Espionage and intrusion technology in russia

Neil McGeeverSpying and intrusion had been happening years before technology became involved. The increase in technology and the dependency on the internet has made espionage and intrusion simpler and more widespread. Various technology has been developed that allows different ways of collecting unlawful information and spying on enemies. Valuable data is being gathered and stored online, and will continue to increase with an emphasis on technology for performing tasks and operations over the internet. This data can be intercepted to provide priceless information.

Spying on the public and hacking sensitive information is certainly breaching the law and new laws are being introduced to protect the government and organisations for partaking in these activities. The public have the right to civil and privacy protection from these actions and should be obeyed, however there are certain cases when this should be permitted, such as against terrorist groups and organisations. This paper will discuss the different technologies being used to collect private information and data. It will also explain the laws that it affects that exist to protect the public and the new laws being introduced to protect the government.

Espionage, Intrusion, Technology, Legal, Russia.

Russia, and previously the Soviet Union, has long been recognised as a country involved in spying and intrusion on rival countries and organisations since the early 1900s. The Soviet Union employed spies in the Cold War to collect information and secrets about the United States of America and were previously used in World War One. This continues today but very different, as

specialised technology has been developed to hack and interfere with information, data and communications associated with their enemies.

Different technology enables different ways of gathering and collecting this information and data. This revolutionary technology allows for quick and effective hacking and intrusion, which is nearly impossible to stop when it is happening and difficult to detect who is responsible. It can be performed hundreds and thousands of miles from the intended target so the offender, or offenders, cannot be caught nearby or close to the crime. Most of the technology used for these activities worldwide was developed in Russia, enabling the Russian government and organisations to easily obtain this technology without having to travel overseas.

The Russian privacy law, the Personal Data Protection Act, is intended to protect the civil and privacy rights of the Russian people. This should be adhered to by the Russian government, but unfortunately it is not. Russia is a country that enjoys to spy on its own people and it has a mass surveillance system in operation to monitor its citizens every move and communications (Russia’s Spying Craze, 2013). The people of Russia are not happy with this as they should be given a right of privacy in their lives without having all their movements and phone calls monitored and recorded.

This document will describe cyber-attacks performed by Russia on other nations, and their severity. Technology created and developed by Russian companies that are used by the Russian government and organisations to interfere and hack confidential and private information or data on other countries and its own people, will also be explained. The law to protect the

privacy of Russian citizens will also be discussed and how it is side-stepped by the Russian government for their own convenience.

Russia is regarded as one of the most active and prevalent nations involved in espionage and intrusion. Cyber-espionage is employed by Russia to hack and obtain secret information from top departmental government agencies and buildings for their own intelligence. They are supposedly responsible for hacking and leaking emails from the Democratic National Committee (DNC) to WikiLeaks in 2016 and to have violated the network at the White House and the State Department activity (Penn-Hall, 2016). The gains and ease of these cyber-attacks on other nations, and because it is difficult to identify who is involved or responsible for the attacks, allows them to continue with this.

James Adams, the CEO and Co-Founder of Infrastructure Defense Inc. (iDefense), regards the Internet as a revolutionary system and declared that “ Cyberspace has become a new international battlefield” (Constantine, 2012). The internet has no governing body or police force, which is perfect for executing such attacks and not be detected. Each country must stand on their own or with their allies, to strengthen their cyber security and defences, and continuously fear that another nation may make a significant breakthrough that poses additional threats to them (Interviews, 2001). This makes each country cautious of new and severe attacks that they may not be able to defend or protect from.

Russia has been accused of organising cyber-attacks on many nations. Between 1998 and 2000, a succession of incidents and attacks on the US

became known as the Moonlight Maze. This was an attack on hundreds of government databases such as the Pentagon, NASA and other agencies by a group of hackers that used specialised computer equipment (Constantine, 2012). The attacks were apparently traced to a mainframe located in Russia, however, they denied this and the perpetrators are supposedly still unknown. Russia has also been accused of a 3-week long cyber-attack on Estonia in 2008. These attacks started when Russia and Estonia were in dispute over Estonia’s plans to remove a Soviet Union war memorial in the country’s capital Tallinn. This encouraged Russia to target some of Estonia’s biggest organisations and corporations such as the president, government ministers, political parties, news organisations and the banks. Russia again denied involvement with Kremlin spokesman Dmitry Peskov stating that “ no way could the state be involved in terrorism” (Thomas, 2009). Russia are not afraid to attack neighbouring countries, especially when they are much too powerful for lesser nations.

