Patriotic Hackers

Steven Wood

A thesis submitted in fulfilment of the requirements of the Manchester Metropolitan University for the degree of Master of Science (by Research)

2017

Faculty of Business and Law

Manchester Metropolitan University

Declaration

No portion of the work referred to in this dissertation has been submitted in support of an application of another degree or qualification of this or any other university or other Institute of learning.

Steven Wood

20/09/2017

Acknowledgements

I would like to thank Professor Dominic Medway for his boundless support and encouragement throughout my studies. I am also thankful to Robert Hegarty and Philip Scown for their backing to the project.

I am also indebted to the participants of my interview groups for giving up their time and sharing their knowledge and contribution to this research project.

I would also like to thank my wife, Jane, and my sons Harrison and Alexander for tolerating their husband and father throughout the whole process. Without their endless support, my studies would have come to naught.

Abstract

Patriotic hackers are a group who have not been widely studied. However, their presence in cyberspace during a conflict or crisis escalates matters and can have harmful consequences. Together with their use of advanced cyber weapons, the implications of their actions need to be better recognised and understood.

Utilising current academic and non-academic literature, alongside interviews with industry experts and the author's own field diary, this study aimed to critically evaluate the current use of patriotic hackers.

In conclusion, contributions to both theory and practice have been made. A theoretical model for patriotic hacking has been developed to aid further research. The advice offered to organisations is not to waste resources preparing for a patriotic hacker attack but rather to work with governments to more effectively respond. Additionally, it is recommended that new, international treaties are required to discourage the use of patriotic hackers, and to attempt to prevent cyber weapon proliferation. Such treaties are required to prevent escalation during crises and to secure the advantages that cyberspace offers to society.

Contents

1. Introduction

The world of the 21st Century is one that will be increasingly wired, with the domain of computer communication across the internet becoming paramount. Whilst many in developed economies may be familiar with using smartphones and tablets, the advent of the Internet of Things (IoT) means that connected devices will become even more commonplace throughout the entire world (Weissman, 2015; Eddy, 2015) . Cyber security has long been recognised as crucial by policymakers, industry and academics (UK Government, 2015). However, as people's fridges, televisions, cookers, heating systems and other household appliances become connected to the network, the scope of the cyber domain becomes that much greater. Additionally, warehouse equipment, office machines and factory devices are become connected to the internet in greater numbers. CNI (Critical National Infrastructure) which includes Nuclear Power Stations, Traffic Light Control Systems, Hospital Equipment, and the financial sector, etc. is exposed to this paradigm shift (Weissman, 2015; Eddy, 2015).

A survey for Business Intelligence in 2014 asked executives to answer questions about the Internet of Things (Weissman, 2015) and found that the greatest barrier to further investment is security. Whilst business executives were already concerned about disruptive and costly hacks, the general public was also becoming more concerned. The Dyn/Mirai attacks of late 2016 demonstrated why the public and policy makers should have concern (Etherington and Conger, 2016). Such attacks established that you do not have to own an IoT device to suffer the consequences of insecure devices. The scope for attack is increasing; the IoT market is expected to hit $7.3 trillion by 2017. In a survey by Trend Micro (Eddy, 2015), the majority of respondents thought their information would be sold by companies for unknown purposes. Despite this, Eddy (2015) confirms that a large majority said they would plan on continuing to use smartphones, tablets and smart home devices. This shows the conflict between ease-of-use and security concerns that is already present in the public. Additionally, the sensitivity of IoT data, e.g. medical devices, presence detection by thermostats etc. causes additional concern. Smartphone data is typically about the digital world, IoT data is about the physical world.

This cyber environment, especially via IoT, is growing larger and more complex as the century continues and gives hackers a broader landscape to operate in and target. However, society has been exposed to hacks since arguably 1903 when the first 'hack' took place (Marks, 2011). Criminal gangs have been using the internet for criminal behaviour since at least the 1990s, with the level of computer skills a key factor in their involvement in cybercrime (Sela-Shayovitz, 2012). One of their favoured attack methods is phishing; a social engineering method to get people to do something they should not – often initiated by an email (Mansfield-Devine, 2013). The number of phishing attacks made against the public has risen considerably and is now considered ubiquitous (Raether, 2008). One of the reasons given for this is that the human element in technology is considered to be the weakest link. There will always be a technical arms race between the attacker and the defender, but the human element remains constant and is therefore attractive to hackers (Mansfield-Devine, 2013).

Another form of online delinquency is hacking and is older than the internet. It has been found that low self-control and deviant peer associations can lead to hacking (Holt et al, 2012). However, when hacking is combined with political activism it becomes hacktivism - a portmanteau of hacking and activism. According to Denning (2015), hacktivism has now become commonplace and activists operate all over the globe; both in democratic societies and more authoritarian regimes. Denning (2015) states that hacktivism began in the late 1980s; antinuclear protesters in Australia launched a computer worm against NASA in 1989. By the mid-1990s, Distributed Denial of Service (DDoS) had been added to be hacktivists toolbox. This is where an attacker takes advantage of security

vulnerabilities to use an innocent partie's computer to attack another computer. The attacker can then force the computer to send spam to particular email addresses or to send large amounts of data to a website. The attack is "distributed" because the attacker is using multiple, distributed computers to instigate the denial-of-service attack (McDowell, 2009). Hacking has become very popular for activists and malware authors and/or crackers alike due to its lack of geographic boundaries, ease-of-use and the limited responses law enforcement agencies can react with (Denning, 2015).

A closely linked group, but with differing viewpoints, are the patriotic hackers who, when under greater organisation, can form what are called cyber militias. The type of warfare used by them is highly asymmetric. One definition of patriotic hackers is "…someone who, with the agreement of their government or without the agreement of their government, is carrying out malicious IT acts on behalf of their country" (respondent D from section 4.2). The rise of patriotic hackers has come later than that of hacktivists but, as opposed to hacktivism, is a poorly researched area (Dahan, 2013). It is this group that this study shall focus upon. However, the wider context of hacktivists, cyberwar and the law relating to it must also be discussed to place things in the correct context.

Against the backdrop of increased interconnectedness, the spectre of cyberwar, criminality and other forms of conflict rises. The general public is gradually becoming more aware of the importance of personal security on the web (Eddy, 2015); but is less likely to be aware of cyberwar and the actors involved in it, let alone the possible repercussions to themselves of such a conflict.

Cyberwar is "any virtual conflict initiated as a politically motivated attack on an enemy's computer and information systems" as given by the techopedia online dictionary. Giesen (2013: 66) pleads for a more restrictive definition with "Cyberwar… can only take place between two or more states". The codification of cyberwar is troubling for lawmakers and academics alike; its amorphous nature, hidden operatives and lack of respect for territorial boundaries make it challenging to define. Chayes (2015) attempts to pin down what constitutes a state act of aggression in cyberspace; in doing so they give credence to NATO's Tallinn Manual and its own attempts at definition. With the repercussions that may come to pass if a state was found to be responsible for a cyber attack, nations have found other ways to act in the use of proxies. Such proxies are often patriotic hackers.

The senior Whitehouse advisor, Richard Clarke, does not believe a cyberwar has happened yet, but he does believe its inevitable (Anon, 2016a). Meanwhile, NATO's Sarin Ducaru states that a cyberwar against one of its members does not automatically trigger Article 5 - the general NATO call-to-arms. However, he adds that any retaliation need not be constrained to cyberspace; it may involve a military response (Anon, 2016b).

The lag between new forms of cyber attack and relevant legal frameworks is another troubling aspect of cyberwar. Whilst lawmakers struggled to keep up, Giesen (2013) believes a superpower may be partially to blame. Giesen suggests that the USA is reluctant to agree new, multilateral agreements on cyberwar conduct due to its primacy in cyber offensive capability; his thinking is that the USA does not wish to constrain itself. The exploits of the Equation Group, believed to be part of the NSA (National Security Agency**)**, give this thinking some credence (Menn, 2015). What is clear is that some of the weapons developed to fight a cyberwar have leaked into the public domain, to the general detriment of society (Thomson, 2017).

1.1. Aim

The aim is to:

- Critically evaluate the current use of patriotic hacking

1.2. Objectives

The objectives are to:

- Analyse the current state of research into patriotic hacking
- Determine the toolkits and techniques the hackers use; highlighting the flaws, strengths and weaknesses
- Explain the perceived motivations of individuals involved in patriotic hacking
- Assess the effectiveness of patriotic hacking in cyber warfare
- Discuss the future role of patriotic hackers in cyber conflicts

1.3. Research impact on practice of management

It is expected that the impact of this research will be the improvement in awareness of patriotic hackers in the practice of management. The research, whilst providing rich insights, will give IT and security managers the opportunity to improve defences against the cyber weapons found during the research. An understanding of the tools and techniques used by hackers will also benefit the same managers by allowing them to better prepare defences. Theoretical knowledge on patriotic hackers will be increased and premises will be made with a view to defining concepts; this will aid further research.

