The adversarial threat posed by the NSA to the integrity of the internet

Jared Naude
Computer Science & Information Systems
North-West University
Potchefstroom, South Africa
jared@naude.co

Lynette Drevin
Computer Science & Information Systems
North-West University
Potchefstroom, South Africa
Lynette.Drevin@nwu.ac.za

Abstract— **In 2013, Edward Snowden, a NSA Contractor leaked thousands of highly classified documents about the activities of the USA's National Security Agency (NSA) and its foreign intelligence partners known as the "Five Eyes" [1]. The documents revealed secret programs about the NSA's mass bulk collection of phone, internet and communications traffic as well as how the NSA and its partners are working to sabotage and weaken encryption algorithms and the security protocols used to secure the internet. This paper presents some of the programs that were revealed as well as the rationale and legislation behind these programs from a global perspective. Mass surveillance is not only done by the Five Eyes partners but also by many other countries who pay private companies to provide them with tools to spy, censor and repress their own citizens [2]. In order to assess the potential harm and the security implications of mass surveillance, this paper looks at how state level actors around the world are conducting surveillance which raise broader issues about internet security such as how common weaknesses are being exploited by both intelligence agencies and criminals. This paper will also explore various technologies and techniques that can be used by both individuals and companies to secure themselves against mass surveillance.**

Keywords: NSA; mass surveillance; security threats; awareness

I. INTRODUCTION

In 2013, Edward Snowden, a NSA Contractor leaked thousands of highly classified documents about the activities of the USA's National Security Agency (NSA) and its foreign intelligence partners known as the "Five Eyes" [3]. To date more than 200 programs have been revealed that detail the wide range of the NSA’s activities such as domestic and foreign bulk surveillance, the weakening of security protocols, spying on military communications, computer network exploitation and signals intelligence to name a few. This paper does not look at all of the NSA programs that have been revealed in specific detail as there are simply too many for the scope of this paper. This paper will however present an overview of some of the programs to get a perspective of what the NSA and its partners can do. This paper will look at how these tools have been misused as well as the false justifications for the use of these tools. This paper will also present mechanisms to protect individuals and organizations against these types of security threats.

II. METHODOLOGY

This paper reports about a study that was undertaken on the topic of the NSA harming the integrity of the Internet [4].

The aims were stated as:

- “To critically evaluate the activities of the NSA and how they harm the integrity of the internet.”
- “To inform the public about mass surveillance and detail what they can do to stop it and how they can protect themselves from it by raising awareness of these security threats.”

The methodology used was to do a comprehensive literature study focusing on key terms such as data mining, exploits, mass surveillance, deep packet inspection, deep packet injection and zero-day vulnerabilities. Content analysis was the approach used to order the information and categorize important topics. Data that were analyzed was content from documents leaked by Edward Snowden of the NSA's programs.

The design science strategy was also used to create certain artifacts for this project. To raise awareness of users, four separate products were created:

- A video,
- Flipboard magazine,
- A website and
- A brochure that was developed and presented to users.

This paper however only concentrates on the results of the content analysis using mainly documents, videos and slides.

The next section describes some programs of the NSA.

III. PROGRAMS OF THE NSA

A. PRISM

In June 2013, the first leaked documents were published by Glenn Greenwald in the Guardian regarding the NSA’s bulk metadata program and the PRISM program. PRISM allows the NSA to retrieve data from major online services including Google, Apple, Facebook, AOL and Skype amongst others [5].

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

The initial leaks rocked the world as outrage and fury over the NSA's activities spread around the world. The leaks were very controversial especially when it was revealed that the US was spying on numerous world leaders and leaders of the United Nations.

B. BULLRUN

The documents also revealed the BULLRUN program which aims to insert backdoors into the telecommunication systems, encryption standards, operating systems and other technologies that are used by everyone every day [6]. NSA documents show that the NSA's goals were to "influence policies, standards, specifications for commercial public key technologies" and to "insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets" [6]. Secure Socket Layer (SSL), Transport Layer Security (TLS) and Virtual Private Networks (VPNs) were specifically targeted by the BULLRUN program. As part of BULLRUN, the NSA also paid RSA, a leading security firm, $10 million dollars to include a weak random number generator Dual_EC_DRBG in its BSafe software which has a backdoor which could allow the NSA to decrypt data encrypted with it [7].