More recently in March 2017, two Russian spies were charged with breaching Yahoo in 2014. This was performed with two other computer hackers and it affected over half a billion user accounts. It is regarded as one of the largest data breaches to occur in the United States of America. The Department of Justice have previously charged Russian hackers related to cyber-crime, however this is the first time that a criminal case has been brought against Russian government officials (US charges two Russian spies, 2017). Despite these charges, this will not deter Russian government officials and organisations to ending these activities.

Many of the most common and most-used spy and intelligence technology employed today was developed in Russia. This technology was created from ideas the Soviet Union had to learn and uncover information and intelligence from other countries and from their own people. The Soviet Union wanted many ways of gathering knowledge and information in secrecy, so having various technologies to perform this, allowed to plan for every situation and scenario. One technology would be more useful than another in certain circumstances which prevented the attackers from being discovered and exposed. These technologies have only been developed from the late 1980s and upwards after the advancements in computers and other technology such as satellites and wired communication. The following will describe the technology used for collecting this information and data.

Voice recognition technology was developed by the Speech Technology Centre (STC) in the city of Saint Petersburg. STC’s beginnings started from a secret Soviet Union unit that had the backing of the Committee for State Security (KGB) and was developed during the Gulag system under Stalin’s rule. The roots of the company grew from a neighbouring prison that housed scientists and engineers, which was called the Sharashka Marfino. These scientists and engineers were forced to work to identify voices that were calling to foreign embassies in Moscow.

Speech Technology Centre has also started to develop face recognition technologies along with voice recognition. STC announced in December 2012 that it installed “ the world’s first biometric identification platform, at a nation-wide level, that combines voice and face identification capabilities”. This new system will allow authorities and governments to store images of

suspects and criminals on a large database. STC has also claimed that it has invented algorithms that “ deliver reliable results even when facial characteristics have undergone physical changes, and the system’s voice and face modalities can be used together or separately – a voice sample or facial image alone is sufficient to make an identification.” STC has publicly made it known that its surveillance technology is only used for utilitarianism uses, however they have been made available to strict and dictatorship government states such as Uzbekistan and Belarus. Most people will be unhappy with these developments as they fear that they will no longer have the right to privacy as their voice may be recorded without consent and that face recognition technology may mistakenly identify them for doing wrong.

Another Russian firm have developed a facial recognition app. This involves submitting photos into the app and the app then searches through Vkontakte, the Russian social network version of Facebook, to find a match for the photo. The app is believed to have a 70% accuracy rate (Russian facial recognition, 2016). While some have no issues with the release of the app, others have concerns about privacy and the potential disclosure of personal information. The company do not have their own privacy policy but they have produced an acceptable use policy and licensing agreement to use on their American customers. The acceptable use policy states that the app can only be used “ for lawful purposes” and the licensing agreement expects the licensee to establish their own privacy expectations (Chiel, 2016).

Intercepting and interfering with private communications by the law has different procedures and standards in Russia compared to other countries. MFI-Soft is a Russian company that develops information security and

telecommunications products for law enforcement agencies, voice over internet protocol (VoIP) carriers and internet service providers. The company has developed an interception technology capable of storing, detecting and analysing information that travels over the internet. The company also states that it develops products for national security and intelligence agencies and for the military. It is the largest Russian producer of telecommunications traffic interceptors and has developed a deep packet inspection filtering tool called Perimeter-F.

Russia has recently implemented a new law that states that companies must store data associated with Russian citizens on Russian soil. This law is an attempt by Russia to gain control of the internet and to eliminate all the data stored on Russian people from other countries. The authorities want superior access to online data by domestic security services and to reduce the access to the data by other countries. Multi-national companies such as Facebook and Google are not happy with this law as they would have to move massive data to servers within Russia borders and to inform Roskomnadzor, the Russian internet watchdog, about their location (Walker, 2015). This is a massive operation for multi-national companies to accomplish as Russia is a huge country with a population of well over 100 million people.

Russia has recently blocked LinkedIn because they didn’t comply with the new laws and didn’t store information about Russian people on servers inside Russia. Roskomnadzor had discovered that LinkedIn had broken their laws on storing data and acted accordingly. President Putin’s spokesman Peskov again said that the blockage is “ in strict accordance with the law” and that the Kremlin will not intervene or interfere with the banning of LinkedIn

(Matthew, 2016). Companies that do not adhere to Russian laws regarding data storage will be punished.