2. Literature review

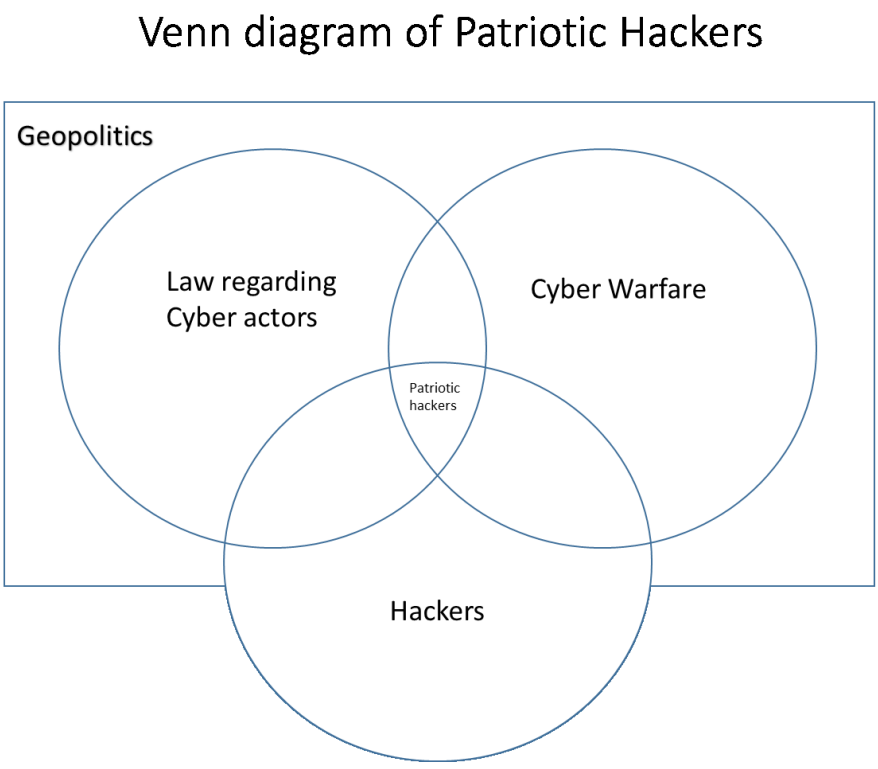
2.1. Introduction

The project undertook an extensive literature review to find any relevant reading on the subject of patriotic hacking. This review considered the potential limitations of a study into patriotic hacking, what research in the area needed to occur, and how much empirical evidence on the subject is already out there. The literature review utilised journal articles, books, conference papers, web blogs and other relevant discourses. The literature was critically evaluated, and a discussion made on areas for further research. The following issues were identified in respect of the research area:

- Confusion – i.e. contradictory evidence
- Neglect – i.e. little robust research
- Alternative perspectives – i.e. other scenarios which may have indirect relevance and/or implications for the subject of patriotic hacking

The aim places the literature review in the following context:

Figure 1 Venn diagram



2.2. Definitions and typology

Attempts have been made to document the different kinds of malfeasant behaviour that goes on in the web, with authors such as Ashenden (2011) stating the importance of doing so for public engagement.

Seebruck (2015) attempted a typology in a paper and gave the following: coders, hacktivists, cyber warriors, criminals, insiders, crowdsourcers, novices and punks. The latter two groups work on the web for recreation. The criminals operated for profit and the coders for prestige. Under the ideology

banner sat the hacktivists and cyber warriors. The final group were defined as operating for revenge and incorporated both the crowdsourcers and insiders.

Borghard and Lonergan (2016) define three types of non-state actors in the cyber domain: alliances, mercenaries and proxies. Alliances are defined here as associations between the state and a collection of individuals. Mercenaries are cyber warriors for hire. The final one, proxies, is where a state may pass cyber weapons to a group of non-state actors to act on their behalf politically.

Borghard and Lonergan's (2016) typology of proxies is shown in a table 1 below:

Table 1: Proxy typology

	Individuals or small, unorganised groups	**Organised groups**
Political ends	Patriotic hackers, hacktivists, cyber terrorists	Cyber armies or militias
Economic ends	Geeks	Criminal collectives

Additionally, but not shown above, 'moonlighters' may flit between each unit as and when the money dictates.

Denning (2000), argued that patriotic hacking is covering state on state conflict with the perpetrators of the cyber attacks being citizens and expatriates rather than governments. This definition implies that these acts only take place when a conflict or war between nation states is going on. Other authors regard this as too simplistic and believe that it can happen outside of a full conflict (Ottis, 2011).

Ottis (2011) has developed a model for classifying non-state actors in cyberspace. Three different kinds of models for volunteer based cyber militias are: the Forum, the Cell and the Hierarchy. They all have the ability to use cyber attacks in order to achieve political goals. The Forum can be considered an ad hoc militia who meet in an online place and assume roles in an upcoming campaign. Such roles could be trainer, malware provider, a temporary leader etc. It is easy to bring together and usually disbands once the immediate objective is gained.

The Cell is more organised, with individuals more likely to know each other whilst remaining anonymous to the outside world. The Cell moves in time with the ebb and flow of the associated conflict and can remain in place a long time. The set-up is resistant to infiltration as everyone knows one another but can be restricted on scalability. That is, there are only so many hackers with the necessary skills willing to perform politically minded attacks.

The Hierarchy is again more organised with a definite structural that is recognisable in traditional warfare models. There is a clear chain of command and it can be retained even in peacetime. They are, however, vulnerable to changes in public mood which may lead to curtailment of funding and possibly disbandment.

As one moves from Forum to Cell to Hierarchy the complexity, level of command and control, together with sophistication, increases. From a traditional military perspective, this seems desirable. However, with the increased command and control also comes less reactivity; the Hierarchy takes a lot longer to form than a simple structure like the Forum. It is likely that the Hierarchy model is the one most nation states would like their cyber militias to form yet, in principle, all three models could be used to support the cyber capability of the state (Ottis, 2011).

Authors sometimes conflate the terms hacktivists and patriotic hackers. This is true for Owens et al. (2009) themselves in their paper "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities". Denning (2015) also conflates them, whilst Borghard and Lonergan (2016) and Seebruck (2015) argue that they are very different kinds of cyber actor. Furthermore, Aschmann et al (2015) claims that patriotic hackers and online religious fanatics can be given the general term of cyber warrior. This is counter to other definitions by Denning (2015) and Borghard and Lonergan (2016) who do not conflate these two groups. Meanwhile, Kshetri (2013) fuses a definition of patriotic hackers with cyber criminals. He argues that, in China, many so-called patriotic hackers are motivated by financial gain. He adds that, if this is true, then they cannot be considered patriotic hackers but merely cyber criminals.

Patriotic hackers have ties of allegiance towards their home country (either nationality or ethnicity) and conduct cyber attacks against whom they perceive to be the enemy of their country (Barata, 2015). Such hackers often serve state interests despite having no official link with them, as President Putin has recently argued whilst discussing Russian hacker incursions into foreign elections (Hille, 2017). Putin was quoted as saying "…hackers are free people like artists" and that they were involved in a "… justified fight against those speaking ill of Russia". Barata (2015) argues that a patriotic hacker is one driven only by political ends rather than, for example, religious ones. Dahan (2013) defines them as parochial, self-identifying by their nationalism and patriotism, being to the right of the political spectrum and with little cohesive ideology. Worrying, Dahan (2013) also states that patriotic hackers set out with the intention to cause maximum damage in any conflict.

As can be seen above, there are multiple definitions of a patriotic hacker.

The definition of non-state actors, such as patriotic hackers, in the cyber world pose problems to easy characterisation. Initial United States thinking on non-state actors engaging in online conflict would have had them characterised as terrorists. This simple definition quickly breaks down when a detailed look at each of the actors online is made (Borghard and Lonergan, 2016). Russian mafia and Asian triad activity online is now recognised as being in the realm of cyber criminals, and not terrorist activity. Indeed hacktivists, patriotic hackers and other online activists who conduct activities online may be in breach of various laws and regulations; however, these do not fit easily under either under terrorist or criminal denominations. Some authors have tried to define the actors by their intended targets e.g. Critical National Infrastructure. Again this quickly becomes problematic, for example a lot of the critical infrastructure in advanced Western countries is privately owned. Is an attack against these an act of terrorism or an act of corporate espionage/ sabotage? Another problem with this approach is the fact that in kinetic warfare, critical infrastructure is often targeted and is regarded as an act of war, not of terrorism (Borghard and Lonergan, 2016). Kenny (2015) concurs that equating cybercrime, hacktivism or cyber warfare to cyber terrorism is not useful.

Robinson et al (2015) state that any comprehensive definition of cyberspace itself reflects its four constituent parts: it is an operational space, it is information based, it is a natural domain and its interconnectedness. Robinson et al (2015) further define it as a global domain within the information environment, using information technologies to exchange, exploit, modify, store and create information using the electromagnetic spectrum. This definition is adopted by this paper.

Cyberwar, and cyber warfare, are a commonly used terms in the mainstream media yet there are multiple definitions within literature. Alford (2001) defined cyberwar as something states engaged with to advance a national agenda and is executed against software controlling processes. However, this definition does not take into account religious beliefs or ideologies that are occasionally the aim

of modern warfare (Robinson et al, 2015). Another definition comes from Carr (2012) who contends that cyberwar is the art of fighting without fighting, with an aim of defeating an opponent with no blood spilt. This must be questioned on the basis that cyberwar can target CNI, which could lead to loss of life, as Colarik and Janczewski (2011) stress. A definition put forward by Cornish et al (2012) stated that cyberwar can be between states or between non-state actors and that its effects can be imprecise and unpredictable. This definition highlights the fact the actors such as patriotic hackers can be involved in cyberwar and that such a conflict may target elements other than that intended, with unforeseen consequences. Robinson et al (2015) give a simpler definition as "cyberwar occurs when a nation state declares war, and where only cyber warfare is used to fight the war". They segregate the terms cyberwar and cyber warfare, with the latter being able to be conducted without necessarily leading to full cyberwar. They also define cyberwar in a way that means as soon as kinetic force is used then it becomes a 'normal' war, not a cyberwar. Robinson et al's definition, rejecting that cyberwar and cyber warfare are synonyms, is one that we shall use.

