proportions. Countries seeking national capacity in this highly technical field, often procure the services of private industry and purchase off-the-shelf products. A 2015 letter has been published, purportedly from the Israeli Ministry of Defence, which invites recipients to tender for the provision of 'Research and Development (R&D) Vulnerabilities and Zero-Day Exploits[35] and when 'Hacking Team', a well-known Italian-based provider of 'legal' malware was itself hacked in 2015, its client base was soon made public. The countries named reflect the full gamut of geographic, political and economic diversity and include: Albania, Azerbaijan, Brazil, Colombia, Czech Republic, Ecuador, Ethiopia, Hungary, Italy, Kazakhstan, Malaysia, Mongolia, Morocco, Nigeria, Oman, Panama, Poland, Romania, Russia, Saudi Arabia, Singapore, Spain, Sudan, Switzerland, Thailand, Turkey, Uganda, UAE, Uzbekistan, and Vietnam.[36] A commercial supplier of malware has also been implicated in the hacking of Whatsapp in May 2019. Whatsapp, a communications application owned by Facebook, emphasises its end-to-end encryption and uses the protection of privacy as a major selling point, but it was compromised and used as the delivery vehicle for a malware program dubbed Pegasus. This malware enables an attacker to take control of a smartphone simply by calling the target's Whatsapp number. It has been alleged that Pegasus was produced by an Israeli-based information security firm, called NSO, and sold exclusively to nation states clients. The list of alleged victims suggests it was deployed against human rights activists, journalists and dissidents.[37]

The use of off-the-shell malware by law enforcement has also encouraged a defence lawyer's tactic called 'Graymail'. As a propriety product, the software code is normally protected by a non-disclosure agreement (NDA) and commercial sensitivity. Where defence counsel successfully applies for disclosure of the code to examine the integrity of its output, the prosecution may be forced into a decision not to proceed with the case rather than breach the NDA and risk release of the code 'into the wild'.[38]

There is, therefore, ample evidence to demonstrate that law enforcement hacking is neither a recent activity nor is it restricted to just a few international actors, but has been widespread and entrenched for years. Can such an activity be justified by the technological realities of the new operational environment? Privacy watchdogs and human rights campaigners have, not unreasonably, expressed considerable discom-

[34] *Coleman* [9] p. 303.

[35] *Times of Israel* [45].

[36] *Wikipedia* [51].

[37] *Regev* [41].

[38] *Bell* [3]. NB Graymail is also used to refer to bulk spam email that was originally authorised by the recipient, but no longer wanted.

fort at the prospect that government authorities may delve into an individual's online existence with such apparent ease. Their areas of concern include:[39]

- The risk of targeting the wrong person: The very fact that the challenge of attribution is a principle justification for law enforcement hacking also means that a target cannot be identified with certainty. Consequently, there is a real risk that data of an innocent third party may be compromised by the malware by mistake;
- Such techniques are indiscriminate: Other innocent users sharing the targeted device, system or network may find themselves affected—whether by disruption or damage to the functioning of the system, or by their data being downloaded and read by law enforcement because it happens to be stored in the same place;
- Data downloaded from a target device may well contain sensitive, confidential and perhaps legally privileged or protected material which is outside the legal scope of the warrant, but will have to be captured and read to be eliminated;
- The extraterritorial nature of law enforcement hacking breaches international law and established, traditional norms of jurisdiction. In most, if not all, cases such action will involve the commission of a criminal offence in the country where the data is stored;
- The unilateral practice of government-based hacking undermines diplomatic relations and invites retaliation and escalation in unpredictable ways;
- Where government agencies discover vulnerabilities in software and/or hardware and then keep that knowledge from the manufacturers or software providers, it reduces the general level of information security for everyone;
- Likewise, when government agencies procure or produce malware to exploit those vulnerabilities, the malware may well escape 'into the wild' and subsequently be used by malicious actors;[40]
- Since the entire process is shrouded (a) in secrecy and (b) in obscure technical detail, it is extremely difficult for those expected to review, oversee and authorise such procedures to be able to ask the necessary, difficult questions;
- The legal frameworks available are often designed for a different, analogue, operational environment. Applying them by analogy to law enforcement hacking does not afford the same safeguards or protection.