C. X-KEYSCORE

The NSA documents revealed two types of surveillance; blanket dragnet surveillance and so called “targeted” surveillance. The blanket surveillance is made possible by a program named X-KEYSCORE, a global passive monitoring system that ties into many interception systems that allows the NSA to analyze global communications by tapping into the global undersea fiber optic cables through 150 interception points and 750 servers around the world [8][9]. X-KEYSCORE is the backend system of the mass surveillance and the front end system for NSA Analysts. X-KEYSCORE also ties into many other NSA programs such as QUANTUMINSERT and is often used for retargeting by other programs. Each X-KEYSCORE interception point can process 125GB of information per second [10].

In order for the NSA to see what is flowing past the X-KEYSCORE interception points, the NSA developed a very sophisticated deep packet inspection technology, codenamed TURMOIL which is a passive monitoring interception system that can inspect and filter data in real time as it passes over fiber optic cables through the X-KEYSCORE program [8]. The X-KEYSCORE system is so powerful that it can scan documents for phrases and images, so a NSA analyst can query a logo and the system will return all documents that have this logo [8]. An NSA analyst can query a so called “selector” which is any identifiable information such as a phone number, IMEI number, MAC or email address tied to an end point of communication. The system will then return all the information stored to the analyst and will also scrutinize further communication from the “selector” [10].

D. TURMOIL and TURBINE

The NSA also uses deep packet injection technology codenamed TURBINE that can inject packets into a connection to compromise a target by injecting malware into the connection [8]. The NSA then uses TURMOIL and TURBINE together in a program called QFIRE that can automate attacks against targets or any person that is doing something that the NSA finds interesting [8]. This deep packet injection technology is used by the NSA in its FOXACID program, which allows the NSA to intercept a user’s connection to a website such as Facebook or LinkedIn. They then direct them to the NSA’s servers where they can exploit the user by infecting the user with malware [8]. This is primarily done by injecting malware into iframes on a web page which then exploits vulnerabilities in web browsers to give system access [11].

E. MUSCULAR

The NSA through its MUSCULAR program has managed to infiltrate private fiber optic links in Google's own internal network as well as the links between Google's and Yahoo's datacenters. The traffic between these links is sent in clear text and makes it easy for the NSA to collect vast amounts of unencrypted information [12]. The FAIRVIEW program allows the NSA to gain access to international cables, routers and switches from ISPs and telecommunication providers [13]. One FAIRVIEW document shows that in a 30 day period in December 2012, it collected more than 200 million records per day for a total of than 6 billion records for the month [13].

F. Other significant programs

Documents about the Cryptologic platform reveal that the NSA has more than 50 000 CNE implants all over the world and further reporting by the New Times reveal that the NSA has infected more than 100 000 computers with malware [13]. EVILOLIVE is a NSA program that does IP geolocation of target connections. The name of the program is interesting because it is both a palindrome and an anagram for "I love evil" [14]. FASCIA is a NSA program that stores location information while NUCLEON stores the content of phone calls. MAINWAY stores metadata regarding phone calls and MARINA stores metadata about internet traffic [14]. The CO-TRAVELER program automates guilt by association, meaning that if a person was in the vicinity of a suspected terrorist, the person is automatically thought to be a terrorist too [14]. All of this information is collected and stored for at least 15 years [8].

MAINWAY is a program that stores metadata about phone calls. This is one of the most controversial programs in the US and hundreds of millions of phone records have been obtained via Section 215 of the USA Patriot Act. The information stored about phone calls includes: the terminating phone number, IMSI number, IMEI number, trunk identifier, telephone calling card numbers and the time and duration of the a call [14]. The NSA claims that it is just metadata. However, it is easier for the NSA to pass and analyze metadata than it is for them to parse and analyze the actual voice content of a phone call. A lot of information can be learned from just the metadata of a phone call. For example: if someone calls a HIV testing service, then their doctor and after that their health insurance, the NSA can make many assumptions based on that information [14].