2.3. Anonymous – prototypical hacktivists

Although hackers are often alone with their computers, they nonetheless habitually belong to larger communities (De ´cary-He ´tu et al, 2012). Anonymous is one such community and is an online anarchist collective that first emerged in 2003 on the website known as '4chan'. The group was set up as a discussion place for like-minded individuals to discuss means of online protest. Anonymous became more widely known in 2008 after an attack on the Church of Scientology. Typically, this hacktivist group came into being when a network of individuals with the same beliefs came together. They were driven by a sense of mischief and the culture of intervening in the affairs of other people (Olson, 2013). The path of individual activists coalescing into the collective "Anonymous" is described by Cavelty and Jaeger (2015) and contends that its creation and operation pose a threat to state power. One of the main aims of the collective appears to be challenging states' desire for unrestrained surveillance. Campaigns against surveillance are thus conducted and pose questions relating to a nation state's agency and legitimacy. This leads credence to the idea put forward by Olson (2013) that the collective was anarchist in nature.

While some individuals were politically minded, a lot more of the participants were simply cyber bullies, who wanted to waste an evening having fun at other people's expense (Olson, 2013). These divergent aims could never be fully reconciled within Anonymous. From Anonymous came a smaller group, LulzSec; according to Olson (2013) a less serious and more comedic chapter, and possibly an attempt to reconcile these differences. It should be noted though, jokey demeanour or not, that LulzSec went on to attack the USA's National Crime Agency and the FBI.

When a particular cause aroused interest, Anonymous discussed targets, their vulnerabilities and possible methods of attack (for an example, see figure 8 in section 5). Such methods of attack include DDoS, website defacement and the exfiltration/ leaking of sensitive or embarrassing information (Buchan, 2016). During the armed conflict between Israel and Hamas in 2014, Anonymous used cyber attacks against Israel. Their status, as civilians in an armed conflict, is a grey area in international law. It can be argued that Anonymous violated international humanitarian law by targeting civilian as well as military sites in Israel. This ambiguity could mean that civilian protest groups, organised online, could become targets for reprisals by a victim state's military. Whilst the Tallinn Manual suggest ways of dealing with this behaviour within international law, it is not binding and further work on codification of cyber conflict is urgently required (Denning, 2015).

Anonymous went on to attack PayPal, the CIA, Fox television and PlayStation network (Olson, 2013).

The main difference between hacktivists such as Anonymous and patriotic hackers is that the former are driven by the defence of a social issue (i.e. targets of their hacking activities are violating certain social issues) whereas the latter are driven by patriotic concern. Indeed, hacktivists often attack their own country if they believe they are violating a certain social issue (Barata, 2015). Hacktivists tend to be international and cosmopolitan in outlook and set out to do minimal damage with often humorous attacks (Dahan, 2013). They have been widely researched (Coleman, 2014; Parmy, 2013) and their methods, psychology and the effectiveness of their hacking activities have all been considered. Conversely, a patriotic hacker is more likely to be nationalistic and parochial. Patriotic hackers are usually volunteers (though some are coerced into action) who engage in Cyber activities on behalf of their nation state, with or without the state's tacit approval (Dahan, 2013; Kesan and Hayes, 2012; Ottis, 2010).

2.4. Cyberwar

Whilst the actions of criminals and disillusioned individuals is widely understood by the public, the online actions of nation states is less well understood. However, it has been widely studied by academics, lawmakers, humanitarian organisations and military theorists (Droege, 2013; Fisher, 2011; Pool, 2013; Barata, 2015). Chen (2010) has argued that the era of cyber warfare began with the advent of Stuxnet, a particularly sophisticated worm with a very specific choice of target. This target was a programmable logic controller made by Siemens and was significant as it was used in nuclear plants in Iran and, specifically, was part of the Uranium enrichment centrifuges.

Knopova and Knopova (2014) have stated that Stuxnet is one of the best examples of malware using a zero day vulnerability. The interesting side story is that the Siemens equipment was allegedly sold to the Iranians by the Italians on the black market in breach of the sanctions in place. It was compromised because it could, therefore, not be updated. A windows vulnerability was used, but the payload that targeted the Step7 software could only be developed by a complicit insider from Siemens, or someone in their supply chain. Additionally, Stuxnet was widely believed to have been initiated due to the efforts of the Equation group (Menn, 2015).

However, it also showed the problem of developing cyber weaponry such as Stuxnet. This worm was the product of the United States of America Equation Group and Israeli computer experts working together between 2005 and 2009, with a specific aim – that of targeting Iran's nuclear program. They did not plan on something that would spread chaotically all around the world, but one which would have a very clear target. In that aim they succeeded. However, Knopova and Knopova (2014) state that the development of this weapon led to variants of it i.e. the Flame, Gauss and DuQu malwares (Hejase et al, 2015) that damaged the USA's allies e.g. South Korean banks. This demonstrates the possible boomerang effect of cyber weapons. An additional example is the recent 'WannaCry' virus outbreak that has been alleged to have come from stolen Equation Group cyber weapons (Thomson, 2017). One author goes further by quoting a source who states that the Equation Group developed malwares were "100 per cent" the work of the USA's intelligence agencies (Fox-Brewster, 2015). The WannaCry virus was quickly followed up by the NotPetya ransomware outbreak, developed from similar code. Knopova and Knopova (2014) conclude that the new cyber weapons being developed represents a paradigm shift in warfare; they also conclude that a worldwide conflict between two countries with equally developed systems has not happened yet as the results would be grave and would therefore be very visible.

The notorious insecurity of the Internet of Things, combined with its widespread adoption, means a much wider scope for malicious actors in cyberspace to try and attack. With network controlled valves operating in the nuclear industry and on things like gas pipelines, respirators in hospitals and

switches on the electrical grid, the list of targets has never been so broad (Kesan, 2011). However, a more optimistic view is taken by some commentators, “Squirrels have taken down the power grid more times than hackers have, which is zero” (Scharf, 2015, p323). In a similar vein, Kenney (2015) contends that despite the concerns raised by the advent of Stuxnet and similar viruses/worms, the necessary skills and knowledge to exploit them and to take down a nation’s critical infrastructure, are not widely dispersed within the non-state cyber community. He explains that the real threat from terrorism online is in the ability to widely reach out to different communities and to attempt to recruit them using the web’s forté; instant communications over large geographical distances (Kenney, 2015). Scharf (2015, p325) comments that Stuxnet “may have been the first ethical weapon ever created” as it only ever targeted exactly what it was designed for with no risk of damaging similar equipment in places other than Iran. However, the fact that it was further developed into Flame and Gauss means this position is contentious.

After Stuxnet, four significant cyber attacks against nation states were recorded. These were against Estonia in 2007, Lithuania and Georgia in 2008 and Kazakhstan in 2009 (Henry et al., 2010; Hejase et al., 2015). It is significant that the cyber attack that took place in Estonia in 2007 involved patriotic hackers (Michael et al., 2010). The first of these, Estonia, can be considered as a leader in information technology, with a high percentage of the local population using the digital economy. Indeed, Estonia has been rated first out of 28 European countries for e-governance (anonymous, 2016a). The ex-president of Estonia, Toomas Ilves, however, recognises this as a double edged sword. With the population using things like a digital signature, which has proved very popular, and with the country’s infrastructure now hooked up to the network, this has meant that the country is open to disruption from a cyber attack. Indeed in the recent past, patriotic hackers from Russia have attacked the country’s infrastructure.

Cyber attacks are now thought to be commonplace (Michael et al, 2010) and range from many nuisance attacks to major disturbances that can threaten to destabilise nation states e.g. cyber attack on the Ukrainian power grid in January 2017. Additionally, during a cyber attack, digital information could be destroyed, exploited or corrupted and Rege (2014) gives this type of attack the denomination Digital Information Warfare.

Some of the key states with known cyber offensive capabilities include the United States of America, the United Kingdom, Russia, China, Bangladesh, North Korea, Pakistan, India, Syria and Iran (Tennant, 2009; Aschmann et al, 2015). They have been called cyber superpowers. However, cyber capability development are not just limited to these powers but to all modern countries of the globe. For example, Kostyuk (2014) debates the capabilities of the Czech Republic in dealing with any cyber attack. They conclude that smaller nations should cooperate more with their allies to defend themselves against cyber attack from the superpowers. However, it is not just smaller powers who are concerned. Americans, according to a poll conducted in 2014, were more afraid of cyber attack than North Korean or Iranian nuclear weapons, Chinese/Russian authoritarianism or climate change (Scharf, 2015).