Admittedly in any law enforcement application of malware, privacy concerns will be manifold and the objections demand careful examination. Unfortunately both hacking and malware are a fact of 'virtual life' and the necessary skills are all too easy to acquire. They are readily available not only to malicious actors, but also to unrestrained governments who will inevitably adopt such tools for use as and how it suits them regardless of negative publicity and remonstrations by watchdogs. Can such techniques, therefore, be reasonably denied to law enforcement for use in the inter-

[39] See, for example: *Kim* [31] or *ACLU* [1].

[40] A good example of this is the Stuxnet case. Unknown nation state actors produced an extremely elegant and sophisticated malware program called Stuxnet that was designed to damage centrifuges allegedly producing enriched uranium in Iran. Stuxnet was surgically and exclusively targeted against a particular process in a particular Siemens device. However, the malware eventually 'escaped into the wild' and the code was soon re-engineered into new versions for criminal use (including DuQu, Gauss and Flame). For a fascinating, if slightly technical, account of the whole saga, please see *Zetter* [52].

ests of justice? They imply a highly invasive investigative strategy, potentially entailing the indiscriminate collection of any third-party data stored in the same e-location. They are also highly likely to disrupt and/or cause damage to the targeted network. However, as shown above, such concerns apply equally to the search of a premises in the physical world where best and established practice entails and requires the mitigation and minimisation of any collateral intrusion. It is also undeniable that using such techniques when a target's location is unknown implies the accessing of data likely stored in a foreign jurisdiction without the formality of a Letter of Request or MLA process. Zoetekouw questions whether under such circumstances 'trained law specialists' can merely assume their own laws apply simply because they are unaware of the actual location of the data[41] and in his 2017 article, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, Ghappour voices concerns about the influence of law enforcement hacking on foreign policy:

> In the regulatory vacuum that results [from the lack of knowledge of location precluding the use of international MLA procedures], rank-and-file officers have discretion that may shape U.S. policy regarding which crimes trigger the use of cross border network investigative techniques, the breadth of hacking techniques that are used to effectuate remote searches, and whose property may be targeted.[42]

> By allowing rank-and-file officials to control how hacking warrants are executed, the existing legal process effectively allows the circumstances of the immediate investigation to dictate foreign policy interests in cultivating soft power.[43]

With the greatest of respect to Ghappour's fervently argued opinion, I would argue that the use of a Network Investigative Technique is not at all a matter of discretion being left to the 'rank and file', but an operational requirement dictated by the circumstances and necessary to satisfy the obligations and duties imposed on law enforcement by society. That discretion lies, rather, with the judicial authority approving the warrant. Whether the judiciary has sufficient skills to exercise such discretion adequately is a separate issue. I would also add that, in my experience, investigators and their managers are usually fully aware of the consequences, sensitivities and risks of the tools they use or are very quickly and robustly reminded of them. Ghappour goes on to suggest that operational approval for the use of an N.I.T. should reside with a high ranking official such as the US Attorney General.[44] This might work where such operations are few in number, but would likely create a significant bureaucratic bottleneck that would undermine progress in an investigation and would be impractical in cases of electronic evidence which are often time-sensitive.

A further important consideration is the concept of jurisdiction. I would argue that traditional notions of territoriality applied to physical evidence are increasingly irrelevant: when electronic evidence is involved and where a crime scene may well ex-

[41] *Zoetekouw* [53] p. 1.

[42] *Ghappour* [25] p. 1108.

[43] *Ghappour* [25] p. 1114.

[44] *Ghappour* [25] p. 1133.

tend across multiple political borders; where counterparts may not be part of a trust-relationship or diplomatically predisposed to cooperate; and, when evidential data may be duplicated, relocated and routinely disseminated to additional jurisdictions at the press of a button.[45] Zoetekouw carefully explores enforcement jurisdiction in cyberspace and reviews different concepts of territory. He describes a 'new contender' which establishes a legal fiction which he terms 'Putative Territory' whereby:

> As long as one does not know or cannot know how their 'position' in cyberspace translates to the real world and its according territorial jurisdiction, any action undertaken occurs and has effect in one's one territory.[46]

He goes on to discuss the possibility of treating:

> ... cyberspace as a kind of 'unregulated commons' that would be a vessel to each state's enforcement wishes.[47]

He is pessimistic as to whether such a concept could be tenable 'for a foreseeable future' given the adherence to more traditional theories of sovereignty of criminal law. And yet, without a new or another novel conceptualisation of cyberspace, any investigations encountering anonymous computer-based criminals will be left without any legitimate lines of inquiry. Even if a preliminary location for the data can be ascertained, it will most likely only be the first in a chain of false fronts. Under traditional MLA rules, pursuing such enquiries would entail multiple, consecutive diplomatic applications, considerable delay and poor prospects.