After having looked at some NSA programs the next section indicates how the surveillance tools may be used for exploitation.

IV. MISUSE OF SURVEILLANCE TOOLS

One of the defenses of mass surveillance is that many countries spy and that may be true. However, the argument is not balanced by any means. There are four aspects that determine whether or not a government is capable of doing mass surveillance; these include their budget, policy, technical ability and strategic advantage which are all interconnected. Many countries who want to conduct mass surveillance do not have the technical ability, budget or strategic advantage to conduct surveillance.

In this respect the US has a major advantage over other countries. After 9/11 the policy of the US government regarding domestic and foreign surveillance went through a radical change to a broader and more encompassing surveillance state. This policy change meant that intelligence agencies received hundreds of millions of dollars in funding to build powerful surveillance systems to collect and store a vast amount of data. They also developed sophisticated exploitation, intrusion, crypto exploitation and data analysis capabilities. In 2013, the national intelligence budget known as the "black budget" totaled $52.6 billion dollars [15].

The US government also has the technical ability to conduct surveillance. Documents show that the NSA is hoarding zero day exploits to use against targets and instead of fixing known vulnerabilities in systems and software; the NSA keeps quiet about these vulnerabilities so that it can exploit them. This leaves everyone vulnerable to attack, not only by the NSA but any malicious hackers that have the time and resources to find these vulnerabilities [8][16].

The NSA also has the infrastructure to conduct surveillance, including a massive data center Blufdale, Utah near Salt Lake City. This facility spans over 100 000 square feet, uses 6 500 tons of water per day and consumes 65 megawatts of electricity and is estimated to cost the NSA $40 million in electricity annually [14][17]. Various estimates have been given regarding how much storage space the NSA has. Conservative estimates are between 3 to 12 exabytes of data and other estimates are much higher than 12 exabytes. That is enough storage to keep content for many years, up to 15 years by some estimates [8][14]. In addition to the data center, the NSA also has 2 supercomputers as well as vast foreign infrastructure which are used to carry out attacks.

The US government also has the strategic advantage to conduct surveillance. The most widely used internet tools, services and products used by millions of people around the world such as Facebook, Google, Dropbox, iOS, Android, Yahoo, Firefox, Chrome, Internet Explorer, Windows and OSX are all made by American companies. If a technology company were to receive a court order from the US government, it would be very hard for them to refuse it whereas if it was received a foreign court order demanding data, it would be easy for the company to reject it.

To understand the harm of surveillance, one needs to look at how governments around the world are conducting surveillance. After 9/11 there was a gold rush for surveillance tools and in 2011 it was revealed by Wikileaks that there are more than 160 companies in 20 different countries that are selling these tools. The big companies selling these surveillance, network intrusion and so called "lawful interception" tools include BlueCoat, Gamma International, HackingTeam and VUPEN amongst many others [2]. Freedom of information requests have revealed that VUPEN is an NSA contractor and sells their exploits to the NSA [8]. Documents published by Privacy International show that HackingTeam is also selling their gear to various US governmental agencies including the FBI and DEA. It is also suspected that HackingTeam is selling their gear to the NSA.

Research done by the Citizen lab has detailed how governments around the world who do not have the technical ability to conduct mass surveillance, purchase these tools and then use these tools to spy, censor and repress their own citizens in addition to cracking down on dissidents and protestors. These tools have also been used to spy on investigative journalists who exposed the government's wrongdoing and corruption [2]. Security researchers have also found that FinFisher software was used by governments in Malaysia and Ethiopia to insert backdoors into the computers of journalists so that they could identify the sources of the journalists [2][8]. The research also shed light on where these tools are being used. These countries include: Colombia, Azerbaijan, Kazakhstan, Libya, Uzbekistan, Oman, Iran, Morocco, Malaysia, Ethiopia, Saudi Arabia, United Arab Emirates and many other embargoed countries. These software tools are often used by governments to illegally spy on their citizens and any political dissidents [2]. These countries claim that it is for national security but fail to give any evidence of them using the tools for national security.