Although Russia is considered heavily involved in cyber attacks (Henry et al., 2010) various authors also raise concern about China. The Economist (2013) maintains that China's current hacking armies are so brazen in their attacks that they simply do not care if they get caught. The conclusion is that there is no penalty from carrying out such attacks. This deduction is given extra weight by the work of Gutmann (2010). Certainly, companies and Non-Governmental Organisations (NGO’s) working in China are very careful not to directly criticise the Chinese Government; they do not want their operations curtailed by the state. It is believed that Chinese hackers have attacked Google, The International Olympic Committee, the World Anti-doping Agency and numerous environmental

NGOs (The Economist, 2013). Some hackers have declared that they have acted patriotically in conducting these attacks, however, The Economist (2013) states that the Chinese government is actually behind them. Their interpretation is that it certainly seems that having patriotic hackers fighting for you gives the government carte blanche to avoid international laws. One of China's first hacking groups (The Green Army) came to the attention of the Chinese police; yet instead of being shut down, the police utilised them for their expertise. It is now believed that the People's Liberation Army (PLA) have a cyber command and control department, PLA Unit 61398, which incorporates hundreds if not thousands of hackers (McMillan, 2013). The exact reason for the increased use of cyber attacks by the Chinese is not known, however, it can be extrapolated from recent events. The USA's use of technology in the war in Iraq has had a major impact on Chinese thinking; they now believe that the only way to win a future war between superpowers is if they establish information superiority (Thomas, 2008). Chinese digital assault on the West has given further credence by Gutmann (2010) in his paper describing the USA's attempts at moderating Chinese hacks. Operation Aurora, Chinese hacks of over 30 western companies during 2009, was put forward as evidence enough of Chinese intentions; conversely the USA's secret service hacks were not mentioned. Chinese control of patriotic hackers is an interesting side note mentioned by Gutmann (2010). However, there are at least two sides to this story; as of 2014, the USA was spending "up to 4 times as much on cyber offence than on cyber defence" (Scharf, 2015, p323).

The USA's and China's relationship with regard to cyberspace is of strategic importance; a great deal of tension has been generated by perceived actions in this domain (anonymous, 2016c). The main charge is that Americans think the Chinese are conducting industrial espionage using the Internet. Numerous security firms, such as Crowdstrike, have reported abundant incidents of espionage that can be traced back to hackers based in China. In the USA, during 2014, 97% of the Fortune 500 companies were aware that they'd been hacked – Scharf (2015) suggested that the remaining 3% had also been hacked but did not yet know it. Scharf also suggested that Initial thinking in Western countries was that China would not and could not be stopped from pursuing industrial espionage. However, Barack Obama's government in the United States challenged this assertion and began to make headway against Chinese hacking. They began this in 2013 by stating to the Chinese Premier that these continued hacks were damaging the bilateral relationship (Knake and Segal, 2016). Additionally, in 2014 the Federal Bureau of Investigation indicted five Chinese army hackers; this was seen as an attempt by the USA's government to ratchet up the attribution of any espionage. This was followed up in 2015 by the administration signing an executive order to allow for economic sanctions against companies benefiting from ill-gotten gains using cyber espionage. The Chinese government responded by agreeing to investigate cybercrimes at the behest of the USA's government (Knake and Segal, 2016). Following on from this for Chinese government also made similar agreements with other western countries such as the United Kingdom. Critics of the deals were sceptical that the Chinese government would cease its cyber activities; previous attempts at reining them in have come to naught (Knake and Segal, 2016).

It has been argued that China, since signing these deals, has attempted to downgrade its own cyber criminals. Whilst some cyber security companies have reported a decline in Chinese cyber attacks, e.g. FireEye, others were more sceptical. For example, Crowdstrike have not detected any appreciable slowdown in activity. With a new USA government now in place, commentators are concerned that China may backslide on previous agreements. Continued vigilance and engagement by the new administration would need to be enacted to increase the chances of China sticking to its commitments (Knake and Segal, 2016).

China's involvement in cyber espionage has also been forensically investigated. Informed sources now talk of a complicated ecosystem of cyber espionage which is multi-layered, highly distributed and difficult to unpick (Deibert and Rohozinski, 2010). Deibert and Rohozinski demonstrate that such systems require expertise and effort to be able to uncover where they originate from. They have shown that the theft of classified and sensitive documents from Indian officials and the office of the Dalai Lama can be traced back to the People's Republic of China. However, they caution that you can not necessarily infer that the Chinese government were behind such attacks, as the attackers' methods involve routing through various servers all over the world – it might still be someone other than the Chinese who launched the attack. Another finding was that Indian officials were compromised by actions taken in a visa office in Afghanistan; this demonstrates the complex nature of the information security challenge – it is without borders. While Chinese Government involvement cannot be ruled in or out, the findings do point to individuals residing in China and being active members of underground hacking communities (Deibert and Rohozinski, 2010).

In response to Western, and particularly the USA, political pressure China has attempted to change the narrative that it is in an irresponsible and dangerous hacker nation (Iasiello, 2016). One way it tried to do this was by arresting hackers that had been identified by the USA and, therefore, proving it could be a responsible partner inside cyber law enforcement. Iasiello (2016), however, suggests this is mere window dressing and is in fact part of China's 'Three Warfares' articulated in their 12th Five Year Plan. The three elements are legal, psychological and media manipulation. These were a bid to influence international relations and forestall any economic sanctions against them in response to their continued hacking. Iasiello's findings support the views expressed earlier by Mattice (2013) where Chinese hacking was considered the USA's greatest national security threat.

Gompert and Libicki (2014) stress that offensive cyber capabilities are inherently exacerbators of crisis instabilities around the globe. Their argument is based on cyber attacks being: short lived, difficult to duplicate, having ambiguity of results, an ambiguity of purpose and the ability to be initiated without senior political knowledge. They conclude that such properties are a particular concern with regard to the geopolitical instability between the USA and China.

Whilst the actions of China have been excising the USA and Indian governments in particular, military experts are troubled by how cyberwar will play out. Concerns over how future cyberwar may escalate, be terminated or may lead to kinetic warfare was expressed by Owens et al (2009). Historically, the USA has always sought to have dominance in military matters – but this is much harder to attain in cyberspace with nations beginning with a level playing field. Defending against cyber attack is challenging, with a wealth of targets available. As cyber attack is not constrained by geographical distances, defending all possible targets is problematic. In regular warfare you concentrate defence on the points closest to the enemy; in cyberspace everywhere is close to the enemy (Tennant, 2009).

In future conflict, it is anticipated that cyber armies will fight alongside kinetic forces as an integrated part of the military structure (Aschmann et al., 2015). Additionally, it is thought that both state and non-state actors will be present on the battlefield. There are various non-state cyber militias currently in active online service; examples include forces such as the Bangladesh cyber army and the K9 network cyber army (USA affiliated). Cyber armies will be expected to take part in both offensive and defensive action. Offensive action includes proactive and reactive offence using worms, viruses and other cyber weapons. Defensive roles include ensuring the internet security of key targets and running network scans etc. to try and spot hidden enemies (Aschmann et al 2015).

How cyberspace and the combatants within it fit into conventional military thinking has been puzzling military theorists for the past decade. Originally, and certainly in the United States, cyberspace was thought of as a physical domain, similar to the domains of air, space, land and sea (Butler, 2013). Butler also demonstrates that the thinking was that cyberspace would be co-opted into the Electro Magnetic Spectrum (EMS) and would therefore sit alongside radio waves, lasers and microwaves. This approach quickly ran into difficulties; for example, if radar is included then why not sonar? Military thinking in the United States has now moved away from attempting to neatly fit cyberspace into one of the existing domains. Current military thinking is that cyberspace is unique and the physical methods of Information Systems are superficial. Its logical and virtual nature are its defining characteristics. This is important for several reasons; it means that cyberspace with its own domain has become as important as an aspect of military thinking as more traditional, physical based domains. Secondly, the existing models of attack and defence (attack to be met by an organised defence) no longer exist. A cyber attack happens at the speed of light and organised defence against an attack in a reactive manner simply will not work. Organised defence can only have been done in advance of an attack. Everything else is retrospective and whilst not unimportant, e.g. a patching service to prevent a similar attack, it does not constitute a defence in kinetic terms. The unique nature of cyber warfare therefore means established methods of waging war do not apply; a new doctrine is needed for future cyber conflict (Butler, 2013).

Henry et al. (2010) hope that a framework for cyber deterrence is possible for the United States and its allies. They hope that these will promote greater cooperation internationally, and therefore prove a deterrent to cyber adversaries. Henry et al. (2010) and Kan (2013) maintain that improved cyber policies are essential to prevent a 'digital Pearl Harbour', i.e. a cyber attack having similar repercussions to the Pearl Harbour attack of 1941 that brought the USA into World War II.

It has been argued that, in contrast to conventional warfare, deterrence doesn't work very well in cyber warfare (anonymous, 2016d). The main reasons for this are, firstly, that every countries network is different, and proving an attack against country A does not necessarily mean that a similar attack could work against country B. Secondly, demonstrating your prowess by annihilating the cyber equivalent of an uninhabited Island is not possible (anonymous, 2016d). The possibility that cyber attacks may fail without being detected increases the likelihood of their use as precursors to kinetic conflict (Gompert and Libicki, 2014). An unnoticed, failed attack costs little; encouraging states to think of them as low risk weapons. The ex-leader of Estonia, however, believes that it is possible to have a credible cyber deterrent and cites the USA as an example of having this (anonymous, 2016a).