The inherent delays and bureaucracy involved are a significant factor militating against the use of traditional Mutual Legal Assistance procedures in cyber-based investigations. The processing time required for Letters of Request has been quoted as being up to two years.[48] A similar conclusion was drawn from an assessment study conducted by the Council of Europe's Cybercrime Convention Committee. Even between states parties to the Budapest Convention (who are committed by treaty to cooperation in such matters), MLA procedures were judged to be impractical.

> The mutual legal assistance [...] process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. *Many requests and thus investigations are abandoned*.[49] (CoE, 2013) (my italics)

Existing MLA mechanisms were, after all, designed and perhaps adequate for a time when malefactors and messages travelled physically across frontiers and where the

[45] Kerr and Murphy actually argue that international cooperation in these matters trumps the threat to sovereignty. 'One government's use of NITs to investigate crimes on the dark web is generally welcomed by other governments rather than feared.' *Kerr and Murphy* [30] p. 63. But I would suggest the lack of objection is more likely a case of reluctant acquiescence to a situation over which there is little control. It is also politically easier to acquiesce and to justify a lack of objection when the matters under investigation relate to universally repugnant crimes such as paedophilia.

[46] *Zoetekouw* [53] p. 10.

[47] *Zoetekouw* [53] p. 13.

[48] *Bellovin et al.* [4] p. 28 Fn10 citing Krempl.

[49] *CoE* [12].

sovereignty of a jurisdiction was reinforced and enforceable by inspection and examination at the border.

A further risk already mentioned above exists where the authorities sponsor or generate their own malware that can then 'escape into the wild' to be adapted and misused by criminals. Cellebrite, for instance, is a leading provider of smart phone forensic software and is widely believed to have helped the FBI gain access to an encrypted iPhone used by a terrorist from the San Bernardino terrorist attack. In January 2017 Cellebrite was itself hacked with the attacker retrieving 900 GB of data including software used for accessing Blackberry, Android and iPhone devices. This data was then publicly dumped on a website. The hacker gave an interview to Motherboard.vice.com explaining his or her motivation and highlighting the political risks involved both in terms of reputation and information security:

> The debate around backdoors[50] is not going to go away, rather, it's almost certainly going to get more intense as we lurch toward a more authoritarian society [...] It's important to demonstrate that when you create these tools, they will make it out.[51]

In another example, it has been claimed that the malware behind the widespread Wannacry ransomware attacks of 2017 was developed from a software tool called EternalBlue created by the US National Security Agency and 'exfiltrated' by a group of hackers known as the Shadow Brokers.[52]

Despite long-standing law enforcement use of hacking techniques, the legal framework has only recently started to catch up. As already mentioned, Rule 41 of the US Federal Rules of Search and Seizure was only amended in December 2016 to authorise the use of Network Investigative Techniques for 'remote access to search electronic storage media and to seize or copy electronically stored information where the location of the device is unknown' and 'concealed through technological means'.[53] Since most technologically astute criminals will be using some sort of anonymizing software, this amendment effectively does away with the need to specify the location of a remote search in a warrant and allows action beyond the direct jurisdiction of the issuing court. As Ghappour has suggested this amendment may well lead to, 'the largest expansion of extraterritorial enforcement jurisdiction in FBI history.'[54]

Recent changes to UK legislation in the guise of the Investigatory Powers Act 2016[55] have also formalised the law enforcement use of hacking techniques through court orders called 'Equipment Interference Warrants' which come in two basic flavours:[56]

[50] i.e. malware that allows unauthorised access to a device.

[51] This article also appears to suggest that Cellebrite may have been using software written by hackers to remove software restrictions on Apple devices to allow the installation of unapproved apps. *Cox* [17].