The US government claims that the surveillance is necessary for national security in order to prevent terrorist attacks. The whole war on terror narrative told by the US government is misleading. A 300 page report compiled by an independent White House review panel has found that the NSA has never stopped a single terrorist attack. According to Edward Snowden, when the NSA goes after terrorists it is the exception to what they do and not the norm. Along with intercepting and storing data for "counterterrorism" operations, the documents show that the NSA has been complicit in economic spying for the US where the NSA helps US companies win big tenders against international rivals [16].

In every major terrorist attack in the western world including 9/11, the Boston Marathon bombing, the attack on Fort Hood, the Charlie Hebdo attack in France and the attack on the Lindt Café in Sydney, the attackers were known to intelligence agencies long before the attacks took place. Authorities in Australia received 18 tip offs about the attacker but did nothing with the information they received. This may suggest that strengthening counter terrorism operations instead of mass surveillance may be a better solution to fight terrorism [18].

Since the Snowden leaks it has become clear that the oversight of the NSA is extremely poor. Behind closed doors, members of congress admitted to Glen Greenwald, the primary journalist behind the Snowden disclosures, that they did not know about the NSA programs and are very glad about the reporting that he was doing. This raises an important issue about the oversight of the NSA, which many analysts, politicians and commentators believe to be extremely poor. In 2012, the NSA violated its own internal rules 2 776 times and the head of the Senate Intelligence committee, Diane Feinstein, did not know about this until she was asked for comment by the media [13]. In addition to these violations, NSA analysts were also using their powers to spy on their loved ones and were also routinely sharing nude photos that were being intercepted. In addition, the NSA's auditing was so poor that they did not know what files Edward Snowden took. This raises important questions about how the data could be misused and the NSA would not know about it. Most of the oversight of the NSA is also done by former intelligence lobbyists. This is particularly troubling as they cannot be expected to be impartial when more than 70% of the national intelligence budget is spent in the private sector [13][19].

At a Senate Intelligence committee hearing in March 2012, the Director of the NSA, General Keith Alexander was asked if the NSA knew how many Americans had their electronic communications collected or reviewed to which Alexander responded that they did not. At another hearing of the Senate intelligence committee in March 2013, Senator Ron Wyden asked the Director of National Intelligence, James Clapper: "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?", "No sir," replied Clapper. The Snowden documents show us this is not true and that the NSA had a tool called Boundless informant which allowed the NSA to see exactly how many events and the countries in which the data was collected. This raises an important question; how is congress meant to do oversight of the NSA when members of the intelligence agencies continuously lie to them? [8][13][14][19]

The following section presents aspects of the debates that followed globally after the information was leaked.

V. THE GLOBAL RESPONSE

The revelations about the NSA's activities have spawned a massive global debate about surveillance and the integrity of the internet. The fundamental problem with mass surveillance is that the information is stored for extended periods of time and if an illegitimate government were to come into power, they could use the NSA's databases to stay in power.

When it was revealed that the NSA had spied on 122 world leaders including the presidents of Brazil and Mexico, the European Parliament and the United Nations, the president of Brazil, Ms. Dilma Roussef, cancelled a diplomatic trip to the US in protest and went to the United Nations to denounce the United States spying as illegal and in contravention of international law. The inventor of the World Wide Web, Sir Tim Berners-Lee, has called the NSA surveillance "an intrusion on basic human rights" and has urged people to seek out and demand better legal protection and privacy safeguards for the services that they use [20]. Sir Tim Berners-Lee has also called on people to help a draft of a global bill of rights that includes protections for the internet [21]. The Electronic Frontier Foundation (EFF) is working on 13 principles for spying and over 300 organizations worldwide are supporting it, and it is being pushed as a basis for a UN resolution [14].

The NSA revelations have hurt US business badly. Brazil has cancelled its contract with Microsoft and many other companies are moving their data to providers in other countries in an attempt to thwart NSA surveillance. Analysts say the revelations about the NSA's activities might cost the US up to $180 billion in lost business as companies seek out alternative places to store their data [22].