The traditional way of listening in on private incoming phone calls is done by monitoring the telecom operator. Due to the massive and continuous increase in mobile phone usage over the years, it is much simpler and effective to intercept phone calls there and then on the spot. Discovery Telecom Technologies (DTT) was established in Moscow and have developed a system that makes this possible. The company’s In-Between Interception System operates by imitating a mobile phone tower and draws in the signals that allows the device’s operator to secretly listen and record the phone call. It claims to have the Kremlin and the Federal Security Service of the Russian Federation (FSB) as some of its clients.

Some Russian people are evidently not happy with this surveillance. The Russian government were brought before the European Court of Human Rights because of their surveillance and interception of mobile phone communications in accordance with Article 8 of theEuropean Convention on Human Rights(See Appendix A). Roman Zakharov, complained that Russian law did not sufficiently protect against uncertainty and abuse from authorities and that it breached his right to privacy (European Court, 2016). Although this system was aimed at protecting the public and preventing crime, it did not guarantee protecting against abuse. The Court suggested that there was high risk with a system that had direct access to all mobile phone communications. The Court also believed that Russian law did not meet the “ quality of law” requirement and that it was not “ necessary in a democratic society” (Soldatov & Borogan, 2013).

The Russian government has introduced new laws and amended the Constitution in recent years because of espionage and intrusion, to lessen and prevent these problems in the future. Article 15, paragragh 4 of the Constitution of the Russian Federation outlines that “ universally-recognized norms of international law, and international treaties and agreements of the Russian Federation shall be a component part of its legal system” (Data Protection, 2016). This includes the ratification of the Strasbourg Convention for the Protection of Individuals regarding the Automatic Processing of Personal Data (ETS No. 108) by Russia in 2005.

The right to privacy, which includes the privacy of telephone and other communications is recognised in Article 23 of the Constitution, and the collection, use and storage of information about a person without their consent is prohibited in Article 24. The laws and requirements of data protection and privacy are outlined in the Federal Law No. 149-FZ on Information, Information Technologies and Data Protection and the Federal Law No. 152-FZ on Personal Data actions (Data Protection, 2016). These laws and articles of the Constitution are implemented to protect the public from the illegal collection of data and intrusion on their life. Individuals have the right to privacy and to only agree to this by giving consent for those.

The Russian government are happy to collect information and spy on the public and this was evident in 1995. The Law on Operative Search and Seizures was legalised that allowed the FSB to operate a legal interception system called SORM, which enabled authorities to receive information from internet providers and phone operators. This technology allowed the Russian Security Service to monitor emails, phone calls and internet searches.

Without consent and with improper use, the Russian people could fight for their right to privacy if they feel they are being violated against.

Other laws have been established and signed to protect against international intrusion and surveillance. The President of the Russian Federation, Vladimir Putin, signed the new Federal Law No. 374 on July 6, 2016, on “ Amending the Federal Law on Counter Terrorism and Select Legislative Acts of the Russian Federation Concerning the Creation of Additional Measures Aimed at Countering Terrorism and Protecting Public Safety”. This recently adopted law contains several conditions that specifically outline the rights of intelligence and secret services when observing private electronic communications and allows law enforcement agencies to collect “ individual computer information”.

The law describes the requirements about the identification of users and the safeguarding of metadata that is transmitted across networks by operators of telecommunication networks. This law works in parallel with the Federal Law on Information and Information Technology, which is an obligation of network operators, to “ keep metadata about all connections, transmissions, and receipts of voice information, written texts, images, sounds, video, and other messages transferred through communications networks” for three years.

Transmitted messages, telephone communication records and other communication information must be saved by network operators for up to six months. The law also enforces providers of information to report “ all information required for the description of received, transferred, or delivered

electronic communications” to the Federal Security Service. Failing to provide this information results in a fine (New Electronic Surveillance, 2017). The Russian government are introducing these laws to protect themselves and other agencies from repercussions and from legal action being taken. However, people can bring their case to the European Court if they feel they have been severely and wrongly victimised.

In 2012, Russian President Putin signed another bill into law regarding crimes by espionage and state treason. The Russian Federal Security Service (FSS) proposed the bill to highlight that espionage and revealing state secrets are a form of state treason. The FSS also wanted the new law to emphasise the need to prosecute people or organisations that are involved in helping international organisations engaged in antagonistic activities such as state treason. This new legislation covers the assistance given to an international organisation by a Russian national targeting the security of Russia, in addition to support given to a foreign country or organisation showing aggressive movements against Russia.