[52] *Fox-Brewster* [22]. See also *Goodin* [26].

[53] *Cornell Law School* [10].

[54] *Ghappour* [25] p. 1075.

[55] *Legislation.gov.uk* [32].

[56] There is a useful summary by *Big Brother Watch* [5].

- Targeted equipment interference warrants (s99(2)) are available to a wide range of intelligence and investigative bodies where the suspect or location is known. Where the application is made by law enforcement, a 'British Islands'[57] (i.e. domestic) connection is required.
- Bulk equipment interference warrants (s136) are available only to the intelligence services and are used internationally when the target or location is unknown.

An equipment interference warrant may be used to obtain:

(a) Communications [the definition of] which includes:

  – anything comprising speech, music, sounds, visual images or data of any description, and,
  – signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus (s135);

(b) Equipment data [which] means data about the system on which a communication is held and any data associated with the communication except for its 'meaning' (Sects. 100(2) and 100(3)).[58]
(c) Any other information.

There are two points of particular interest here: Firstly, that the targeted equipment interference warrants may be used for preventing as well as detecting serious crime (s106(1)(a)). This is consonant with the UK's proactive policing philosophy, but rather unusual in the international context for such an invasive measure. In effect, it appears to allow hacking to take place before an offence has been committed; and, secondly, that British intelligence services have a mandate that also includes preventing and detecting serious crime (in addition to national security responsibilities). This is not always the case in other jurisdictions and indeed may be prohibited by national constitutions.

In 2017, the European Parliament commissioned a helpful report contrasting and comparing the legal frameworks applicable to law enforcement hacking in six EU member states (France, Germany, Italy, the Netherlands, Poland, UK) and three other countries (Australia, Poland and the USA).[59] The report concluded that the case for law enforcement hacking had been established, but that the protection of the rights of the individual, although a primary concern, had received less attention. All the countries reviewed had until recently been using hacking techniques without a specific legal framework but, of the EU Member States reviewed and at the time of writing, only France, Poland, and the UK had introduced specific legislation (and then only in

[57] The term 'British Islands' is not defined in the Act. In Schedule 1 to the Interpretation Act 1978 it is defined as the United Kingdom, the Channel Islands and the Isle of Man.

[58] It would appear, therefore, to be limited to traffic and transaction data. Metadata (or data that describes other data) can often provide an understanding of the meaning of a message and it is not clear from the wording to what extent this may be captured under an interference warrant. S100(2)(c) uses the wording 'anything that might reasonably to be considered the meaning (if any) of the communication or the item of information, disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact.'

[59] *EU Parliament* [20].

2016). The other three EU countries reviewed in the report have since adopted their own specific laws. New Dutch powers permitting the covert use of remote access tools came into force in the Netherlands on 1st March 2019.[60] On 22 June 2017, Germany adopted an amendment to its criminal code allowing use of the State Trojan software mentioned above.[61] Also in June 2017, the Italian government approved an amendment to the code of criminal procedure regulating the use of hacking techniques, but these procedures have since been circumscribed by a decision of the Italian Supreme Court.[62]

Even where a dedicated legal framework is properly in place, if the relevant judicial authority does not have the skills or sufficient knowledge to be able to assess and understand the applications and technical evidence before her or him, the legal framework will prove inadequate and the quality of justice will suffer. Even where expert witnesses are tendered to assist the court, a judge must be in a position to ask the right questions in order to make an informed decision. Ghappour suggests that all too often the legal safeguards are in the hands of:

> ... a judiciary whose umpiring capabilities are limited to preserving individual rights in the domestic sphere and who lack technological expertise to spot irregularities.[63]

In other words, if those charged with policing legislative safeguards are unable to assess and review them from a position of knowledge and confidence, those safeguards are all, but meaningless. Electronic evidence is not yet a core subject in the curriculum of most judicial academies.