Technology companies that were named in the NSA slides have responded strongly by adopting HTTPS by default along with Transport Layer Security (TLS) and forward secrecy. These companies have also fast tracked various encryption plans such as Google which has now started to encrypt their data center links and offer better encryption on its software and tools. Dropbox, Facebook, Google, Microsoft, Twitter and Yahoo also took out a full page advert in the New York Times to protest the programs of the NSA [14].

Both iOS and Android will soon encrypt users' data by default and it cannot be decrypted by Apple or Google even with a warrant. This is a move which has been heavily criticized by the FBI which claims that it will hinder their ability to do investigations. In response to this, law enforcement agencies have rallied governments to add backdoors to encryption algorithms as they claim that they are going dark when in reality they are gaining more access than ever before [10][23]. In theory there could be many ways to backdoor encryption algorithms. However, security experts caution against doing this as it is very dangerous and in many respects impossible to do as there will always be ways to get around the backdoors [23].

During Barack Obama's presidential campaign, he rallied for greater transparency and accountability. Yet his administration has prosecuted more whistleblowers than all of the previous administrations combined [24]. Many governments claim that they want to stop corruption and increase transparency and accountability but then pass laws to add secrecy to their activities. This is why the need for privacy is extremely important. Investigative journalists who work with whistleblowers need privacy to expose the wrongdoing of governments around the world. The president of Brazil said "If there is no right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy" [25].

In order for people to take responsibility for their electronic resources' protection it is necessary to raise awareness about possible defense mechanisms. The next section introduces such methods.

VI. DEFENSE AGAINST MASS SURVEILLANCE: METHODS AND TECHNIQUES TO PROTECT USERS AND SYSTEMS FROM NSA SURVEILLANCE

A. *Encrypted communication*

Messages need to be encrypted when they are in transit. This prevents malicious users, ISPs and state level actors like the NSA from reading these messages. Emails can be encrypted with PGP which provides reliable and secure end to end encryption. In December 2014, Der Spiegel revealed that the NSA cannot decrypt emails encrypted with PGP [26].

Swapping public keys for PGP email can be a challenge and there are a few services that are trying to make this process easier. One such service is Keybase.io, a public key directory service which allows users to look up and update their public keys.

As PGP is hard for the average user to use, Google is in the process of researching and creating browser based secure end to end encryption for email through Gmail. This feature is still in alpha testing at the moment and relies on OpenPGP to encrypt messages via JavaScript inside the browser so that the email message does not travel to Google's data center unencrypted [27]. Documents published by Der Spiegel show that the NSA in its own internal documents claim that they cannot decrypt PGP which is a very good endorsement of the technology [26].

The NSA documents show that the NSA is collecting almost 200 million text messages a day from around the world. They are using the text messages to extract locations, contact details and credit card details of users [28]. To counter this, numerous mobile applications for Android and iOS are being developed allowing users to send end to end encrypted instant messaging. These applications include Telegram, Text Secure, Chat Secure, and Gibberbot amongst many others. Telegram is an instant messaging app similar to WhatsApp and Snapchat that is available for both Android and iOS that has risen to fame after Facebook bought WhatsApp for $19 billion. Telegram has a feature called secret chat which provides end to end encryption that users can use to send encrypted messages to one another [29]. Messages sent through leave no trace on the companies servers. Telegram also has a Snapchat like feature in which users can set their messages to self destruct. The creators of Telegram are so confident about the security of their app that they are offering $200 000 to anyone who can crack the security of the app [29].

In October 2014, WhatsApp announced that it will be adding encryption to its app. However, analysis of this encryption reveals that WhatsApp is only implementing encryption without authentication which guards against passive surveillance but does not counter active attacks such as man in the middle attacks. Users can also use Off the Record (OTR) chat which is encrypted end to end which Der Spiegel also revealed that the NSA cannot decrypt [26].

