The European Review of Organised Crime

Original article

Dealer, Hacker, Lawyer, Spy. Modern Techniques and Legal Boundaries of Counter-cybercrime Operations

Kamil Bojarski*

Abstract: Fighting cybercrime differs from tackling conventional criminal activity in both technical and legal aspects. To execute effective operations, law enforcement has to possess significant understanding of computer technology and to follow the latest developments in the area of network security. At the same time, they are bound by criminal procedure which has to be adapted to new circumstances in order to provide effective, yet not excessively intrusive, legal instruments. Cybercrime is a global phenomenon. Cybercriminals have already transnational access to computers, software, and information. As a result, such crimes require the attention of national authorities. This article analyses the main challenges encountered by law enforcement and the involvement of Signal Intelligence (SIGINT) agencies when it comes to countering cybercrime operations.

Keywords: Cybercrime – Remote search – Targeted surveillance – SilkRoad – Encryption – Key disclosure law

*Kamil Bojarski is a LLM candidate at Nicolaus Copernicus University, Torun, Poland. He is president of the Student Scientific Group of ICT Law at Nicolaus Copernicus University and author of blog dedicated to legal aspects of network security lawsec.net.
Email: kamilbojarski7@gmail.com

The European Review of Organised Crime 2(2), 2015, 25-50
ISSN: 2312-1653

Introduction

The effective fight against cybercrime requires knowledge of cutting-edge technology from both law enforcement and the judiciary. Due to the availability of network security training materials, encryption solutions, and penetration testing tools, criminals often outmatch law enforcement in terms of expertise and tools used. The critical value of these factors in tracking down cybercriminals has converted the fight against cybercrime into an arms race between criminals and law enforcement. Through the means of Signal Intelligence (SIGINT) and other sophisticated techniques employed against cybercrime, government agencies still maintain a lead in the battle against cybercrime. However, this level of technological advantage is not always nor readily available to local or regional law enforcement. This is because operations executed by powerful intelligence agencies such as the US National Security Agency (NSA) or the UK Government Communications Headquarters (GCHQ) are often too intrusive to be used in the criminal justice system. Just as military forces are not deployed to fight criminal groups, intrusive surveillance and advanced persistent threats are not suitable means of law enforcement. Ultimately, on the level of ordinary law enforcement both sides, criminals and law enforcement, are almost equally capable (Gercke, 2012).

The aim of this article is to analyse how counter cybercrime operations are executed and identify major technical and legal challenges involved, as well as predict possible future trends. Based on documents leaked by whistleblowers such as Edward Snowden, it is also possible to assess capabilities of the SIGINT agencies and their application. The article concentrates on operations where law enforcement has to engage in active surveillance and access computer systems using the same or similar methods to those used by criminals.

Analyses of techniques used, legal instruments and their relationship to procedural guarantees will be based on examples of counter cybercrime operations followed by a discussion on technical and legal challenges encountered by law enforcement. Technical discussions will involve an analysis of methods in terms of their technical complexity and a spectrum of criminal activities to which they might be applied. Legal discussions compare and analyse legal instruments related to electronic means of investigation included in criminal procedure in Europe and the US. As those instruments are constantly adapted to new circumstances, the discussion here concentrates on the actual application rather than a theoretical analysis. The discussion on signal intelligence operations is based on documents released by Edward Snowden that contained a description of technical and operational properties of tools used by intelligence services.

Accordingly, the article is divided into four parts. First, it presents a case study of law enforcement operations against an underground drug market "SilkRoad". This serves as a basis for further discussion. Second, it analyses the technical obstacles faced by law enforcement in this case. Third, it concentrates on the legal boundaries and instruments used to overcome technical challenges. Lastly, it looks at understanding the involvement of intelligence agencies and their technological advantage on the scale of counter cybercrime operations.