The support given to foreign countries or organisations that define state treason is explained in Article 2, paragraph 4 of the Law as “ financial, material, technical, advisory or any other support given to a foreign country or to international or foreign organizations engaged in activities against the security of the Russian Federation” (Federal Law No. 190-FZ). Another area of Federal Law No. 190-FZ has been amended to state that any person that gains knowledge of state secrets and discloses such information to a foreign or Russian organisation will be liable for such act, whereas before, it was only persons who had been entrusted with the information that would be

liable and prosecuted. This law has also established a new crime for anyone convicted of breaking this law, which may provide a prison term of up to four years or a fine. This new law covers illegal access to state secrets due to theft, violence and other methods. This punishment for this crime may be a prison term of between three to eight years if the person or people are convicted of using more specialised techniques of espionage (“ Espionage and State Treason”, 2017).

Russia will continue to spy on other nations and hack confidential information as they will constantly be paranoid and in fear that other countries and organisations are planning terrorism or other attacks against the state. They are also aware that enemy countries are engaged in spying and intrusion as most of the super power nations of the East and West are involved in this activity. Russia recognises that information is a valued asset, which needs to be protected, whether at peace or at war. When using this information and data correctly, the enemy can be beaten militarily and politically, and without having to occupy the country.

New laws will be introduced in the future and the Constitution will be amended as ambiguities will be exposed in Russian laws as an unhappy Russian society will continue to pursue their protection for civil and privacy rights. Also, large corporations, who can seek powerful legal advice will not be intimidated or afraid to stand against the Russian administration. In recent years, the ban on overseas companies and organisations from storing data about Russian people outside of Russia was introduced, however multi-national companies were causing no harm and only storing the data on databases for their own use. Russia just does not want this data in the hands

of other groups and organisations out of fear of the knowledge gained from others from this data.

“ Data is the new oil” was phrased by Clive Humby in 2006, a UK Mathematician and architect of Tesco’s Clubcard scheme (Data is the new oil, 2013), to highlight the massive use of technology and storage of data. Data and information collected legally and illegally is a powerful resource for government bodies and organisations. The increase in the use of technology and the internet has led to a growth in data stored online. For example, data uncovered may have been used to plan and prepare for organised attacks against the state, or for criminal gangs and groups to plan their own attacks. Technology used to collect this data will divide opinions, and if the technology is used unlawfully such as secretly collecting data about Russian people, it will cause discontent among the Russian public. This technology will clearly be a benefit for uncovering and capturing criminals but should not be used widespread to collect information on everybody. The Russian government needs to be careful about crossing this dividing line.

References

ComputerWeekly. 2017. Russian personal data law set to come into force despite fears. [ONLINE] Available at: http://www. computerweekly. com/feature/Russian-personal-data-law-set-to-come-into-force-despite-fears. [Accessed 19 February 2017].

Early Cold War Spies: The Espionage Trials That Shaped American Politics – Central Intelligence Agency. 2017. Early Cold War Spies: The Espionage Trials That Shaped American Politics – Central Intelligence Agency. [ONLINE]

Available at: https://www. cia. gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/intelligence-in-recent-public-literature. html. [Accessed 19 February 2017].

The Guardian. 2017. Spies, sleepers and hitmen: how the Soviet Union’s KGB never went away | World news | The Guardian. [ONLINE] Available at: https://www. theguardian. com/world/2014/nov/19/spies-spooks-hitmen-kgb-never-went-away-russia-putin. [Accessed 19 February 2017].

International Business Times UK. 2017. Russia gets new Putin-approved cybersecurity doctrine following cyberespionage attack fears. [ONLINE] Available at: http://www. ibtimes. co. uk/russia-gets-new-putin-approved-information-security-doctrine-following-cyberespionage-attack-fears-1595050. [Accessed 19 February 2017].

Roland Heickerö. 2010. Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations . [ONLINE] Available at: http://www. highseclabs. com/data/foir2970. pdf. [Accessed 19 February 2017].

Chapter 1. The Fundamentals of the Constitutional System | The Constitution of the Russian Federation. 2017. Chapter 1. The Fundamentals of the Constitutional System | The Constitution of the Russian Federation. [ONLINE] Available at: http://www. constitution. ru/en/10003000-02. htm. [Accessed 19 February 2017].

Dentons – Russia’s new anti-terrorist law . 2017. Dentons – Russia’s new anti-terrorist law . [ONLINE] Available at: http://www. dentons.

com/en/insights/alerts/2016/july/19/russias-new-anti-terrorist-law. [Accessed 19 February 2017].