The abilities of cyber 'superpower' armies and possible constraining influences on them is much discussed by legal experts. A NATO manual (The Tallinn Manual) laying out the rules of engagement for cyber warfare, allied to the Geneva Convention, was prepared in 2009 (Schmitt, 2009). However, this document has not yet been adopted internationally (Aschmann et al, 2015).

In a recent interview with the assistant secretary general for security at NATO (Sorin Ducaru), it has emerged that cyberspace is now recognised by NATO as an independent operational domain in much the same way as land, sea and air (anonymous, 2016b). This recognition of the importance of cyberspace means that NATO can better manage the resources allocated to defend this domain. It also means NATO can now develop policy, doctrine and training whilst also pushing for international law to catch up on developments in cyberspace. The issue of activating Article 5 (an attack on one is an attack on all and all must come to the attacked nation's defence) is an interesting one and the assistant Secretary General would not confirm that a cyber attack would necessarily trigger it. They indicated that the specific political context of the attack would need to be taken into account in

much the same way that other forms of kinetic attack are. Thus, NATO's stance on cyber attack fits in with in its wider doctrine of its defensive mandate. There are no hints from the interview that the more aggressive, proactive or pre-emptive forms of cyber warfare was being contemplated e.g. using proxy forces.

Nonetheless, one of the particular challenges around attribution when cyber attack is to take place is the propensity for some states to use proxy forces e.g. patriotic hackers. Combined with current gaps in international law, this makes the use of proxy forces in cyber attack attractive to nation-states. Various frameworks have been suggested to try and assist with attribution. One of these frameworks suggests that there is a much narrower window for state-sponsored action than conventional wisdom implies (Cantil, 2016). It suggests that where the proxy forces are unskilled or broadly in opposition to the nation-state then their use as proxy forces is unlikely. Conversely, where proxy forces are either highly skilled or very supportive of the sponsoring state, then their use is much more attractive. The framework also suggest that states with unsophisticated cyber capabilities are more likely to engage with proxy forces to pursue a cyber campaign against an enemy. The author also argues that the use of such a framework would mean that fewer false positives in attribution would be made.

A final point, made by Scharf (2015), was that cyberwar is coming and, technologically speaking, nations will not always be able to defend themselves. Therefore, nations should focus on their citizens being psychologically resilient, so that individuals and organisations are prepared for when cyberwar occurs and defences are breached.

2.5. The law with regard to cyberwar

Pool (2013) states that whilst an applicable legal regime needs to be crafted for future cyberwars, the rules over what constitutes a cyber attack need first to be discussed internationally. Once the definition of a cyber attack is enshrined in international law, then a framework to govern future cyber conflicts can be made (Pool, 2013; Kirsch, 2012). Pool (2013) also establishes that Western democracies may find common ground with more authoritarian states when discussing an information war. However, other problems exist; the difficulty of attribution during a cyber attack (Pool, 2013; Sample, 2013) and the unknown consequences of such an attack. Addressing these problems will require International cooperation, possibly involving a global network that can easier pinpoint attack origins, and further treaties. They conclude that without developments in international law, the technology that has been such a boon to humanity may well end up being its bane (Pool, 2013).

Kesan (2011) and Kirsch (2012) argue that self-defence in cyberspace is a necessity and can be justified under existing laws. Kesan (2011) further suggests that counter-striking is also justifiable to protect critical infrastructure of both nation-states and corporations. Kesan and Kirsch add that to keep within the current laws, the principles of mitigation need to be followed. A DDoS attack originating from a 'zombie' botnet maybe one example where a mitigative counterstrike is permitted. However, Kesan (2011) recognised that innocent third-parties may be harmed when conducting such a strike. They ask that the legal foundations be solidified to provide cover for such actions, with liability rules provided to protect innocent third-parties.

With regard to irregular cyber forces and attribution, Barata (2015) argues that nation-states have some control over patriotic hackers. Conversely, Beech (2013) suggests that they often act without the knowledge of the nation they are protecting, which makes attribution problematic.

Additionally, Barata (2015) demonstrates in his paper the ambiguity within the United Nations Charters with respect to cyber attack and whether it is permissible or not. An example area in the Charter is in respect to the use of force and its comparison in normal kinetic warfare. How and when does a cyber attack bridge the threshold of the use of force? Consequently, Barata (2015) expects that patriotic hackers are often used to avoid international law. By allowing or empowering such hackers to attack an enemy, they can bypass the laws governing nation states. Barata (2015) also argues that the difference between unorganised individuals acting in a patriotic manner, and those that are state-sponsored, must be defined in law to help combat their use.

Moreover, as an example, the effects of the attacks against Estonia in 2007 were out of all proportion to the cause. The events that precipitated the crisis was the moving of Soviet war memorials. This minor action offended the sensibilities of Russian patriotic hackers, which led to serious repercussions for the country of Estonia (Kozlowski, 2014). Therefore, Barata (2015) suggests that there is an urgent necessity for cyber warfare to be legally regulated.

Questions arising from cyber conflict are fairly fundamental: what constitutes an attack? At what point are you allowed to use self-defence? And at what point does an attack fall under the United Nations Security Council, chapter VII (the sanction of military action to return peace)?

Chayes (2015) demonstrates that what some people call a cyber attack are in fact just forms of commercial espionage and therefore should not be a prelude to a full war. Repeated attacks on banks all over the world, combined with cyber attacks on state infrastructure e.g. nuclear power plants, are, however, blurring the lines between criminal activity and outright war (Chayes, 2015; Kan, 2013).

International law when applied to the cyber security space has been found to be limited and authors argue that it needs to be strengthened (Droege 2013; Kirsch, 2012). As a result, humanitarian organisations, such as the Red Cross, have become interested in cyber warfare and its effects upon civilians. Droege (2013) states that existing humanitarian law is not sufficient to protect civilians from the effects of cyber warfare. Droege (2013) then argues that when military and civilian infrastructure overlap and are not easily distinguishable, then one of the basic tenets of a just war, that of protecting the civilian population where possible, becomes difficult to do.

Chayes (2015) also illustrates the point that many governments are not willing to self-limit their own cyber attack potential as it may be too politically damaging to do so. This is given additional weight by the findings of Barnhill (2016), who concurs that there is a disincentive for those in power to accept cyberwar norms and their restraints. It may take a disaster in their own cyber sphere, possibly involving loss of life, before politicians feel compelled to act. However, nuclear arms control negotiations may be seen as a framework for getting cyber weapons agreement between the superpowers (Chayes, 2015). Torturous and long, international negotiations were needed to bring these treaties into being, and yet they prove that, with enough political will, superpowers will sign up to controlling weapons of global significance. Cyber weapons obviously fall into this categorisation (Chayes, 2015).

If such treaties follow the same path as the nuclear proliferation treaties then agreements between nation states on the reduction and control of cyber weapons will eventually emerge. This should prevent them falling into the hands of non-state actors e.g. terrorists, hacktivists and patriotic hackers (Chayes, 2015). Such treaties will take a long time to draft, gain agreement and ratify – but what can be done in the short term? Chayes (2015) suggests that, initially at least, a code of conduct between nations may help signal the shift in thinking about cyberwar and the weapons used in it.

Once enough nations sign up to this code of conduct, the direction of travel will become apparent to all and encourage more and more nations to sign up (Chayes, 2015). Denning (2015) further illustrates the challenges for international law as most cyber attacks fall below the required level of the use of force. A follow-up to the Tallinn Manual was proposed to help answer these challenges. However, the Tallinn manual was drafted by legal expert at the behest of NATO yet, when completed, NATO's most powerful member said they would not be bound by it; this was, of course, the USA (Scharf, 2015).

2.6. Patriotic hackers and cyber militias

Patriotic hackers have been mentioned in texts from the beginning of the century. Following the 2001 attack on the twin Trade towers, USA patriotic hackers defaced Arabic websites (anonymous, 2003). These attacks, however, were not welcomed by the state that they were defending i.e. the USA. Karatzogianni (2012) argues that forthcoming cyberwars will be waged principally by non-state actors e.g. hacktivists and patriotic hackers. To illustrate this, he points out that patriotic action by hackers has taken place in numerous incidents in the past two decades. Some of these incidents occured in the Middle East e.g. between Palestinian and Israeli hackers at the time of the Second Intifada (Dahan, 2013). Additionally, the Palestinian – Israeli conflict of 1999/2000 was conducted primarily by patriotic hackers from the two opposing sides and mirrored the unrest going on in the physical world (Allen, 2003). The two main types of attacks made in the conflict were DDoS and website defacement; typical tools used by patriotic hackers.

Other conflicts have even occurred between two superpowers, China and the USA. Two examples are the colliding military aircraft in 2001 and the accidental bombing of the Chinese embassy in Belgrade in 1999; following both incidents patriotic hackers attacked the cyber presence of the opposing countries (Owens et al., 2009).

There are both benefits and disbenefits to the use of proxy forces e.g. patriotic hackers, by nations inside conflicts. One of the chief benefits of them is that the state can act at a remove and therefore make it difficult for them to be a justifiable target of any retributive action. However, some of the dangers of using these actors in this way are that things can escalate beyond the state's control, and indeed, the cyber weapons may be turned upon the state themselves (Borghard and Lonergan, 2016).