Dealer: The SilkRoad Case Study

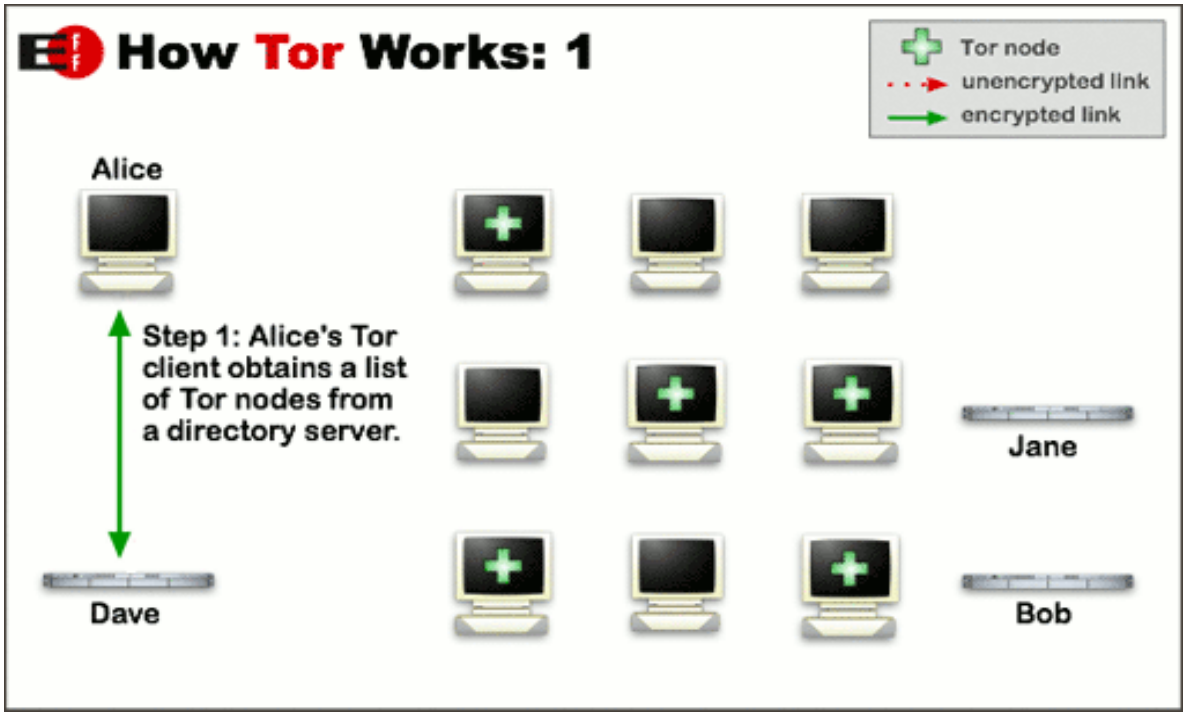
Background

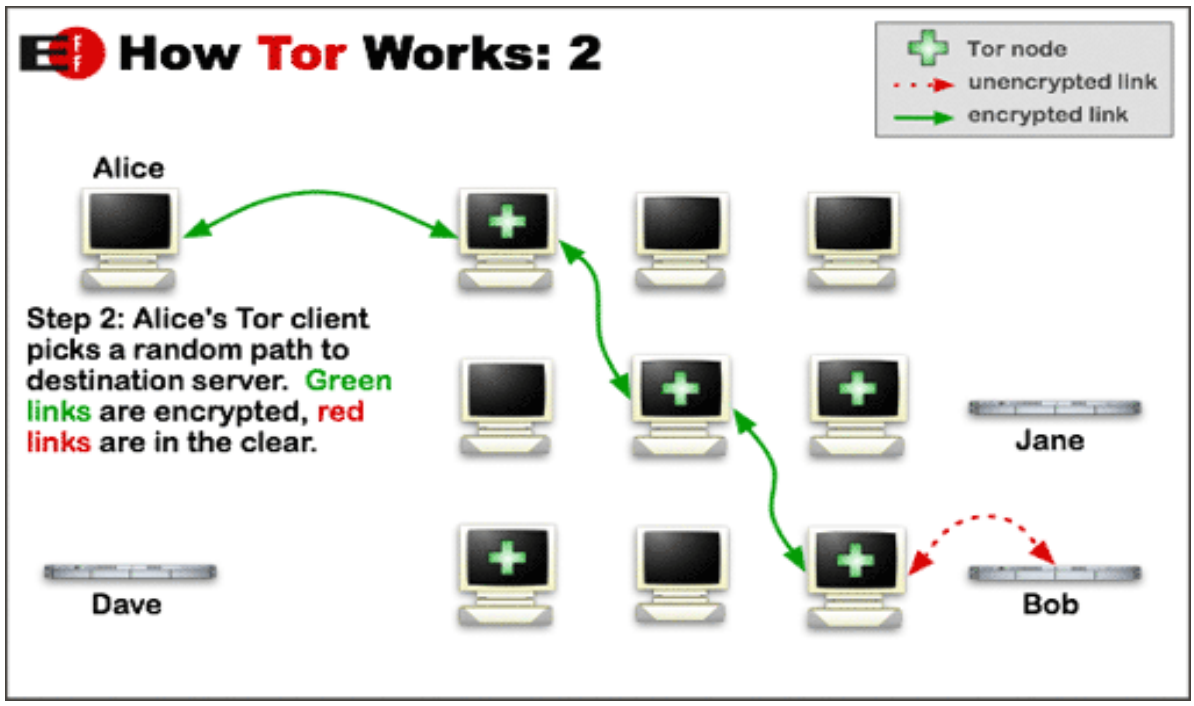
Launched in February 2011 and shut down in October 2013, SilkRoad became a flagship Tor drug marketplace. Its administrator, Ross Ulbricht, also known as Dread Pirate Roberts, was charged with drug trafficking conspiracy, computer hacking conspiracy, and money laundering conspiracy (United States of America v. Ross Ulbricht, Sealed Complaint, 13 MAG 2328). Ultimately, in January 2015, Ulbicht was convicted on all charges laid in relation to SilkRoad. Due to substantial evidence gathered during investigation, which includes Ulbricht's personal journal describing details of his criminal activity, the chance of a successful appeal or retrial is low (Greenberg, 2015; McCoy, 2015). The case of Ross Ulbricht is an example of how tracking down criminals who use modern encryption solutions relies on performing technically complex operations combined with exploiting negligent behaviour of perpetrators. The SilkRoad service looked and worked like an ordinary e-commerce platform. Users had to make individual accounts in order to enter buy or sell products. Offers were catalogued into categories and users were able to comment on the quality of service after each transaction. Also an escrow service was available in order to ensure safety of transactions and prevent frauds (Christin, 2012). Furthermore, Silk Road administration provided guidelines on how to ensure the safety of transactions. Guidelines also covered technological aspects with instructions relating to the usage of Tor browser, cryptography, and system configuration (United States of America v. Ross Ulbricht, Sealed Complaint, 13 MAG 2328). Customer service, similar to those used by legitimate e-commerce platforms, was also implemented to deal with technical problems.

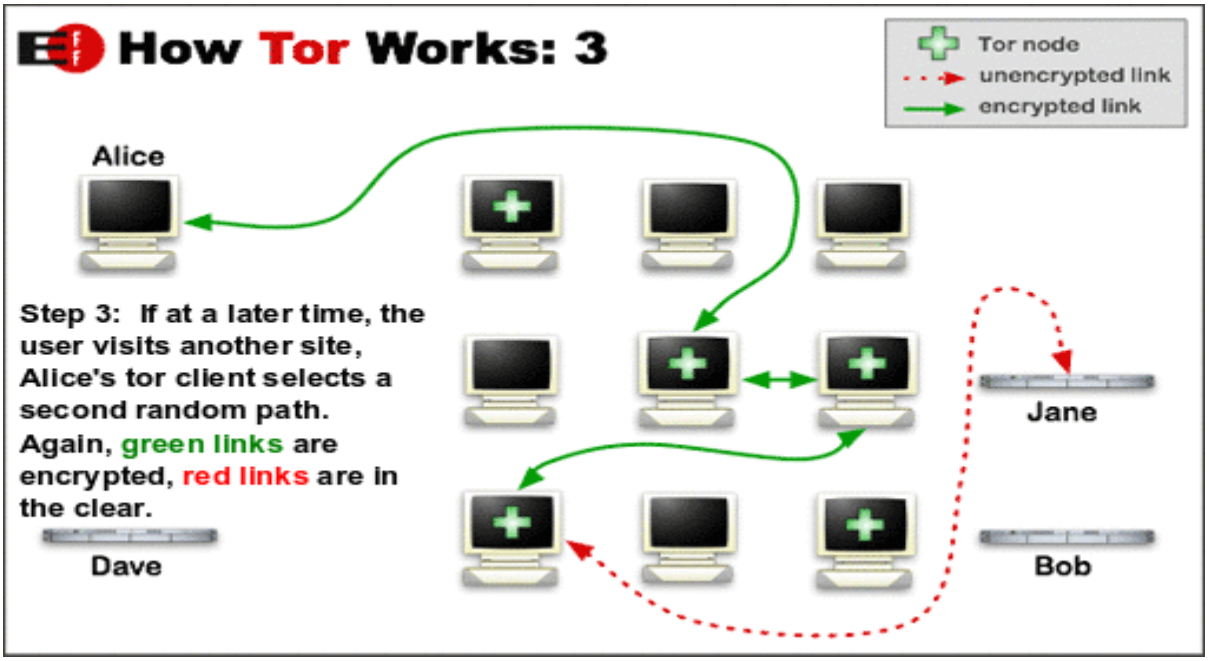
Technical Setup

Two major safeguards secured SilkRoad's servers location and the identity of its owner. First, the use of the Tor network—SilkRoad was available only as a hidden service. Tor is a software which enables obscuring Internet Protocol (IP) addresses of its users by utilising so-called "onion routing". Traffic in Tor network is sent through a number of relays voluntarily hosted by users around the world. Relays are computers used to transmit data to its destination. The term onion refers to layers of

encryption used—data, including IP address, is encrypted and send through a circuit of relays, each of them adding another layer of encryption (Dingledine et al., 2004). The point is that each relay decrypts only the data required to establish another circuit (or to reach the destination, in case of final relay). As a result, an individual relay does not know about the origin of traffic and as a result, traffic cannot be traced back to the original user. Overview of Tor network is presented on following illustrations (Tor Project, 2014):







Hidden service functions similarly to a website. It is a server configured to receive inbound traffic only from within the Tor network. Addresses of the hidden services always end with an "onion" domain name. Such addresses are recognised by clients of the Tor network, which reroute them to or from specific hidden service (Dingledine et al., 2004). Tor, when used properly is extremely effective method of hiding IP address, up to the point where users who use it strictly to browse websites, with any additional content such as JavaScript elements disabled, are effectively immune to identification.

The second safeguard was limiting payment to only one method: a Bitcoin based payment system. Bitcoin is decentralised form of electronic currency, existing only as digital data with information about transactions available to all users through public block chain. Bitcoins themselves are essentially proofs that certain mathematical calculations have been completed by a particular computer and by using this mechanism it is possible to control the number of Bitcoins in circulations as new coins are generated only after set number calculations has been completed (Grinberg, 2011). To start using Bitcoins the user has to generate his own digital wallet, which is essentially a pair of keys for public key cryptography. As wallets are simply strings of characters, they may be stored in text files or even written down on paper. In terms of transaction authorisation, public key is used as account number and enables other users to transfer funds into specific wallet, while private key is used to sign transactions, enabling the owner to spend their own Bitcoins. Users obtain currency by "mining" (thus contributing processing power of client's computer to maintenance of transaction system) or they can buy it through exchange services. Currently no state recognises Bitcoins as a currency, however in most countries they can be used as payment on basis of individual contractual

agreements[1]. All transactions are recorded in "block chain", which is a public ledger of all transactions made. Users of the network maintain block chain in the form of a distributed database (whose maintenance is possible due to processing power donated by users in the aforementioned process of mining). The distributed and public nature of block chain functions as a safeguard against frauds and malicious manipulation of transactions. In case of SilkRoad users had to make an online wallet stored on SilkRoad's server (Christin, 2012). Users send funds to the online wallet, and purchase goods using these funds. After making a purchase, the buyer's funds were transferred to an escrow wallet and released after the transaction had been completed. SilkRoad tried to obscure transaction records by using a so-called "tumbler"—i.e., an algorithm that sends actual payment through series of dummy transactions (United States of America v. Ross Ulbricht, Sealed Complaint, 13 MAG 2328).