I began by describing the standard process of gaining entry and searching a premises. Executing a search can be unpalatable, brutal and invasive for those searched, but it is also an effective way of gathering evidence and an important weapon in the armoury of criminal justice. And yet, take away the legislation, the judicial oversight and authority, and those very same actions would be characterised as burglary. Currently, whenever law enforcement employs a hacking technique which takes effect in another, remote jurisdiction, it will most likely be breaking the law in that second country (even if it is most likely also in that country's interest for the targeted criminal to be identified and apprehended[64]). And yet, as demonstrated, law enforcement use of hacking is well established. The legal and supervisory safeguards may not yet be fully developed and, internationally, there are still significant and serious accommodations to be made. Kerr and Murphy argue pragmatically:

> When a widespread practice by states exists, either in the form of active practice or in the form of acquiescence to the practice of others, undertaken in a belief that the practice is lawful [...], then a rule forms around that practice.[65]

[60] *Govt. of the Netherlands* [27].

[61] *Deutsche Welle* [18].

[62] *Corte di Cassazione* [11]. See also *Privacy International* [39] and [40].

[63] *Ghappour* [25] p. 1114.

[64] The discussion here is related and restricted to matters of criminal investigation and not to military or intelligence attacks on cybersecurity or critical infrastructure.

[65] *Kerr and Murphy* [30] p. 67.

In other words, when confronted by a foreign law enforcement agency engaged in the unauthorised access of data stored within its jurisdiction what can that other, remote, jurisdiction do on a practical level to prevent such action? Its government might complain or retaliate (or threaten to), but these are reactive measures rather than preventive. To date, not only has the most usual response been one of acquiescence, but, indeed, of providing even more cooperation.[66]

In the final analysis law enforcement has a statutory responsibility to protect the society it serves and it cannot do so without being provided with a sufficient and adequate toolkit to investigate an increasingly technical criminal adversary for whom anonymity and the laying of false trails is a powerful defence. Society expects its communities to be protected from criminal predation and while law enforcement hacking is certainly not an ideal solution (with its attendant challenges of attribution and its disruption of international cooperation and norms of mutual legal assistance) it is effective in bringing to justice criminals who are otherwise able to reach across frontiers with 'virtual' impunity. There are no borders in virtual space. In the same way that a physical search involves intrusion into an area of life normally considered inviolable, law enforcement hacking should certainly be circumscribed by a high degree of control and evidential expectations. Although it may not be the most welcome or palatable investigative strategy, given the emerging operational environment and the need to protect society, what is the alternative?

References

1. ACLU: Challenging government hacking in criminal cases (2017). Available at https://www.aclu.org/sites/default/files/field.../malware_guide_3-30-17-v2.pdf. Accessed 9 July 2018
2. Altvater, B.J.: Combatting Crime on the Dark Web (2016). Available at http://www.ndaa.org/dyk/20161219-Dark%20Web_FINAL.pdf. Accessed 10 July 2018
3. Bell, C.: Surveillance technology and graymail in domestic criminal prosecutions. Georgetown J. Law Public Policy **16**, 537 (2018). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269915. Accessed 6 March 2019
4. Bellovin, S., et al.: Lawful hacking: using existing vulnerabilities for wiretapping on the Internet. Northwest. J. Technol. Intellect. Prop. **12**, 1 (2014)
5. Big Brother Watch: Equipment interference (14 March 2016). Available at https://bigbrotherwatch.org.uk/?s=equipment+interference. Accessed 8 July 2018
6. British Broadcasting Corporation: Snowden leaks: GCHQ 'attacked anonymous' hackers (2014). Available at https://www.bbc.co.uk/news/technology-26049448. Accessed 8 July 2018
7. Brunker, M.: Judge OKs FBI hack of Russian computers (2001). Available at https://www.zdnet.com/article/judge-oks-fbi-hack-of-russian-computers/. Accessed 4 July 2018
8. Bundtzen, S.: Why you should know about Germany's new surveillance law (2017). Available at https://www.opendemocracy.net/digitaliberties/sara-bundtzen/why-you-should-know-about-germanys-new-surveillance-law. Accessed 5 March 2018
9. Coleman, G.: Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. Verso, New York (2013)
10. Cornell Law SchoolFederal Rules of Criminal Procedure (2018). Available at https://www.law.cornell.edu/rules/frcrmp/rule_41. Accessed 8 July 2017

[66] *Kerr and Murphy* [30] p. 63.