In a discussion on hackers' effectiveness, Bibighaus (2015) argues that cyberwar is subject to Power-Law randomness and not the usual Gaussian distribution – this implies that outliers are much more important than the average. Thus, one especially gifted cyber warrior is worth far more than a thousand average ones. This has implications for patriotic hackers and their effectiveness; it is quality not quantity that matters.

The growth and capability of China's cyber capabilities has led to alarm in some of the USA's quarters. One report argues that cyber warfare is now integrated into the formal order of battle of the military forces of China (Henry et al, 2010). In addition to these formal institutions, China makes use of patriotic hackers. Henry et al (2010: 150) illustrate this with "most of the USA's serious computer incidents in 2007 were from Chinese patriotic hackers". They also noted that the Red Hacker Alliance counted 300,000 members back in 2006. Again, the lines between cybercrime and cyber warfare are blurred, with the state making use of patriotic hackers and cyber militias who are all too willing to fight for their country. In 2011, it was estimated that the cost of cyber security was around $200 billion a year for the United States alone (Fisher, 2011). The USA believe that a large number of these attacks originate from within China. Interestingly, it may also be a Pandora's box

that the Chinese government have opened by supporting the hackers - over 250 million people in China were victimised online by such groups in 2011/12 (Beech, 2013).

Patriotic hackers are occasionally used internally as well as externally. In Russia in 2012, contested local elections lead protesters to mobilise online. Patriotic hackers, with or without state sanction, launched cyber attacks against the protesting parties' online presence. These were resisted in part by the local Anonymous chapter, hence neatly showing the difference between hacktivists and patriotic hackers (Lysenko and Endicott-Popovsky, 2013). Additionally, whilst patriotic hackers are represented as the foot soldiers in a cyberwar, Anonymous and similar hacktivist groups are not fighting a war, but are in a perpetual struggle for hegemony (Barnard-Wills, 2011).

Another country involved in conflict, the Syrian government, is suspected of active support for patriotic hackers with the collection of cyber warriors known as the Syrian Electronic Army (SEA). Al-Rawi (2014, p427) stated that they are used by the Baath government of Syria as an "online public relations tool" to protect and further their own interests, using Cyber weapons provided by the state. Cyber weapons are relatively low cost and easy to use. This makes them very attractive to states and non-state actors for cyber conflicts. The patriotic hackers in Syria, called the SEA, are thought to be used to steal information from opposition groups, to launch website hacks and to generally try and cultivate an image of a sophisticated regime. Al-Rawi (2014) commented that their use would be similar in other totalitarian regimes, such as North Korea.

Another authoritarian country, China, has repeatedly stated that information superiority is required before any future kinetic conflict. As such, China has integrated cyber warfare into the People's liberation Army (PLA); it can also call upon thousands of patriotic hackers to assist in the cause (Chansoria, 2012).

Two hacker groups based in Russia have become well known and are considered Advanced Persistent Threats (APT's). They go by the denominations 'Cozy Bear' and 'Fancy Bear'; and both have been linked to Russia's highly capable intelligence services (Alperovitch, 2016). Crowdstrike, an internet security company, investigated these cyber actors when breaches were made to the USA's Democratic Party's files in 2016. Crowdstrike believes these cyber gangs are too sophisticated, with superb trade craft and excellent operational security, to not be part of a nation's state apparatus. The choice of target is telling as well, as the USA elections in 2016 were of high interest to the Russian state. The technique both groups used to infiltrate a network were based around spearphishing campaigns; this allowed a wide range of implants to be placed on the opponent's network. These include software called a RAT (Remote Access Tool) which utilises the HTTP protocol for command and control (Alperovitch, 2016). Whilst these two groups are closely linked to state security apparatus, they can be called patriotic hackers.

The motivation of patriotic hackers is not found within the literature with the exception of Dahan (2013) who states that they are willing to act criminally out of a sense of patriotism; he doesn't believe they have any manifesto or ethic beyond that of nationalism. Motivations for other hacker types, however, can be found. Jordan (1998; p768) commentated that hackers often acted out of boredom claiming that "…offline life is boring compare to the thrill of hacking". Jordan also suggested that curiosity and the thrill of the illicit were additional powerful motivations, whilst Holt and Kilger (2012) suggested that individuals must simply desire to express themselves online to have motivation to hack. Meanwhile, Steinmetz and Gerber (2015) suggest that concern for privacy laws is a possible motivator for some hackers.

2.7. Summary

The threat of cyber warfare has increased with the combination of the advent of the IoT, the failings of international laws and the increasing use of non-state actors as proxies for national forces. One of these proxies are patriotic hackers; not always controlled by their host nations and able to use current cyber weapons when affiliated more closely to the host's security apparatus. Direct studies about patriotic hackers are few and far between, Dahan (2013) being one notable exception. As such, the literature had to be studied to find more oblique references to them. It transpires that they are an emerging threat in cyberspace, which itself is becoming ever more widespread and important to society.

To summarise, patriotic hacking, as opposed to hacktivism, is a poorly researched area (Dahan, 2013), yet its importance to nation states (Deibert and Rohozinski, 2010) and the risk of further escalation means additional research would be valuable in assessing its impacts on future conflicts in cyberspace.

3. Methodology

3.1. Introduction

To ensure that the study could be repeated if needed a discussion of the techniques employed to fulfil the aims and objectives was necessary (Marshall, 2002). The selection of data collection methods depended on both the type of information required and the nature of the enquiry (Bell, 2006). The choice of a method is based on what type of information is sought, under what circumstances and from whom, agreed Robson (2006).

Various research methods were available, comprising of primary and secondary research areas, and these were analysed to ensure the correct methods were chosen. Two secondary research methods were considered relevant to the study; a literature review and cyber crime statistics gathered from the Internet. The literature review allowed the identification of relevant literature pertaining to previous, current and future work in the field whilst establishing the research need. The cyber crime statistics were gathered from the Federal Bureau of Investigation (FBI) and helped with context setting. Although some quantitative data was collected, the research project overall was focused on qualitative data collection.

Many different primary, or empirical, data collection methods were assessed. These consisted of interviews, questionnaires, focus groups, observations and feel diaries. The interview, observations and field diary research methods were chosen ahead of the questionnaires and focus groups. The latter two were discounted as they were deemed to be less relevant and useful to this particular project. It was felt that a focus group of hackers or cyber security experts would not be practical and using questionnaires would not elicit the detailed narrative that multiple, comprehensive interviews would.

An auto-ethnographic approach was taken throughout the project's course and this yielded the field diary; this recounted online and off-line interactions by the researcher with members of the hacker community and allowed interpretations to be translated. The individuals involved in these interactions were anonymised in these notes for purposes of their confidentiality. There were several methodological challenges in this netnography of accessing hackers on the Dark Web (a part of the Deep Web) and these are detailed in section 3.3.2.

3.2. Secondary research

It was necessary to establish current knowledge in the chosen field and leverage any other research pertinent to the study (Bell, 2006). Denscombe (2002: 54) concurs "the literature review paves the way for research". Blaxter et al (2002) comment that it forms a base from which a further study can arise. Blaxter et al (2002) also state that the literature review can ensure mistakes made previously can be avoided in any further study. The literature review also helped identify and clarify which research methods best supported the research aims (Davies, 2007). Additionally it was important to be critical of existing work when summarising so that values could transcend subject matter divisions, as noted by Blaxter et al (2002). Robson (2002) and Bell (2006) state the importance of precisely and clearly referencing any materials used. In the case of this research project, the Harvard referencing system was used.

To assist with context setting, secondary data was collected from the FBI via the IC3 (Internet Crime Complaints Centre) report for 2016. This is discussed in chapter 6.

Objective 1, analyse the current state of research into patriotic hacking, was achieved by conducting a thorough literature review. This was mostly achieved by using the information within academic

literature; however, this was supported by reviews of personal websites, blogs and some non-academic articles such as books and newspaper reports.

The other objectives were achieved by combining pertinent information from the literature review with collaborating information from the empirical data collection. Thus, the literature review only partially satisfied these objectives, though it remained an important part.

Where any conflicts arose between the primary and secondary research these were highlighted and discussed further.

3.3. Primary research

3.3.1. Interviews

Interviews are considered the 'gold standard' of qualitative research (Barbour, 2003) and can give both verbal and non-verbal in-depth information. They are considered 'gold standard' because the "elicitation of employee stories may give not only strategists and managers but also the employees telling their stories a deep, contextual, and particular understanding of organizational behaviour" (Kryger, 2017: 2). Fowler and Mangione (1990:11) describe an interview as a "conversation with a purpose" whilst Barbour (2013:132) describes them as an "intense exchange which is seldom seen outside therapy". This intensity allowed full and frank interviews to be held with the respondents which elicited interesting information. There are variations in how interviews are conducted, primarily around structure and technique. A successful interview depends on the selection of the correct structure (Fowler and Mangione, 1990). The simplicity of the interview is discussed by Kvale (1996), which implies speed, whilst Gillham (2000) argues that it can carry a heavy time penalty to fully plan, execute and analyse an in-depth interview. This planning of an interview must be carefully done to ensure appropriate information is gathered.