The NSA has access to the metadata of phone calls which is collected through the MAINWAY program and the content of the phone calls can be collected through the NUCLEON program [8][14]. In order to thwart the NSA's collection and snooping in of phone calls, users have a few options to choose from when encrypting their phone calls. One of the preferred and most secure options is RedPhone which is a free open source Android only application that offers secure VOIP encryption for phone calls. If both parties are using RedPhone the call is encrypted end to end [8][30]. Other alternatives include Slient Phone which is available for iOS and Android which requires a subscription but can work on cross platforms. Another alternative is Ostel which is a paid app available for iOS and Android which uses the Open Secure Telephony Network to encrypt calls across various apps on different platforms [30].

Cryptographers and security experts caution against using untested applications that claim to provide end to end encryption as mistakes in implementing encryption are very common. Users should use audited applications such as RedPhone and TextSecure which have been proven to be secure.

B. Secure Socket Layer (SSL) and Transport Layer Security (TLS)

Secure Socket Layer enables a web server and client to send data to each other over an encrypted connection. The client connects to the web server where it receives the public key of web server, the client's browser verifies the web server's identify from the relevant certificate authority. Once the browser has authenticated the web server, a client can then browse the web server securely and all communication sent between the server and the client is secure. This makes it very difficult for the NSA and other intelligence agencies to intercept these communications [31].

Google may start using SSL as a ranking factor when ranking websites with its page rank algorithm. Websites that use SSL are more likely to care about the safety of their users and thus should benefit from an increased ranking in Google search results. Secure Socket Layer adds significant security to a connection. However, this security can still be improved with Transport Layer Security and Forward Secrecy which generates a unique key derived from a session key and the server’s public key. This means that if the private key of the web server is compromised, all of the sessions cannot be decrypted.

The University of Michigan, Mozilla and the Electronic Frontier Foundation (EFF) are working on a project known as the Let’s Encrypt project which will enable websites and other computerized systems to get free, secure, self-renewing SSL certificates that will be trusted by browsers as the project will have its own Certificate Authority (CA). This tool will make it easy for system administrators to install these certificates by using a single command in command line after which the tool will validate the domain and will install and configure the web server to use HTTPS [32].

C. Tails

The amnesic incognito live system (Tails) is a live operating system that can be mounted on most computers from a DVD, USB stick or SD card and is aimed at preserving the privacy and anonymity of users. This is done by routing all internet traffic through Tor, leaving no trace of it on the host computer and using state of the art cryptographic tools to encrypt users’ data [33]. Tails is used by many investigative journalists to protect their privacy and their sources [8].

D. TOR

One of the most effective and widely used ways of protecting the privacy of users is Tor. Tor or "the onion network" is a network of internet connected servers that are voluntarily run that enable users to browse the internet anonymously, circumvent government censorship and prevent ISPs from snooping into their users activities [8]. Tor has been heralded as a force for social good and is an essential tool for many users in oppressive countries to get around censorship such as the great firewall of China [2].

Tor in conjunction with Tails is recommended and is used by many journalists as an operational security measure to protect themselves and their sources. Tor enables whistleblowers to raise the alarm anonymously when something that they are involved with is not above board. Orweb is a mobile browser for Android that uses the Tor network and allows people to access the internet anonymously from their phones [30].

E. Webcam sticker

Security researchers have demonstrated numerous ways in which adversaries can gain access to the webcams of laptops without the webcam light switching on. The MARINA program of the NSA and the Optic Nerve program of the GCHQ collect webcam photos and store them. One of the recommendations of the Electronic Frontier Foundation (EFF) is that every user puts a sticker on their webcams as the webcams can easily be accessed by the NSA and other adversaries [8][14].

F. Full disk encryption

One of the basic and rudimentary ways a user and developers can protect their systems is to use full disk encryption which completely encrypts the hard drives / flash drives of their systems. This is a very good security practice when a hard drive is stolen or removed without permission. The data on the hard drive cannot be accessed without the encryption keys as the data is encrypted.

Most operating systems have their own implementation of full disk encryption. Windows has BitLocker, OSX has FileVault and Linux has LUKS. It should be noted however that it is best to use an open source encryption program like TrueCrypt which has been audited rather than using a closed source solution which may be backdoors in them.