Investigation and Operational Techniques

Apprehending Ulbricht required using both digital and traditional methods of information gathering. In terms of non-technical leads, Ulbricht's most serious mistake was mixing his public and criminal persona. Given that he certainly knew SilkRoad was under investigation, one would assume that he was aware of how vital it is to separate information posted on the internet publicly from data that could identify him as Dread Pirate Roberts. In spite of this, he used the nickname "altoid", which was linked to email address "rossulbricht@gmail.com", to promote SilkRoad on public forums dedicated to the drug trade. Furthermore, he once again used his real credentials when he asked for help on IT forum stackexchange.com (United States of America v. Ross Ulbricht, Sealed Complaint, 13 MAG 2328). While the request seemed benign, its specificity later enabled linking him to SilkRoad. Ulbricht had asked for a particular technical solution, which was later found to be implemented on the seized SilkRoad servers. The most important piece of evidence, however, was a package seized by US border control. US Customs and Border Protection during routine control intercepted a package from Canada addressed to Ulbrich, which contained dozen of fake id documents including driver's licences, passports, and ID cards. Ultimately, this led law enforcement to Ulbricht's location, and as a result, seizure of the servers responsible for controlling SilkRoad.

For the purpose of this article, it is more important to examine the digital evidence obtained and the electronic methods of investigation. The first group of evidence relates to the data captured on seized servers. Forensic analysis revealed that Secure Shell (SSH) keys used to access them were signed frosty@frosty (the same nickname Ulbricht used on stackexchange.com forum). In addition servers

---

[1] Bitcoin is not regulated in any way in most countries, it is however outright banned in some e.g. Bangladesh, Bolivia, Russia, Thailand.

were configured to accept connections only from specific IP address of a Virtual Private Network (VPN) server. Ulbricht regularly erased access logs tied to his VPN, but some of them were recovered which in turn revealed that it was accessed from internet café where Ulbricht also logged into his gmail account. These methods of investigation and evidence gathering, which were revealed when a criminal complaint became public, caused little controversy. In fact, they can be seen as a natural evolution of criminal procedure in the era of information. Before mainstream use of computer networks, search warrants authorised physical search of property, today search warrants have been expanded to authorise law enforcement to seize digital data. In the United States, Federal Rules of Criminal Procedure states that a warrant issued for search or seizure of evidence, contraband or property intended for committing a crime authorises seizure of electronic storage media or the seizure or copying of electronically stored information (Federal Rules of Criminal Procedure, Rule 41 (e)(2)(b)). In the case of SilkRoad, servers contained both evidence of crime, and contraband in form of Bitcoins. Precedents for obtaining warrants in modern cases are increasingly linked to the correlation between digital evidence and criminal activity. Modern cases have increasingly used these digital links. In United States v. Terry, 522 F.3d 645, 650 n. 2 (6th Cir.2008), probable cause was established by demonstrating that email account was used to send child pornography, while in United States v. Adjani, 452 F.3d 1140 (9th Cir. 2006) the fact that criminal extortion was conducted by physical mail did not matter, as circumstances established that there is fair probability that evidence of crime will be found in computer. This resulted in a warrant being issued (Jarrett et al., 2009). While it appears that SilkRoad's servers were seized in compliance with procedural guarantees, explanation of how the FBI tracked down its physical location stirred controversy regarding legality of procedures used.

Legality of Obtained Evidence

In September 2014, the US government released a declaration by Christopher Tarbell, an FBI computer forensic investigator who tracked down the IP address of SilkRoad servers. Tarbell explained that Tor software is not an omnipotent tool, but is effective only when configured properly and used with compatible external applications. This is not unknown and in fact, Tor developers specifically warn about users about this[2]. However, the explanation of techniques employed that followed this statement raised two major questions: were the methods of investigation in compliance with criminal procedure, and is the explanation provided probable from technical point of view.

To answer the first question, it is necessary to present facts from the FBI report

[2] See answer to "So I'm totally anonymous if I use Tor?" question in Tor Project's FAQ, available at: https://www.torproject.org/docs/faq.html.en#AmITotallyAnonymous

that raise suspicion about the lawfulness of procedure. Tarbell claims that his team operated by interacting with the SilkRoad login page, which contained three prompts: login, password and CAPTCHA (United States of America v. Ross Ulbricht, Declaration of Christopher Tarbell, S1 14 Cr. 68 (KBF)). CAPTCHA is a method of verifying if a user is really a human as opposed to computer algorithm which could automatically login into the page, for example to distribute spam messages. Most commonly, CAPTCHA is composed of pictures with words or numbers presented in a partially obscured way and a prompt for user input. While content of the picture is easily readable for human, it is almost impossible for a computer to translate it into separate characters and provide the correct answer. On SilkRoad, it served exactly the same purpose as it does on normal websites. In the report, Christopher Tarbell says that agents were interacting with user login interface, which was fully accessible to the public, by typing in miscellaneous entries into the username, password, and CAPTCHA fields. As a result, the website would send data back to the computer: either a successful login redirect into SilkRoad main page or an error message after an unsuccessful login. Additionally packets exchange between agents' computers and servers were analysed. Packets can be considered as small packs of information exchanged between computers in network containing data to be presented, data request from one machine to another and vice versa. Up to this point, explanation provided by the FBI was reasonable. However, agents claim that packets contained IP address not associated with any node of Tor network, which should not be possible given how a Tor network works (Cubrilovic, 2014). Furthermore, allegedly accessing this particular address with a normal internet browser led to the SilkRoad login page. This, according to investigators, confirmed that servers were not configured properly and were leaking true IP address.

Such an explanation does not seem probable as technical documentation and configuration files found on the seized server confirms that the login page, with CAPTCHA fields included, were hosted on the same server as the rest of the page (Krebs, 2014). The IP mentioned belongs to the front-end server, which was set to be accessible only through Tor. The packet analysis part of the story is also questionable. If the investigators were using Tor to access the networks (and they had to in order to connect to SilkRoad), all the packets they received would come through the Tor, not directly from client to server. Furthermore released traffic logs of SilkRoad servers suggested that investigators directly accessed MyAdmin page without any IP leaks. Further analysis of the statement "simply interacting with website [...] by typing miscellaneous entries" reveals additional ambiguity and questionable technique. It is unlikely that what agents meant is synonymous to how normal user interacts with login pages. This would mean that server was leaking IP address with every login request, which is extremely unlikely and is extremely unlikely to have remained unnoticed by SilkRoad's administration (Greenberg, 2014). What is much more probable is that investigators were engaging in hacking techniques such as fuzzing and perhaps even SQL injection (Cubrilovic, 2014). Both

of these methods certainly go beyond standard user-webpage interaction as they aim to cause execution of unauthorised commands by target servers. In fact, using any of them on legitimate websites would be a crime under Computer Fraud and Abuse Act (18 U.S. Code § 1030). Furthermore, as the FBI essentially conducted a search of digital storage, and the servers were located overseas, a transnational warrant was required to perform such actions. These facts were revealed when Ulbricht's lawyers issued a memorandum arguing that evidence obtained in this way was inadmissible, as the FBI had violated the fourth amendment of the US constitution (United States of America v. Ross Ulbricht, Memorandum of law in support of defendant Ross Ulbricht's pre-trial motions to suppress evidence, order production of discovery, for a bill of particulars, and to strike surpluage, 14 Cr 68). The government on the other hand, argued that searching property used for criminal activity overseas was within the boundaries of the Fourth Amendment. The judge eventually rejected the memorandum on procedural grounds. In order to gain Fourth Amendment protection Ulbricht should have claimed personal privacy interest by submitting a sworn statement, which could not be later used against him during the trial (United States of America v. Ross Ulbricht, Opinion & Order, 14 Cr.68 (KBF)). From a legal point of view therefore, the status of the FBI's operation will remain unknown until similar precedence will occur again.