11. Corte di Cassazione: Penale Sent. Sez. 6, Num. 45486, Anno 2018 (2018). Available at www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snpen&id=./20181009/snpen@s60@a2018@n45486@tS.clean.pdf. Accessed 18 May 2019
12. Council of Europe T-CY assessment report (T-CY(2013)17rev): The mutual legal assistance provisions of the Budapest Convention on Cybercrime Para 5.1.1. Conclusion 1 (2013). Available at http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c. Accessed 10 July 2018
13. Cox, J.: Australian dark web hacking campaign unmasked hundreds globally (2017). Available at https://motherboard.vice.com/en_us/article/4xezgg/australian-dark-web-hacking-campaign-unmasked-hundreds-globally. Accessed 5 March 2018
14. Cox, J.: In a First, Judge Throws Out Evidence Obtained from FBI Malware (2016). Available at https://motherboard.vice.com/en_us/article/gv5yqj/in-a-first-judge-throws-out-evidence-obtained-from-fbi-malware. Accessed 5 July 2018
15. Cox, J.: Second judge argues evidence from FBI mass hack should be thrown out (2016). Available at https://motherboard.vice.com/en_us/article/78kxkx/second-judge-argues-evidence-from-fbi-mass-hack-should-be-thrown-out. Accessed 5 July 2018
16. Cox, J.: The FBI hacked over 8,000 computers in 120 countries based on one warrant (2016). Available at https://motherboard.vice.com/en_us/article/53d4n8/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant. Accessed 7 March 2018
17. Cox, J.: Hacker dumps iOS cracking tools allegedly stolen from cellebrite (2017). Available at https://motherboard.vice.com/en_us/article/5355ga/hacker-dumps-ios-cracking-tools-allegedly-stolen-from-cellebrite. Accessed 3 July 2018
18. Deutsche Welle: Things to know about Germany's recent surveillance laws (2017). Available at https://www.dw.com/en/things-to-know-about-germanys-recent-surveillance-laws/a-39421060. Accessed 18 May 2019
19. DOJ: US DoJ/OLA letter to Senator Grassley (14 July 2015). Available at https://www.judiciary.senate.gov/download/justice-department-to-grassley_-dea-spyware. Accessed 10 February 2018
20. EU Parliament LIBE Committee: Legal frameworks for hacking by law enforcement: identification, evaluation and comparison of practices (2017). Available at http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2017)583137. Accessed 8 March 2018
21. Europol: Are you sharing the same IP address as a criminal? Press release (12 October 2017). Available at https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online. Accessed 28 June 2018
22. Fox-Brewster, T.: An NSA cyber weapon might be behind a massive global ransomware outbreak (2017). Available at https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#64d7f487e599. Accessed 3 July 2017
23. FBI: Playpen creator sentenced to 30 years. Press release (5 May 2017). Available at https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years. Accessed 6 July 2017
24. FBI: Going dark (2018). Available at https://www.fbi.gov/services/operational-technology/going-dark. Accessed 16 July 2018
25. Ghappour, A.: Searching places unknown: law enforcement jurisdiction on the dark web. Stanf. Law Rev. **69**, 1075 (2017)
26. Goodin, D.: NSA-leaking shadow brokers just dumped its most damaging release yet (2017). Available at https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/. Accessed 3 July 2017
27. Government of the Netherlands: new law to help fight computer crime (2019). Available at https://www.government.nl/topics/cybercrime/news/2019/02/28/new-law-to-help-fight-computer-crime. Accessed 18 May 2019
28. Greenberg, A.: Global web crackdown arrests 17, seizes hundreds of dark net domains (2014). Available at https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/. Accessed 11 July 2017
29. Justia: US Law Rule 41 Search and Seizure (2018). Available at https://law.justia.com/codes/us/2001/title18/app/federalru/dup1/rule41. Accessed 8 July 2018
30. Kerr, O.S., Murphy, S.D.: Government hacking to light the dark web: what risks to international relations and international law? 70 Stan. L. Rev. Online 58 (2017)
31. Kim, S.: Privacy international's work on hacking (2017). Available at https://medium.com/privacy-international/privacy-internationals-work-on-hacking-153a0565e1ce. Accessed 9 July 2018