TrueCrypt is an open source encryption solution that offers full disk encryption and file encryption for Windows, Mac and Linux. TrueCrypt was the encryption solution of choice for Edward Snowden who even spent time teaching people how to use the software [34]. TrueCrypt offers various encryption algorithms including AES, Serpent, Twofish, AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES and Twofish-Serpent to encrypt disks or file containers. In May 2014, the working version of TrueCrypt was removed from the TrueCrypt website unexpectedly and a warning message was shown advising users that it is not safe. However many security researchers believe the fundamental security of TrueCrypt is intact and that the developers may have been pressured by the NSA to stop development on the project [34]. In April 2015, a security audit carried out by an independent team of cryptographers has shown that there are no backdoors or critical weaknesses of Truecrypt.

This section looked into possible ways to protect systems against mass surveillance. The next section will conclude this paper.

VII. CONCLUSION

In this paper, some of programs of the NSA were discussed while highlighting how the NSA and its partners are working to undermine the security protocols and standards that are used to secure the internet in addition to doing bulk surveillance on the entire world.

The contribution of this study is to make people aware that these programs have very serious implications for privacy, democracy and the integrity of the internet. Individual internet users and organizations should be made aware about these threats and use protection mechanisms to secure their resources. Further work can be to focus on ways to educate users and organizations regarding online safety.

REFERENCES

[1] Greenwald, G., Borger, J. & MacAskill, E. 2013. The National Security Agency: Surveillance giant with eyes on America. http://www.theguardian.com/world/2013/jun/06/national-security-agency-surveillance. Date of Access: 01 April 2015.

[2] Guarnieri, C & Marquis-Boire, M. 2013. To Protect And Infect - The militarization of the Internet [30c3]. https://www.youtube.com/watch?v=sW-N7qQU-tA. Date of Access: 26 May 2014. [Video]

[3] Greenwald, G. 2013. XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. Date of Access: 26 May 2014.

[4] Naude, J. 2014. How the programs of the NSA are harming the integrity of the internet. ITRI 671 Project. NWU. Potchefstroom. S.A.

[5] Barrett, B. 2013. What Is PRISM?. http://gizmodo.com/what-is-prism-511875267. Date of Access: 21 March 2014.

[6] New York Times. 2013. Secret Documents Reveal N.S.A. Campaign Against Encryption. http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=0. Date of Access: 21 March 2014.

[7] Menn, J. 2014. Exclusive: NSA infiltrated RSA security more deeply than thought – study. http://www.reuters.com/article/2014/03/31/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331. Date of Access: 14 April 2015.

[8] Appelbaum, J. 2013. Jacob Appelbaum: To Protect And Infect, Part 2 [30c3]. https://www.youtube.com/watch?v=vILAlhwUgIU. Date of Access: 21 March 2014 [Video]

[9] Biggs, J. 2013. NSA Project XKeyscore Collects Nearly Everything You Do On The Internet. http://techcrunch.com/2013/07/31/nsa-project-x-keyscore-collects-nearly-everything-you-do-on-the-internet/. Date of Access: 21 March 2014.

[10] Snowden, E. 2013. Citizenfour produced by Laura Poitras. [DVD]

[11] Schneier, B. 2013. Attacking Tor: how the NSA targets users' online anonymity. http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity. Date of Access: 10 April 2015.

[12] Gallagher, S. 2013. How the NSA's MUSCULAR tapped Google's and Yahoo's private networks. http://arstechnica.com/information-technology/2013/10/how-the-nsas-muscular-tapped-googles-and-yahoos-private-networks/. Date of Access: 21 March 2014.

[13] Greenwald, G. 2014. No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state. ISBN: 978-1-62779-073-4. N.Y., NY.

[14] Opsahl, K. 2013. Through a PRISM, Darkly - Everything we know about NSA spying [30c3]. https://www.youtube.com/watch?v=BMwPe2KqYn4. Date of Access: 21 March 2014. [Video]

[15] The Washington Post, 2013. The Black Budget. http://www.washingtonpost.com/wp-srv/special/national/black-budget/. Date of Access: 26 May 2014.