This case provides a valuable source of information about modern investigations aimed at technologically advanced organised crime groups. It is also the first case of an investigation against Tor service operators that resulted in a criminal trial. Insights into investigation techniques were possible because SilkRoad was a passive entity. As opposed to crimes like hacking, its activity did not produce evidence outside of the service's infrastructure. On the other hand, law enforcement agencies had to engage in network exploitation in order to track down Ross Ulbricht.

Hacker: Technical Challenges of Tracking down Criminals and Obtaining Cybercrime Evidence

Proliferation of Strong Cryptography and Its Effect on Criminal Investigation

The investigation of SilkRoad demonstrated several technical challenges in countering cybercrime. Particularly, the problem of unbreakable encryption solutions became apparent. In this context, encryption has two major applications: hiding IP addresses and protecting data. As it will be explained more in detail below, properly encrypting incriminating materials can completely prevent law enforcement from obtaining evidence. First, the breaking of certain encryption solutions is currently mathematically impossible. A good example of this is provided by the encryption algorithm Advanced Encryption Standard (AES), which in 2001 was officially recognised by the National Institute of Standards and Technology (NIST, 2001) and, since then, is officially used by various government agencies including the

NSA and US Department of Defence. Because of the design of the algorithm, currently there are no known effective attacks against AES. Bruteforce attack (that is, testing every possible encryption key) is completely impractical: AES-256 involves key of 256 bits resulting in 2^{256} combinations (string of 256 units of information, each can have value of 1 or 0). Given that the actual key is at an unknown position we can assume that only half of the combinations need to be tested (for a total of 2^{255} combinations). At two quintillions keys per second, it would take $9.18 * 10^{50}$ years to break encryption (for reference the current estimated age of the universe is $1.4*10^{10}$ years)[3]. In 2010, for instance, the FBI was asked by Brasilian National Institute of Criminology to decrypt hard drives obtained as part of a money laundering investigation. After twelve months, the FBI returned disks and admitted that they were not able to crack encryption (Techworld, 2010). Furthermore, given the strategic importance of unbreakable encryption, AES would be scrapped and replaced by better algorithms if a vulnerability was found. Moreover, it should be kept in mind that it is desirable for certain encryption to be unbreakable, considering its role in protecting civil liberties. Government institutions, human rights activists, as well as journalists and lawyers use AES to protect data of critical importance.

As a brute force attack is impossible, often the only way to decrypt data is by obtaining the password from the user. Regardless of legal challenges, which will be discussed in next section, the gathering of evidence is not straightforward even when the password in known. This is due to the "hidden volume" feature offered by various encryption programs. When this option is used, encryption software creates two volumes: an outer "public" volume and hidden volume within it. If a user is forced to decrypt data, they may provide the password for the outer volume, while the hidden volume would remain encrypted. This is concept known as deniable encryption (Canetti et al., 2006). Plausible real world scenarios could even involve criminal purposefully placing incriminating materials in the outer volume, leading law enforcement to believe that sufficient evidence has been obtained. Meanwhile evidence for heavier penalised crimes would remain safe in the hidden volume—for instance, files that demonstrate copyright violation could exist on the outer volume and child pornography in the hidden volume.

Properly implemented encryption causes data to be indistinguishable from random strings of bytes, therefore proving existence of hidden volume is not impossible. Some implementations include also option of a "nuke" password, which deletes the header of the volume, effectively making decryption entirely impossible[4]. This method however has limited use against law enforcement, as any forensic analysis should be performed on a copy, not the original data (Council of Europe, 2012).

---

[3] Formula is: $2^{255} / (2*10^{18} * 60 *60 *24 *365) = 9.18 * 10^{50}$

[4] For example, penetration testing oriented Linux distribution Kali offers this feature. Description available at: https://www.kali.org/how-to/emergency-self-destruction-luks-kali/.

Regarding the possibility of obtaining the key without cooperation of the suspect, the only effective angle of attack available to law enforcement is a cold boot attack (Halderman et al., 2010). In case of full disk encryption, a key has to be stored in RAM (Random Access Memory) when a computer is in use. Due to technical properties of RAM modules, when power is cut, content of the memory blocks do not disappear instantly but gradually degrade. If the computer of a criminal is captured while it is operating, or shortly after its shutdown it might be possible to capture keys stored in RAM. Commonly used procedure is cooling memory modules with compressed air (which prolongs time available), installing them in an earlier prepared machine and booting the operating system prepared for dumping memory instantly after boot. While this method requires physical access to machine and high level of expertise from the investigator, it is often the only way to secure evidence from encrypted drives.

Given that quantum cryptography is still at early stage of development, it is hard to extrapolate how it will influence the discussed problem. The main issue is that while current encryption solutions rely on mathematical algorithms (that is, certain calculations which can be performed by any computer) while quantum cryptography requires dedicated hardware. Therefore, until such devices will not be available for ordinary users, the importance of this method is marginal, especially given how effective contemporary solutions such as AES are. Theoretically, quantum key distribution could enable exchange of cryptography keys immune to eavesdropping. An example of such a mechanism is the protocol BB84 developed by Charles H. Bennett and Gilles Brassard (Benett and Brassard, 1984). This protocol relies on using photon polarisation to transmit information. According to no-cloning theorem of quantum mechanics, the state of certain particles cannot be measured accurately without disturbing the original state. Therefore, a potential attacker would both gain incorrect information and prevent successful communication between author and recipient of original message. As noted however, implementation of such methods are still relatively rare. On the cryptanalysis side, using quantum computing it might be possible to break encryption algorithms based on prime numbers such as the RSA. For example, Shor's algorithm, developed by mathematician Peter Shor is a theoretical algorithm to be run on quantum computer that would find prime factors of any given integer (Shor, 1997) rendering some algorithms obsolete. However, while there are some real world applications of quantum key distribution, current quantum computers are not able to have meaningful role in cryptoanalysis (McMillan, 2014). The bottom line is that currently there is no incentive to use quantum cryptography, as available mathematical encryption solutions are effectively unbreakable and much more portable.

Law Enforcement Attempts of User Deanonymisation

Currently, in terms of strength, Tor falls into the same category as AES. There are attempts and theoretical scenarios of massive deanonymisation of users; however, none of them can be applied in practical terms. Sophisticated and aggressive attempts will be discussed in the section on involvement of SIGINT agencies. To track down users of Tor, law enforcement still has to rely on mistakes made by criminals, or bypassing need for attacking Tor by targeting its external components. The FBI's operation "Magneto" might be considered as an indirect success in breaking Tor. In August, 2013, law enforcement managed to track down the owner of popular Tor hosting service, Freedom Hosting, as well as members of various child pornography links. The FBI tracked down these perpetrators by embedding malicious JavaScript script on hidden services seized (Poulsen, 2013). This technique turned out to be successful, but as it relied on lack of adequate use of software by perpetrators, it was not successful attack against Tor per se, but rather the users. The exploit deployed worked only on outdated Firefox browser and required JavaScript to be enabled for execution. As a result, "Magneto" was effective only against less advanced Tor users—probably consumers and distributors of child pornography with minimal technical knowledge, who used Tor due to its easy installation and popularity. Furthermore, the attack would be unsuccessful even if criminals took minimal attention to their anonymity and regularly updated Tor bundle. Considering those factors, apprehending drug vendors who possess the expertise needed to set up and administrate hidden services is unlikely using this method. A similar operation was conducted also in 2012, under codename "Torpedo". FBI used a Metasploit exploit framework to deploy malware to child pornography sites in order to identify its users (Poulsen, 2014a).