Practical Law . 2017. Practical Law . [ONLINE] Available at: http://uk. practicallaw. com/2-502-2227#a594893. [Accessed 19 February 2017].

History Learning Site. 2017. Spies of the Cold War Era – History Learning Site. [ONLINE] Available at: http://www. historylearningsite. co. uk/modern-world-history-1918-to-1980/the-cold-war/spies-of-the-cold-war-era/. [Accessed 19 February 2017].

Fox News. 2017. Russian facial recognition app sparks interest, controversy | Fox News. [ONLINE] Available at: http://www. foxnews. com/tech/2016/12/14/russian-facial-recognition-app-sparks-interest-controversy. html. [Accessed 19 February 2017].

Fusion. net. 2017. Hyper-accurate face recognition tech goes global | Fusion. [ONLINE] Available at: http://fusion. net/story/358817/findface-ntechlab-face-recognition-privacy/. [Accessed 19 February 2017].

Mail Online. 2017. Moscow blocks LinkedIn because it does not store data on citizens on Russian servers | Daily Mail Online. [ONLINE] Available at: http://www. dailymail. co. uk/news/article-3946982/Moscow-blocks-LinkedIn-latest-clampdown-Internet-freedoms-does-not-store-data-country-s-citizens-Russian-based-servers. html. [Accessed 19 February 2017].

International Justice Resource Center. 2017. European Court: Russian Interception of Mobile Phone Communications Violates Convention | International Justice Resource Center. [ONLINE] Available at: http://www.

ijrcenter. org/2016/01/14/european-court-russian-interception-of-mobile-phone-communications-violates-convention/. [Accessed 19 February 2017].

WIRED: WIRED. 2017. 5 Russian-Made Surveillance Technologies Used in the West | WIRED. [ONLINE] Available at: https://www. wired. com/2013/05/russian-surveillance-technologies/. [Accessed 19 February 2017].

The Cipher Brief. 2017. Russia, China, and Cyber Espionage | The Cipher Brief. [ONLINE] Available at: https://www. thecipherbrief. com/article/tech/russia-china-and-cyber-espionage-1092. [Accessed 19 February 2017].

Interviews – James Adams | Hackers | FRONTLINE | PBS. 2017. Interviews – James Adams | Hackers | FRONTLINE | PBS. [ONLINE] Available at: http://www. pbs. org/wgbh/pages/frontline/shows/hackers/interviews/adams. html. [Accessed 19 February 2017].

Russia – Data Protection 2016 – ICLG – International Comparative Legal Guides. 2017. Russia – Data Protection 2016 · ICLG – International Comparative Legal Guides. [ONLINE] Available at: https://www. iclg. co. uk/practice-areas/data-protection/data-protection-2016/russia#chapterconte nt1. [Accessed 19 February 2017].

Russia: New Electronic Surveillance Rules | Global Legal Monitor. 2017. Russia: New Electronic Surveillance Rules | Global Legal Monitor. [ONLINE] Available at: http://www. loc. gov/law/foreign-news/article/russia-new-electronic-surveillance-rules/. [Accessed 19 February 2017].

Russia: Espionage and State Treason Concepts Revised | Global Legal Monitor. 2017. Russia: Espionage and State Treason Concepts Revised | Global Legal Monitor. [ONLINE] Available at: http://www. loc. gov/law/foreign-news/article/russia-espionage-and-state-treason-concepts-revised/. [Accessed 19 February 2017].

Inquiries Journal. 2017. Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat – Inquiries Journal. [ONLINE] Available at: https://www. inquiriesjournal. com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat. [Accessed 19 February 2017].

Timothy L. Thomas. 2008. Nation -State Cyber Strategies: Examples from China and Russia. [ONLINE] Available at: http://ctnsp. dodlive. mil/files/2014/03/Cyberpower-I-Chap-20. pdf. [Accessed 19 February 2017].

The Guardian. 2017. Russian data law fuels web surveillance fears | World news | The Guardian. [ONLINE] Available at: https://www. theguardian. com/world/2015/sep/01/russia-internet-privacy-laws-control-web. [Accessed 19 February 2017].

Russia’s Spying Craze. 2017. Russia’s Spying Craze. [ONLINE] Available at: https://themoscowtimes. com/articles/russias-spying-craze-29105. [Accessed 24 February 2017].

‘ Data is the new oil’: Tech giants may be huge, but nothing matches big data. 2017. ‘ Data is the new oi