[16] Snowden, E. 2014. Edward Snowden: Here's how we take back the Internet. https://www.youtube.com/watch?v=yVwAodrjZMY. Date of Access: 21 March 2014. [Video]

[17] Adams, A. 2013. New Utah NSA center requires 1.7M gallons of water daily to operate. http://www.ksl.com/?sid=25978926&nid=148. Date of Access: 26 May 2014.

[18] Piggott, M. 2015. Sydney cafe siege: Security hotline had 18 calls about Man Haron Monis before attack. http://www.ibtimes.co.uk/sydney-cafe-siege-security-hotline-had-18-calls-about-man-haron-monis-before-attack-1488996. Date of Access: 01 April 2015.

[19] Greenwald, G. 2015. Edward Snowden and the secrets of the National Security State. https://www.youtube.com/watch?v=-1jAOJHvll0. Date of access: 2 May 2015. [Video]

[20] Warr, P. 2013. Tim Berners-Lee calls NSA surveillance an 'intrusion on basic human rights'. http://www.wired.co.uk/news/archive/2013-06/10/berners-lee-nsa-prism. Date of Access: 21 March 2014.

[21] Meyer, D. 2014. 25 years after inventing the web, Tim Berners-Lee invites users to help draft global “bill of rights”. http://gigaom.com/2014/03/12/25-years-after-inventing-the-web-tim-berners-lee-invites-users-to-help-draft-global-bill-of-rights/. Date of Access: 21 March 2014.

[22] Waldman, P. 2014. The economic blowback from NSA spying begins. www.washingtonpost.com/blogs/plum-line/wp/2014/03/21/the-economic-blowback-from-nsa-spying-begins/. Date of Access: 21 March 2014.

[23] Mayer, J. 2015. You can’t backdoor a platform. http://webpolicy.org/2015/04/28/you-cant-backdoor-a-platform/. Date of Access: 5 May 2015.

[24] Ackerman, S. & Pilkington, E. 2015. Obama's war on whistleblowers leaves administration insiders unscathed. http://www.theguardian.com/us-news/2015/mar/16/whistleblowers-double-standard-obama-david-petraeus-chelsea-manning. Date of Access: 1 April 2015.

[25] Borger, J. 2013. Brazilian president: US surveillance a 'breach of international law'. http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance. Date of Access: 26 May 2014

[26] Der Spiegel Staff. 2014. Inside the NSA’s war on internet security. http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html. Date of Access: 1 April 2015.

[27] Doctorow, C. 2014. Google announces end-to-end encryption for Gmail. http://boingboing.net/2014/06/04/google-announces-end-to-end-en.html. Date of Access: 26 May 2014.

[28] Ball, J. 2014. NSA collects millions of text messages daily in 'untargeted' global sweep. http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep. Date of Access: 26 May 2014.

[29] Hamburger, E. 2014. Why Telegram has become the hottest messaging app in the world. http://www.theverge.com/2014/2/25/5445864/telegram-messenger-hottest-app-in-the-world. Date of Access: 26 May 2014.

[30] Neal, R. 2014. PRISM-Proof Your Smartphone: 10 Apps To Keep The NSA Out Of Your Phone. http://www.ibtimes.com/prism-proof-your-smartphone-10-apps-keep-nsa-out-your-phone-1321085. Date of Access: 26 May 2014.

[31] Zhu, Y. 2014. Why the Web Needs Perfect Forward Secrecy More Than Ever. https://www.eff.org/deeplinks/2014/04/why-web-needs-perfect-forward-secrecy. Date of Access: 26 May 2014.

[32] Eckersley, P. 2014. Launching in 2015: A Certificate Authority to Encrypt the Entire Web. https://www.eff.org/deeplinks/2014/11/certificate-authority-encrypt-entire-web. Date of Access: 1 April 2015.

[33] Tails. 2014. Privacy for anyone anywhere. https://tails.boum.org/. Date of Access: 27 June 2014

[34] McMillan, R. 2014. Snowden’s Crypto Software May Be Tainted Forever. http://www.wired.com/2014/05/truecrypt/. Date of Access: 26 May 2014.