In those examples, the problem of the indiscriminate nature of such attack becomes apparent. Malware infected every computer accessing the site, whether warrant for such blanket surveillance violates the fourth amendment is a question that will have to be answered by US judiciary[5]. If a more sophisticated vector of attack is required, governments may use zero-day exploits provided by commercial vendors. Companies like Vupen provide high-grade vulnerabilities for government agencies, security companies and security departments of corporations[6]. The term "zero-day exploit" describes a vulnerability in software found by a security researcher, but not disclosed to the software vendors. Therefore, the first offensive use of such exploits is always successful because it is impossible for the vendor to address and patch the vulnerability. At the same time, after such a vulnerability is used, it is no longer "zero-day" as developers can now learn about the issue and fix it.

---

5 Proceedings related to outcome of operation "Torpedo" are ongoing at the moment of writing this article.

6 Examples of such cooperation were revealed during Wikileaks spyfiles release of documents, i.e. https://wikileaks.org/spyfiles/files/0/279_VUPEN-THREAD-EXPLOITS.pdf.

Using them, however, is not beneficial for safety of ordinary internet users. Zero-day exploits usually have a limited time span, as it is a matter of time before software vendor, or worse, ordinary cyber-criminals will discover them. Unfortunately, as a result vulnerabilities that help law enforcement track down criminals, make common users more susceptible to cyber-attacks.

Taking into account the safety of ordinary users, a more responsible course of action would be to disclose vulnerabilities, instead of stockpiling them for offensive use. Engaging in hacking by law enforcement is tied to the issue of remote search. Accessing computers used by criminals is now included in official procedures of law enforcement agencies (Reich, 2012). Given the number of vulnerabilities that are made public every day, it is reasonable to assume that utilising common hacking techniques is sufficient to gain access to most of the computers connected to the internet, especially taking into account resources available to law enforcement in terms of time and tools available.

Role of Bitcoin in Obfuscating Flow of Funds

The use of Bitcoin facilitated illegal online trade by enabling the bypassing of conventional means of payment and as a result, scrutiny of banking institutions. Effectiveness of Bitcoin as a means of hiding one's identity is co-dependent on using external anonymisation tools. As block chain might be used to associate IP address with particular transactions (Kaminsky, 2011), if a user transfers funds using an exposed machine, identification of the physical location can be easily achieved. To avoid surveillance of specific wallets, criminals obfuscate transactions by creating new wallets, combining old addresses into new accounts or using laundering services, like SilkRoad's "tumbler" (FBI, 2012). A FBI report mentions also that current software available makes those techniques easy to apply for even less technically skilled users.

Legal Challenges and Possible Future Trends of Countering Cybercrime

Every presented technical issue correlates with the problem of including in criminal procedure means for law enforcement to conduct effective investigations. However, as technologies described are used not only by criminals, but also by legitimate users, a balance has to be struck between intrusiveness of methods allowed and the right to privacy.

Right against Self-incrimination in Terms of Encryption of Data

As mentioned before, in the case of unbreakable encryptions, often the only way of decrypting data is obtaining key from the suspect. The spectrum of possible legal solutions to situation where the suspect is not cooperating lies between two

approaches: either that forcing suspect to provide encryption key is unacceptable violation of right against self-incrimination or that pragmatism requires limitation of this right. Laws providing the right to remain silent or against providing self-incriminating evidence are the foundation of a fair trial (Sottiaux, 2008). They are often included in legal acts that codify basic rights, such as the Fifth Amendment of the US constitution and Article 6 of European Convention on Human Rights (ECHR). Therefore, it appears that particularly grave justification is required for limiting those rights. Laws that require individuals to provide cryptographic key are known as key disclosure law or mandatory disclosure law. While the problem of mass use of unbreakable encryption is still relatively new and laws tend not to be yet clarified, specific provisions are included in many legal systems. The most prominent example is Regulation of Investigatory Powers Act 2000 enacted in United Kingdom. Under its provisions a judge may issue notice imposing the requirement of providing an encryption key or providing data in intelligible form. Failure to comply with notice is punishable with a fine or even imprisonment. This act was criticised on both human rights and practical grounds. Experts predict that businesses involved in criminal activity, and possessing incriminating encrypted materials, will simply move out of the UK (Pollack, 2006). A similar law also exists in France (Loi no 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne) and Finland (Pakkokeinolaki, 30.4.1987/450). The latter, however, exempts the suspect from the obligation. On the contrary, in Poland, a suspect can be compelled to provide blood or DNA samples, but at the same time has the absolute right to remain silent and may refuse to answer any question, which extends to potential knowledge of cryptography keys (Kodeks Postępowania Karnego Dz.U. 1997 nr 89 poz. 555).

In the Council of Europe countries, compliance of key disclosure laws with ECHR has to be considered as well. Regarding relation of RIPA provisions to the ECHR, Lord Bassam of Brighton brought up the case of Saunders v. United Kingdom (ECtHR application no. 19187/91), where the European Court of Human Rights (ECtHR) stated that obtaining data that exists independently of the will of the suspect by use of compulsory power falls outside of protection of the Article 6[7]. This is however, a narrow interpretation of the Court's jurisprudence. In Saunders, examples of evidence, which can be obtained by compulsory power, were: documents seized, DNA, blood and urine samples. None of which require cooperation, but rather passiveness of suspect, which does not actively aid law enforcement. This seems to be in line with provisions similar to those enacted in Poland rather than blanket approval of use of compulsion. Furthermore, the ECtHR in Perez v. France (ECtHR application no. 47287/99) explicitly warned against interpreting Article 6 restrictively due to its immense importance. Actual status of compliance of RIPA as

[7] Full statement is available at: http://www.theyworkforyou.com/lords/?id=2000-06-28a.952.1#g971.0

well as other key disclosure laws with ECHR is yet unknown, as no application has been made to the Court in that regard.

The US takes a rather case-by-case approach to the problem. Generally the Fifth Amendment does provide a right to not disclose encryption keys, as ruled by Court of Appeals of Eleventh Circuit in United States v. Doe (In re: Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 2012). However, in cases where content of a storage device is already known courts rejected granting protection of the Fifth Amendment (In Re Boucher, 2007 WL 4246473 (Nov. 29, 2009).

Table 1: Examples of Key Disclosure Laws

Legal system	Mandatory disclosure of cryptography keys
France	Yes, court or prosecutor order required.
Finland	Yes, court order required. Suspect is exempted from the requirement.
Poland	No, suspect has absolute right to remain silent.
United Kingdom	Yes, court order is required.
United States	Generally no, case-by-case analysis.
European Convention on Human Rights	No relevant case law yet.

Any legal instrument, regardless of how strict it would be, however, will never solve the problem of unbreakable encryption. Ultimately, it is impossible to prove that the suspect knows password at all, as it is easy to imagine that the suspect may simply forget a long encryption key. Furthermore if a criminal were to use hidden volume, existence of any additional data, beyond that revealed in the outer volume, is also impossible to prove. Therefore imposing any further disclosure notices would be impossible, as there can be no reasonable grounds to believe that there is anything more to be disclosed. Finally, such laws have limited practical use – penalties for crimes like the possession of child pornography or money laundering are significantly harsher than penalties for not disclosing the key. Criminals therefore, have little incentive to decrypt data anyway.

Legality of Remote Searches in Terms of Procedural Guarantees and Transnational Investigations

The case of SilkRoad also highlights the problem of remote searches in terms of techniques used and transnational authority of warrants. As mentioned in the earlier case study, it seems natural that limiting the scope of search warrant to physical seizure and analysis of storage devices would be extremely constraining to law enforcement. Enabling government hackers to gain remote access to machines, facilitates investigation on many levels: it saves time, bypasses the requirement of

physically finding storage, and enables instantaneous reaction, which is especially important when a transfer of funds can be done within seconds.