32. Legislation.gov.uk: Investigatory Powers Act 2016 (2018). Available at http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted. Accessed 11 July 2018
33. Lemos, R.: FBI "hack" raises global security concerns (2002). Available at https://www.cnet.com/news/fbi-hack-raises-global-security-concerns/. Accessed 4 July 2018
34. Leyden, J.: Russians accuse FBI agent of hacking (2002). Available at https://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent/. Accessed 4 July 2018
35. Mason, J.: Are VPNs legal in your country? Thebestvpn.com (2018). Available at https://thebestvpn.com/are-vpns-legal-banned-countries/. Accessed 11 July 2018
36. Murch, R.S.: FBI files brief on Scarfo Keylogger (2001). Available at https://yro.slashdot.org/:story/01/10/10/161256/fbi-files-brief-on-scarfo-keylogger. Accessed 4 July 2018
37. Norton.com: Malware (2017). Available at https://us.norton.com/internetsecurity-malware.html. Accessed 28 June 2017
38. Oerlemans, J.: Hacking without a legal basis (2014). Available at http://leidenlawblog.nl/articles/hacking-without-a-legal-basis. Accessed 20 November 2016
39. Privacy International: Italy's Supreme Court decision limits hacking powers and applies safeguards (2 November 2018). Available at https://www.privacyinternational.org/blog/2423/italys-supreme-court-decision-limits-hacking-powers-and-applies-safeguards. Accessed 18 May 2019
40. Privacy International: Privacy International's analysis of the Italian hacking reform, under DDL Orlando (2017). Available at www.privacyinternational.org/sites/default/files/2018-01/PI_hacking_DDL%20Orlando.pdf. Accessed 18 May 2019
41. Regev, D.: WhatsApp's security breach: made in Israel. implemented worldwide (17 May 2019). Deutsche Welle. https://www.dw.com/en/whatsapps-security-breach-made-in-israel-implemented-worldwide/a-48740524
42. Rumold, M., Playpen: The story of the FBI's unprecedented and illegal hacking operation (2016). Available at https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation. Accessed 7 March 2018
43. Schroeder, S.: The Lure (2012). Course Technology, Boston
44. Steifel, K.: Bundestrojaner geknackt Wiener Zeitung (10 October 2011). Available at https://www.wienerzeitung.at/themen_channel/wz_digital/digital_news/403092_Bundestrojaner-geknackt.html. Accessed 8 July 2018
45. Times of Israel: Israel reached out to US hackers for 'Zero Days' tools (2016). Available at https://www.timesofisrael.com/israel-reached-out-to-us-hackers-for-zero-days-exploits/. Accessed 30 June 2018
46. Tor Blog: Did the FBI pay a university to attack Tor users? (11 November 2015). Available at https://blog.torproject.org/did-fbi-pay-university-attack-tor-users. Accessed 11 July 2017
47. Tor Blog: Tor security advisory: "relay early" traffic confirmation attack (30 July 2014). Available at https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack. Accessed 11 July 2017
48. UNODC: Comprehensive study on cybercrime (2013). Available at https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Accessed 6 June 2018
49. Vitaris, B.: Australian DarkWeb pedo site admin sentenced to 35 years in jail. www.deepdotweb.com (11 August 2015). Available at https://www.deepdotweb.com/2015/08/11/australian-darkweb-pedo-site-admin-sentenced-to-35-years-in-jail/ Accessed 5 March 2018
50. Vitaris, B.: Third judge rules FBI's playpen warrant invalid. www.deepdotweb.com (29 September 2016). Available at https://www.deepdotweb.com/2016/09/29/third-judge-rules-fbis-playpen-warrant-invalid/. Accessed 11 July 2016
51. Wikipedia: Hacking team (2018). Available at https://en.wikipedia.org/wiki/Hacking_Team. Accessed 11 July 2018
52. Zetter, K.: Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (2014). Crown Publishers, USA
53. Zoetekouw, M.: Ignorantia Terrae Non Excusat Conference Paper Crossing Borders: Jurisdiction in Cyberspace Conference (March 2016). Available at https://c.ymcdn.com/sites/www.iisfa.net/resource/resmgr/Slide_seminari/Convegno_Milano/c-mzoetekouw-ignorantia-terr.pdf. Accessed 12 July 2018