Barbour (2013:120) describe a semi-structured interview technique as "crucial as it refers to the capacity of interviews to elicit data on perspectives of salience" and Robson (2006) concurs. However, Gillham (2000) suggests that interviews need to be structured, otherwise a full disclosure of the anticipated data can be missed. Bell (2006) counters this by extoling the ability of a semi-structured interview in allowing the interviewer and interviewee to talk freely and in-depth. Barbour (2013) stresses that piloting of interviews can be effective in ensuring the correct questions are covered by each respondent. The thinking of Barbour (2013), Robson (2006) and Bell (2006) informed this study. Hence, a semi-structured interview approach was taken and used its first interview as a pilot. It then adjusted the topics for subsequent interviews.

Robson (2006) states that audio recording is particular effective for interviews; it allows the interviewer to fully concentrate on the subject whilst ensuring transcription errors are kept to a minimum. It was therefore decided to audio record each interview in this study, with the agreement of each interviewee having been given.

The interview participants were chosen to ensure that they could give insight to the subject matter, whilst also being available when required – their backgrounds are covered in section 4.1. Random sampling was not used as the research was generalising to a theory not a population.

Semi-structured interviews were carried out between February and May 2017 with four respondents. Two of these interviews were done face-to-face, the other two over the telephone. All were recorded by an audio device. The background of the respondents is shown in table 2 in chapter 4.1. Two of the participants were informally approach by the researcher; they were known to the author due to his previous work in cyber security. The other two became available after following

leads from one of the initial participants i.e. snowball sampling. Snowball sampling uses the method where participants' referrals to new prospects add value as the trust and obligation relationship between the identified person and the referrer means a suitable candidate is more likely to be found (Noy, 2008). It is, however, liable to various forms of bias which need to be carefully mitigated. The key bias of associating with very similar people needs to be recognised when using this method. Prior to each interview, the respondents were given an interview consent form, a list of themes for conversation and a participant information form. These can be found in appendices V, VII and VIII respectively. Whilst the respondents were given a list of starter themes, it was emphasised that it was just a guide and additional topics of interest was actively encouraged.

3.3.2. Field diaries

The act of researching intimate moments in partakers' lives can be challenging for academics who seek to understand hard to reach groups, such as hackers (Alaszewski, 2006). To counter this, social researchers have encouraged the idea of field diaries as a method for recording the events of daily life (Harvey, 2011). Diaries can collect qualitative data as part of a multi-method approach, in this research case alongside interviews. Additionally, field diaries can be used to provide additional insight and context to a study (Barbour, 2013). Whether they are unstructured or structured, they can provide additional topics to explore during the interview process.

For the purposes of this study, a field diary was kept using an auto-ethnographic approach. This comprised online and offline interactions by the researcher with members of the hacker community. The individuals involved in these interactions were anonymized in these notes for purposes of their confidentiality. The field diary comprised:

- Personal reflections on the process of data collection, including the requirements to obtain computer hardware and software to engage in online research without leaving trace of search histories or cookies, which is something familiar to those within the hacker community.
- Post-fieldwork reflections

The keeping of a field diary allowed the research to record explorations on the Dark Web. To minimise avoidable exposure whilst doing this the following methodology was used:

A second-hand Lenovo ThinkPad x230 was purchased to communicate with the hacker community. To improve the author's privacy, laptop settings were changed; the web camera was disabled and a piece of black masking tape put over the camera lens; a general password was set up for the machine; the existing SIM card was removed; location services were disabled.

Additionally, new software was added to the machine to provide a virtual environment to communicate within. This utilised VMWare technology to create a virtual machine, and then used TAILS software (The Amnesiac Incognito Live System).

TAILS is designed to help preserve anonymity whilst traversing the Internet; it leaves no trace of your presence. It is free software, based on Debian GNU/Linux and utilises the TOR (The Onion Router) anonymity network. The Dark Web is a part of the Internet that cannot be accessed by mainstream software - this is why TOR is used. Onion routing was prototyped by the USA Navy in 1998, although the project began many years before that. The project had been funded by the United States Department of Defence Advanced Research Projects Agency (DARPA) in an effort to allow computers to send and receive information over the Internet whilst remaining anonymous (Haraty and Zantout, 2014). Its ease of use and protection against strong and weak attacks has made TOR (The Onion Router) one of the main methods of accessing the Dark Web. However, there are numerous

disadvantages to using it; one of the key ones which is the increased latency whilst using it. This hinders any research done over TOR by increasing the time requirements to use it effectively (Haraty and Zantout, 2014).

The Dark Web includes hidden sites that end in .onion or other top level domain names that are only available through modified browsers and specialist software. Additionally, those running websites ending in .onion are able to hide their identities and locations from most Internet users. It is often the case that a visitor to an onion site will not know the identity of the host; conversely the host will not know the identity of the visitor (Raether, 2008). This is very different from the mainstream Internet where identities are closely managed and tracked via cookies, IP addresses etc. These technical conditions offer additional challenges to an ethnographic method. The Dark Web has its own privacy policy which can be summarised by saying that in order to protect everyone's privacy you have to protect your own. This means that you cannot use personal emails, real names or specific locations. It also implies that when you are communicating with people on the Dark Web you may not know their name, age, location or gender (Raether, 2008).

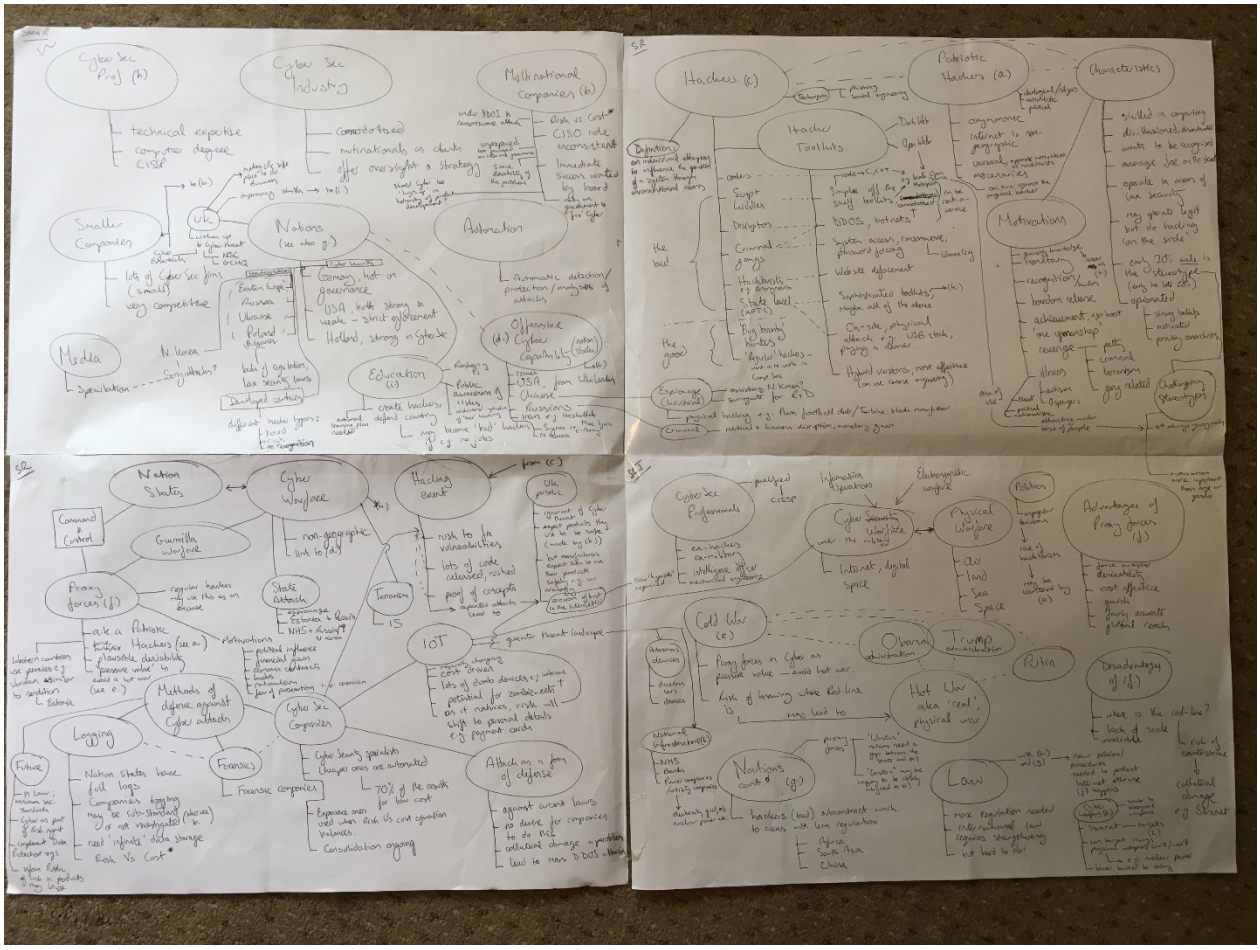
This method of connecting privately to the Internet is widely used by both the underground community of the Dark Web and, routinely, by law enforcement agencies e.g. Greater Manchester Police's cyber unit.

These measures were taken to eliminate avoidable exposure and minimise the risk to the author, their machine and anyone hosting the Internet connection. The identified risk was from disaffected hackers or any misguided law enforcement agency, either of whom may target the author's machine due to some perceived infringement (Raether, 2008).