In terms of operational techniques, modern legislation provides adequate means for engaging in remote search. Provisions do not specify particular methods of accessing targeted machines, providing law enforcement freedom to use the best technology available. An example of such approach is Polish law. Act on Police specifies that after obtaining judicial warrant to engage in operational control (targeted surveillance), law enforcement is authorised to use "any technical means enabling clandestine gathering and storage of information and evidence, especially content of phone calls and other information transmitted using telecommunication networks" (Ustawa o Policji, Dz.U. 1990 nr 30 poz. 179). Similarly, law in Canada and France extends search warrants to all data stored digitally within the area of search (Lach, 2011). In the US procedure varies between states, however generally remote searches have to satisfy standard of protection guaranteed by fourth amendment (Feikert and Doyle, 2006; Brenner, 2012). Federal law requires search warrants comply with constitutional requirements as well. Belgian criminal procedure allows extending the search of a computer, to the computer network situated beyond the area of original search warrant, if it is necessary to preserve evidence and no other means are available (Lach, 2011). In case of computer networks located out of Belgium, the Minister of Justice informs targeted country about actions taken.

The last point touches on a subject especially important and delicate in terms of remote search: transnational regulations. Given how global the phenomenon of cybercrime is, an effective remedy seems almost impossible without authorising law enforcement to pursue perpetrators beyond the border of given state. On the other hand, there are serious issues related to safeguarding privacy and abuse of power if law enforcement would be given blanket authority to engage any computer network in the world after a warrant has been issued. Furthermore, due to differences in criminal procedural code, it might constitute an offence (Pradillo, 2011). Controversy was caused by the US Department of Justice, which declared need for expanding authority of judges to authorise remote searches on property outside of US jurisdiction. American Civil Liberties Union opposed the idea, stating that there are virtually no safeguards against spread of malware deployed globally by law enforcement (ACLU, 2014). However, even now warrants authorising engagement in hacking of foreign computers are not unheard of. In 2013, federal magistrate in Denver approved installing surveillance software on the computer of a terrorist "Mo" who operated out of Iran (Timberg and Nakashima, 2013). On the other hand, some judges decided that issuing such a warrant would breach federal law, which enables judges to authorise searches only within their own district. The District Court for Southern District of Texas has even refused to authorise remote operation, which would lead to learning about a suspects location, as the court claims they cannot sufficiently guarantee that procedural obligation has been satisfied (United

States District Court, S.D Texas, Houston Division, Case No. H-13-234M, April 22, 2013).

In Europe, generally, law enforcement does not have the authority to engage in remote investigation of computers situated beyond borders of its own country (Council of Europe, 2009). The Budapest Convention on Cybercrime, on the other hand contains number of provisions, which aim to facilitate the process of transnational investigation. Article 32 specifies that a Party may request another Party to conduct remote search and seizure of computer networks situated on its territory if there are grounds to believe that relevant data is vulnerable to loss or modification. Furthermore, if data is publicly available or voluntary consent has been obtained, authorisation of Party-host of data is not required. In Europe's case, however, a much more promising development is the involvement of specialised task forces and international units, especially in the light of formation of European Cybercrime Centre. One evident example of how effective can be this kind of cooperation is Operation Onymous, an international investigation involving US and European agencies that resulted in 27 hidden services, and 400 domains being taken down (Europol, 2014) as well as arrest of Blake Benthall, the administrator of SilkRoad 2.0 (United States of America v. Blake Benthall, Sealed Complaint, 14 MAG 2427). Joint task forces are considerably less constrained by differences in legislation (Council of Europe, 2008), as each unit can collect evidence in a way that will be admissible in specific national court. Furthermore, cooperation of multinational units enables the simultaneous engagement of criminals in different geographical locations. This is especially important, given that information about the seizure of a single service may reach other criminals instantaneously.

Table 2: Examples of Legal Status of Remote Search

Legal system	**Status of remote search**
Belgium	Search warrant may extend to computer network situated beyond designated area of search if it is necessary to preserve evidence.
Canada	Search warrant extends to digital data (law enforcement may access networks connected to computer that is being searched).
France	Search warrant extends to digital data (remote search possible within computer networks accessible from computers included in warrant).
Poland	Legal after obtaining court order.
United States	Generally legal; search has to satisfy the Fourth Amendment guarantees.
Convention on Cybercrime	Legal; includes provisions on requesting transnational remote search.

Evidential Value of Bitcoin

Within the involvement of Bitcoin, and its evidential value, the problem seems binary. If law enforcement manages to capture wallets on seized machines, Bitcoins are treated as proceeds of crime and are subject to regulations concerned with seized assets (United States of America v. Ulbricht, partial judgement by default and order of forfeiture, No. 13 Civ. 6919 (JPO)). This is what happened with Bitcoins during the apprehension of Ross Ulbricht—law enforcement seized and ultimately auctioned currency found[8]. Furthermore, these assets are evidence of profit obtained from criminal enterprise. On the other hand, the value of account address is rather minimal. While it might be used to track down transaction and potential clients or conspirators, due to anonymisation mechanisms, the chance of obtaining a significant lead is remote. Furthermore, as users can generate an unlimited number of wallets, establishing links between accounts and particular machines sufficient to be presented as evidence is almost impossible.

Spy: Targeted Operations Conducted by SIGINT Agencies

Involvement of intelligence agencies is impossible to omit while discussing the modern fight against cybercrime. Resources, expertise and technical means available to those entities make them the most capable actors on the landscape of counter-cybercrime operations. The role of such agencies described in this article is not always what is commonly understood as "law enforcement". Their main role remains engaging with foreign actors, however as use of intelligence in domestic investigation increases (von Voorhout, 2006) not describing techniques at their disposal would result in an incomplete picture of the power available to governments. Furthermore, influx of incidents like the Sony security breach might result in a necessity of involving SIGINT entities in protection of commercial networks. While, by their nature, such operations are classified, leaked documents provided insight into operations conducted by major intelligence agencies.

Technical Advantage of SIGINT Agencies

The analysis of documents released by Edward Snowden provides great insight into the technical means available to signal intelligence and enables a comparison against methods used by civilian law enforcement. Asymmetric capabilities is best described in these terms: law enforcement routinely use traditional investigative techniques, while counter-cybercrime operations require involvement of cybersecurity experts;

---

8 This is also great illustration of how available are transaction made with Bitcoins. Operations on funds made by law enforcement can be accessed by anyone at https://blockchain.info/address/1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

SIGINT agencies routinely engage in extremely advanced surveillance methods, while targeted operations involve methods beyond capabilities and resources of any civilian law enforcement agency.

Programs which gained most popularity in media were mass surveillance programs such as PRISM or TEMPORA. However in terms of counter-cybercrime operations the capability of targeted attacks is significantly more important. Mass surveillance programs relied on massive storage capabilities and legal authority to coerce service providers to cooperate with intelligence agencies. On the other hand, targeted operations present the cutting-edge technology and evident technological superiority available to SIGINT.

One of the operational units exposed during NSA document leaks was the Office of Tailored Access Operations (TAO). Active since 1998 aimed at infiltrating, monitoring and gathering intelligence from computer networks. Effectiveness of TAO relied on obtaining data from upstream collection, a term used by the NSA to describe interception of data from "internet backbone"—major internet routers, cables, and switches. One famous example of upstream collection is Room 641A, a telecommunication interception facility where the NSA tapped directly into fibre optic cables of telecommunication services provider AT&T. This type of data interception was conducted under program XKEYSCORE. TAO has developed 'fingerprints' of specific hardware-software configurations which then could be correlated with data obtained by upstream collection. Due to the global nature of the internet, even tapping US based fibre cables provided targets from all over the world (Gallagher and Greenwald, 2014). To perform successful remote operations and remain undetected TAO employed the QUANTUMSQUIRREL program, which enabled masquerading as any routable IP address in the world (a technique commonly known as "spoofing"). Unfortunately, no documents regarding the technical side of QUANTUMSQUIRREL were leaked. What is known however, is that the whole suite of penetration facilitating tools was developed under the umbrella term "QUANTUM" (NSA, 2010). These tools provided multiple capabilities; most prominent was QUANTUMINSERT, which was able to mimic whole services such as YouTube or Yahoo. After capturing enough data about a target's online behaviour, the tool was able to redirect traffic from the subject's computer to NSA servers without any noticeable change on victim's side (Schneier, 2013b). In reality however, after accessing a particular service, QUANTUM launched tailored exploits enabling access to targeted machines (NSA, 2010). This type of attack is available exclusively to government agencies, as it requires access to the internet backbone. This is because an attacker requires a privileged position on the network in order to win race condition and therefore responds to the request of the user before the legitimate server does. Another important tool is FoxAcid. Described in NSA presentations as an "exploit orchestrator." The purpose of FoxAcid was to launch targeted attacks at specific machines. FoxAcid ran on publicly accessible servers, which waited for so-called FoxAcid tags (Schneier,

2013b). A tag being a specially prepared URL (Uniform Resource Locator), which commanded FoxAcid to launch an attack against a computer. TAO was tricking victims into using tagged URLs through a variety of methods including injection and phishing attacks. Frameworks were also equipped with several payloads, updated on regular basis by TAO. To remain effective for a considerable period of time FoxAcid used a sophisticated detection prevention mechanism, able to deceive commercial anti-virus software and modify operating systems in order to survive reboot. The type of attack was based on an assessment made by FoxAcid: in case of well-secured systems, it could launch zero day exploit, or even decide not to attack at all. As, by definition, it is only possible to use zero-day exploit once FoxAcid may however, decide that using it would be wasteful. Because of how automated this process of exploitation is, some researchers criticised the system claiming that it provides enormous power to employees who do not fully comprehend the gravity of their actions (Schneier, 2013a). Furthermore, these methods are not overly different from those used by cybercrime groups, as they rely on massive propagation of malware, similar to i.e. spread of botnet[9].

The deanonymisation of Tor users ranks high on the list of priorities of targeted operations (NSA, 2013b). In fact, the agency developed an entire program for identifying machines within Tor network, using the functionality of QUANTUM (NSA, 2007). Using upstream collection of data, the NSA created a database of Tor users – which is easy to achieve, as by design all Tor clients should look the same. To distinguish individual users QUANTUM analysed each system it detected, and produced software-hardware 'fingerprints' of system configuration. Gathered patterns were automatically processed and matched with possible FoxAcid attacks for further exploitation. According to presentations on project EGOISTICALGOAT/EGOISTICALGIRAFFE, the NSA tried to attack specific Tor users by targeting the Firefox browser included as a part of the Tor bundle (NSA, 2007). Similarities between this proposition and FBI operations "Magento" and "Torpedo" show that in the case of Tor, identification tools used by the agencies are different but the ultimate method of attack remains similar. Furthermore, the NSA admits that it is impossible to deanonymise a significant portion of network (NSA, 2012), and that Tor remains the best online anonymity tool available (NSA, 2013c). Targeting Tor is also becoming part of official operations. In December 2014, British Prime Minister David Cameron officially announced that GCHQ would cooperate with the National Crime Agency to tackle child pornography groups in dark net (gov.uk, 2014).

---

9 View represented by some security researchers i.e. "the grugq" : https://twitter.com/thegrugq/statuses/388250720907980800

Conclusion

Taking into consideration the cases of counter cybercrime operations analysed here and the challenges faced by law enforcement the following points can be made. Criminals can easily obtain high-grade tools due to quality of open source software. This generates an equality of capabilities between law enforcement and cybercriminals. The best example of this phenomenon is operation "Torpedo". The fact that FBI determined freely available Metasploit suite to be the best tool to attack Tor users shows how both sides have similar software capabilities. This is a by-product of the open nature and culture of the development of exploit and hacking tools. Databases of vulnerabilities have found over thirty thousand exploits and are being updated every day, while professionally prepared penetration testing distribution (Kali Linux) is open source. Criminals use legitimate products for illegitimate actions, i.e. Metasploit framework that is a penetration testing tool. This situation is unlikely to change as the nature of security research promotes disclosure of vulnerabilities in order to make the internet safer as a whole. Attempts to limit distribution of such tools are not only ineffective, but cause more harm than good by stifling legitimate security research—as proven by German legislation which caused many information security researchers to leave the country (Naraine, 2007).

It is impossible to prevent the proliferation of unbreakable encryption in the form of data encryption, and internet connection anonymisation. Law enforcement will have to circumvent these solutions or rely on their unconventional implementations. The fact that Tor appears during many high profile cases means that SIGINT agencies have put a high priority on it, results from the fact that it is extremely effective. NSA attempts at tackling it based on attacking its peripherals proves that, as for this moment, Tor protocol itself remains completely secure. This is even more significant for data encryption, as its essential role in protecting government information ensures that state authorities themselves will help with the development of unbreakable algorithms. Furthermore, it is impossible to create legal instruments capable of effectively forcing suspect into providing key. Even disregarding civil rights concerns and imposing strict punishment for not complying with disclosure orders does not change the fact that ultimately it is up to owner of the data to decrypt it. Given legitimate aims of such tools, statements about the availability of software is even more applicable than in the case of the penetration of testing tools used for illegitimate hacking.

Law enforcement has been provided with adequate legal instruments to engage in various forms of targeting electronic surveillance, due to the fact that criminal procedure provisions provide blanket authority on techniques used. On the other hand, the issue of the transnational character of cybercrime becomes increasingly problematic. The law rarely authorises law enforcement agencies to conduct remote searches beyond the borders of its own country. Therefore, the role of multinational task forces and international cooperation will have to increase in

order to effectively combat transnational cybercrime. The formation of EC3 in Europe is a step in this direction; however transatlantic partnerships will have to further develop as well.

SIGINT agencies possess capabilities to engage in operations of extreme levels of sophistication. However, they tend to be too intrusive and their use results in the compromise of security for ordinary users. In addition, due to their nature, use of such methods in domestic law enforcement is limited. As their most important role remains targeting foreign threads and terrorist activity, proceeding with a criminal justice system which usually requires disclosure of investigative methods is unacceptable for SIGINT agencies. This is illustrated by the secrecy that surrounded the FoxAcid program and the attempts to prevent further release of information following the Edward Snowden's leak. On the other hand, given how much publicity programs have already received and taking into account David Cameron's declaration about GCHQ, it is not unlikely that SIGINT agencies will become more involved in criminal investigations—which also means that more detailed regulations regarding authorisation of deployment of their capabilities against domestic targets will be required.

References

ACLU (2014) *ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media*. April, 4.

Biryukov A, Khovarotivich D and Pustogarov I (2014) Deanonymisation of clients in Bitcoin P2P network. *University of Luxemburg*.

Bennett CH and Brassard G (1984) Quantum Cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore*.

Brenner SW (2012) Law, dissonance, and remote computer searches. University of Dayton School of Law.

Canetti R, Dwork C, Naor M and Ostrovsky E (2006) Deniable encryption. *Lecture Notes in Computer Science*. Volume 1294, 1997, pp 90-104.

Chakravarty S, Stavrou A and Keromytis AD (2008) Approximating a Global Passive Adversary against Tor. *Computer Science Department Technical Report CUCS-038-08*, Columbia University.

Christin N (2012) Traveling the Silk Road: A measurement analysis *of a* large anonymous online marketplace. *WWW '13 Proceedings of the 22nd international conference on World Wide Web*. p. 213 -224.

Council of Europe (2008) *The effectiveness of international co-operation against cybercrime: examples of good practise*. Prepared by Pedro Verdelho. March, 12.

Council of Europe (2009) *Cybercrime and Internet jurisdiction*. Prepared by Prof. Dr. Henrik W.K. Kaspersen. March, 5.

Council of Europe (2012) *Electronic Evidence Guide*. Data Protection and Cybercrime Division.

Europol (2014) Global action against dark markets on tor network. Press release. November, 7. Retrieved from: https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network (accessed: 20.12.2014).

Cubrilovic N (2014) Analyzing the FBI's Explanation of How They Located Silk Road. September, 7. Retrieved from: https://www.nikcub.com/posts/analyzing-fbi-explanation-silk-road/ (accessed 11.12.2014).

Dingledine R, Mathewson N and Syverson P (2004) *Tor: the second-generation onion router. SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium, Volume 13.*

FBI (2012) *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. April, 24.

Feikert C and Doyle C (2006) Anti-terrorism authority under the laws of the United Kingdom and the United States. Congressional Research Service.

Gercke M (2012) Understanding cybercrime: phenomena, challenges and legal response. ITU.

Gallagher R and Greenwald G (2014) How the NSA Plans to Infect 'Millions' of Computers with Malware. *The Intercept*. March, 12. Retrieved from: https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/ (accessed: 12.12.2014).

Greenberg A (2014) FBI's Story of Finding Silk road's Server Sounds a Lot like Hacking. *Wired*. August, 9. Retrieved from: http://www.wired.com/2014/09/fbi-silk-road-hacking-question/ (accessed 11.12.2014).

Greenberg A (2015) Silk Road Mastermind Ross Ulbricht Convicted of All 7 Charges. *Wired*. February, 4. Retrieved from: http://www.wired.com/2015/02/silk-road-ross-ulbricht-verdict/ (accessed: 15.04.2015)

Grinberg R (2011) Bitcoin: an innovative alternative digital currency. *Hastings Science & Technology Law Journal*, Vol. 4, p.160.

Gorman S (2010) U.S. Plans cyber shield for utilites, companies. *Wall Street Journal*. July, 8. Retrieved from: http://www.wsj.com/news/articles/SB10001424052748704545004575352983850463108?mod=WSJ_hpp_MIDDLETopStories&mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748704545004575352983850463108.html%3Fmod%3DWSJ_hpp_MIDDLETopStories (accessed: 11.12.2014).

Gov.uk (2014) PM announces new global action to deal with online child abuse. Press release. December, 11. Retrieved from: https://www.gov.uk/government/news/pm-announces-new-global-action-to-deal-with-online-child-abuse (accessed: 18.12.2014).

Halderman JA, Schoen SD, Heninger N, Clarkson W, Paul W, Calandrino JA, Feldman AF, Appelbaum J and Felten EW (2008) Lest We Remember: cold boot attacks on encryption Keys. *Proc. 17th USENIX Security Symposium (Sec '08).*

Jarrett HM, Bailie MW, Hagen E and Judish N (2009) Searching and seizing computers and obtaining electronic evidence in criminal investigations. *Office of Legal Education Executive Office for United States Attorneys.*

Kaminsky D (2011) Black Ops of TCP/IP. Presentation during BlackHat 2011 conference.

Krebs B (2014) Silk Road Lawyers Poke Holes in FBI's Story. *Krebs on Security.* October, 2. Retrieved from: http://krebsonsecurity.com/2014/10/silk-road-lawyers-poke-holes-in-fbis-story/ (accessed: 20.12.2014).

Lach A (2011) Remote search of computer network. *Prokuratura i Prawo* 9, 2011.

MacAskill E, Borger J, Hopkins N, Davies N and Ball J (2013) GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian.* June, 21. Retrieved from: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (accessed: 11.12.2014).

McCoy T (2015) Secret journal of Silk Road founder Ross Ulbricht. *Washington Post.* January, 26. Retrieved from: http://www.washingtonpost.com/news/morning-mix/wp/2015/01/26/the-truth-of-silk-road-founder-ross-ulbricht-in-his-own-words/ (accessed: 15.04.2015).

McMillan R (2014) The NSA Is Building a Quantum Computer? We Already Knew That. *Wired.* January, 3. Retrieved from: http://www.wired.com/2014/01/hard_targets/ (accessed: 01.05.2015).

Mohan V and Villasenor J (2012) Decrypting the fifth amendment: the limits of self-incrimination. University of Pennsylvania Journal of Constitutional Law Heightened Scrutiny, volume 15, pages 11-28.

Naraine R (2007) Exploits, security tools disappear as German anti-hacker law takes effect. *ZDNet.* August, 13. Retrieved from: http://www.zdnet.com/article/exploits-security-tools-disappear-as-german-anti-hacker-law-takes-effect/ (accessed: 15.04.2015).

NIST (2001) *Announcing the Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197. November, 26.

NSA (2007) *Peeling back the layers of Tor with EgotisticalGiraffe* presentation.

NSA (2010) *QUANTUMTHEORY presentation*, 2010 SIGINT development conference.

NSA (2013a) *PRISM/US-984XN Overview* presentation.

NSA (2013b) *Tor stinks* presentation.

NSA (2013c) T*ypes of IAT – Advanced Open Source Multi-Hop* presentation.

Pollack P (2006) UK wants power to demand encryption keys. *Arstechnica*. May, 18. Retrieved from: http://arstechnica.com/uncategorized/2006/05/6870-2/ (accessed: 15.12.2014).

Poulsen K (2013) FBI Admits It Controlled Tor Servers Behind Mass Malware Attack. *Wired*. September, 13. Retrieved from: http://www.wired.com/2013/09/freedom-hosting-fbi/ (accessed 11.12.2014).

Poulsen K (2014a) Visit the Wrong Website, and the FBI Could End Up in Your Computer. *Wired*. August, 5. Retrieved from: www.wired.com/2014/08/operation_torpedo/ (accessed: 17.12.2014).

Poulsen K (2014b) The FBI Used the Web's Favorite Hacking Tool to Unmask Tor Users. *Wired*. December, 16. Retrieved from: http://www.wired.com/2014/12/fbi-metasploit-tor/ (accessed: 17.12.2014).

Pradillo JCO (2011) Fighting Cybercrime in Europe: the admissibility of remote searches in Spain. *European Journal of Crime, Criminal Law and Criminal Justice*, Volume 19, Number 4, 2011.

Reich PC (2012) Law, policy, and technology: cyberterrorism, information warfare, and internet immobilization. IGI Global.

Schneier B (2013a) How the NSA Thinks About Secrecy and Risk. *The Atlantic*. October, 4. Retrieved from: http://www.theatlantic.com/technology/archive/2013/10/how-the-nsa-thinks-about-secrecy-and-risk/280258/ (accessed: 15.12.2014).

Schneier B (2013b) How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID

Schneier on Security. October, 7. Retrieved from: https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html (accessed 11.12.2014).

Shor PW (1997) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. 26 (5): 1484–1509.

Sottiaux S (2008) Terrorism and the limitation of rights: the ECHR and the US Constitution. Bloomsbury Publishing.

TechWorld (2010) FBI hackers fail to crack TrueCrypt. Open source encryption on Brazilian banker's hard drive baffles police dictionary attack. June, 10 Retrieved from: http://news.techworld.com/security/3228701/fbi-hackers-fail-to-crack-truecrypt/ (accessed 11.12.2014).

Timberg C and Nakashima E (2013) FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance. *The Washington Post*. December, 6. Retrieved from:

http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html (accessed: 18.12.2014).

Tor Project (2014) Tor Overview.

van den Berg R, Ideler HAW, Slobbe J and Verberkt SLC (2011) Remote search by justice authorities: a legal advice to the Dutch court and European legislator.

van Voorhout JEBC (2006) Intelligence as legal evidence: comparative criminal research into the viability of the prosed Dutch scheme of shielded intelligence as witnesses in England and Wales, and legislative compliance with Article 6 (3) (d) ECHR. *Utrecht Law Review*, Volume 2, Issue 2 (December) 2006.