3.3.3. Thematic analysis

Data from interview transcripts, and the field diary was all treated as text, and analysed thematically. Consistent with the approaches of Abdallah and Langley (2014) and Heracleous (2006), the researcher began from a position of viewing the data as text (interview transcripts and field notes). The researcher and an assistant independently reviewed this data, noting points of interest and key observations. Following the tenets of confirmability testing and inter-coder reliability (Campbell et al, 2013) the researcher reviewed their independent data interpretations and those of the assistant collectively, thus allowing key themes to be aggregated and to emerge via an iterative and inductive negotiation.

An example of how the draft appeared is shown below and demonstrates how the themes were laid out and linked together:



3.4. Limitations

Issues regarding interview structure, data reporting and analysis need to be considered when undertaking semi-structured interviews. These considerations need to be agreed at an early-stage to ensure accurate information is collected (Kvale, 1996). Whilst the structure of the interview allows for additional questions, Robson (2002) stresses that the interviewer needs to have a clear idea of what needs further probing; this can be difficult for inexperienced researchers. The semi-structured interviews key strength is it flexibility; however, this can cause data quality variations due to this very components lack of standardisation (Fowler and Mangione, 1990). Robson (2002:274) states that you "should listen more than you speak" to avoid what Gillam (2000) describes as the possibility of the interviewer not being attentive enough during the interview. An underlying limitation of interviews is commented on by Barbour (2013:132), "even when two researchers employ the same interview schedule the data produced may vary".

The use of field diaries is relatively infrequent within qualitative research and they "tend to focus on individuals' experiences" (Barbour, 2013:173). It may be more useful to use them to provide contextual detail and this needed to be considered at the onset of this study.

3.5. Ethics

With the absence of any formal interview with a current hacker, the sensitivity of the study was lowered. Interview respondents were able to give informed consent for their input to be included in the report and the subjects broached were not deemed delicate. Nonetheless, reasonable steps

were still taken with the respondents not being identified in the report; they were also given participant information sheet and consent forms. These were all returned by the respondents with their approvals. Although a security sensitive category was touched on, terrorism, it was not the main focus of the study and minimal references to it were made.

Again, the lack of access to hackers when attempting to contact them via the Dark Web meant that thorny issues of anonymity for the hackers and the researcher whilst being as transparent as possible did not have to be grasped.

An ethical aspect of a study that needed to be considered was the safety of the researcher whilst conducting research via the Dark Web. To this end various steps were taken and are detailed as per section 3.3.2.

3.6. Summary

Several methodologies were employed during the study to achieve the aims and objectives of the project. The utilisation of a literature review, interviews and field diaries created a multimethod approach that Bell (2006) calls 'triangulation'. This allows for a fuller and more balanced study. Denscombe (2003) concurs and adds that a multimethod approach can allow contrast as well as complementing the data. Both Bell (2006) and Denscombe (2003) state that individual methods have their own limitations and the analysis needs to take this into account as these are not ameliorated by the multimethod approach. Critical thinking was used to mitigate these limitations by ensuring non-concurring viewpoints were given due regard. To reduce bias multiple investigators were used to thematically analyse the information gathered.

Primary data was collected using semi-structured interviews and field diaries. The participants in the former were selected according to the criteria set out in section 3.1.

Secondary data was obtained via a literature review of both academic and non-academic publications as described in section 3.2 and comparisons made with both conflicting and supporting literature.

After data collection, the data was analysed and discussed using an iterative tabulation; this is covered in chapter 6.

4. Report of interviews

4.1. Background of respondents

The four respondents were chosen based on their:

- Experience in cyber security
- Actively practising as cyber security professionals
- Willingness to participate
- Availability

All four are working currently as professionals in cyber security and have been for at least the last three years. One had come from the United Kingdom Armed Forces, one had links to GCHQ, one had a mechanical engineering background and the other had moved through various IT roles to get to his current position. As an aside, all are white males from the United Kingdom who are in the age range 30 to 50. Two of the four explain their interest in computers and programming from an early age. All had commercial cyber security resumes and one is currently practising at a UK university. Three of the respondents worked as consultants (pre-and post-sales), one as an IT contractor. They had various relevant qualifications, typified by the Certified Information System Security Professional (CISSP) certification.

Table 2: Summary of the respondents

Respondent	Age	Gender	Nationality	Current Role	Differentiating experience
A	31 – 40	Male	UK	cyber security consultant	GCHQ
B	41 - 50	Male	UK	cyber security consultant	UK Armed Forces
C	41 - 50	Male	UK	cyber security consultant	Information Security
D	41 - 50	Male	UK	cyber security contractor	IT Architect

4.2. Report of interviews

The interviews were conducted in accordance with the methodology discussed in chapter 3.3.1 and were all conducted between February and May 2017.

Respondent A attempted a hacker definition "…an individual attempting to influence through unconventional means the operation of the system". There was consensus amongst the respondents that there were different types of hackers and that they could be represented as follows:

i. Coders
ii. Script kiddies
iii. Disruptors
iv. Criminal gangs
v. Hacktivists
vi. State-level / APT's
vii. 'Bug bounty' hunters
viii. 'Regular' hackers

The latter two were considered to be 'good guys'; bug hunters would try and nullify malicious code whilst regular hackers are hacking for knowledge gain and may be beneficial to society. It should be noted that none of the respondents volunteered patriotic hackers as a type. When pressed on this respondent D offered a definition "…someone who, with the agreement of their government or without the agreement of their government, is carrying out malicious IT acts on behalf of their country". In contrast, respondent A called out the concept as "unusual" and as "a bit of an oxymoron". When the interviewer equated patriotic hackers with proxy force hackers respondent C became more enthusiastic about the concept and stated their motivations as "kudos, I helped my country, I targeted my enemy, I help take down the enemy website". Respondent B took the concept and developed it further "…with patriotic hackers there will be an ideological, national and political motivation". He also commented that the patriotic hackers may as much be about targeting someone they do not like and were using nationalism as an excuse for their action. On the comparison between patriotic hackers and hacktivists, respondent D noted that they were "…the same thing … their motivation goes into different directions". On the subject of hacking motivation, the below list was compiled from the combined responses:

I. Knowledge gain
II. Monetary gain
III. Recognition and kudos
IV. Boredom release
V. Achievement
VI. Revenge
VII. One-upmanship
VIII. Illness
IX. Being coerced
X. Political and ideological
XI. Nationalistic

The respondents felt that the **highlighted** items above were the key motivations for patriotic hackers. The motivations were closely linked to the characteristics of hackers. The combined thoughts of the respondents could be split into the person and the space they operate in. An example of the latter is that "…hackers (sic) operate in areas that (sic) lacks security". The former could be represented by the following quotes "disenchanted", "opinionated" and "twentysomething male". However, this last example led to a challenging of this stereotype by more than one respondent. They argued that the ease-of-use of new cyber toolkits attracted a wider base of people into hacking and this stereotypical view no longer prevailed.

The new, easy to use cyber toolkits were another key feature of the discussions. It was stressed by multiple respondents that you no longer need to be a coder (skilled) to cause cyber disruption. Tools such as Kali and Metasploit are widely available, and not just on the Dark Web, and these give unskilled users the ability to conduct hacks.

These unskilled individuals ("script kiddies" as respondent C called them) were the foot soldiers in conflicts in cyberspace. The more advanced actors were "…coders with a massive amount of skill", according to respondent D, and were the individuals responsible for writing code using, for example, C++. This code would form the basis of ransomware, systems access, password forcing and other viruses. Respondent A went into some detail on physical IT attacks with "…a security guard that goes for a cuppa at 3:57 on Friday afternoon" leaving an organisation vulnerable to a virus infection via a USB stick. This demonstrates that organisations are vulnerable to both Internet led cyber attacks and on site led cyber attacks. However, the latter is only a viable option to those with the time and

resources to conduct it i.e. state led. Respondent A refers to this physical security as the “soft underbelly” of organisations who otherwise feel secure with “…a great solution for the web front-end, hosted in a nice managed space, completely disjointed from their internal infrastructure”.

The larger organisations, which include multinational companies, had begun to recognise the risk posed by cyberspace (respondent A talks about “board awareness”) by appointing CISO’s (Chief Information Security Officer). However, the costs imposed by becoming more secure in cyberspace have caused some to have “…almost a deniability that it's even a problem” (respondent B). Of course, commercial companies act on a risk versus cost matrix in their decisions but respondents also highlighted their unpreparedness, their focus on internal governance and their boards push for immediate answers, to the detriment of cyber security.

A lot of these companies use automation software to defend themselves but respondent A recognised it is still took humans to analyse the output and “… humans in the process is never going to be perfect”. It was used as one of the justifications for cyber security consultancy, which respondent A was employed in. When the same respondent was queried about a state-level attack (patriotic hackers acting as a proxy force) he was blunt “…if you’re in the attack category for those then you’re going to get got no matter what”.

An area of concern of the respondents was the development of the Internet of Things (IoT) by multiple, global companies. Respondent A said it was “…taking us back to 1991” with a large number of cost led devices whose cyber security was neglected. He was concerned with the volume of these devices initially, but thought it would pose a different challenge as their intelligence improved. The “…much greater threat landscape” was a concern to respondent B. Similarly, the problem of having a “…botnet of 10 million WebCams” was excising respondent D. However, he was also optimistic about the developments industry could make with IoT and that bad practice would be exposed. The respondents discussed how repeated hacking events, combined with the shift to personal attacks via IoT devices, would lead to “…an erosion of trust in IT”. Respondent D reasoned that this erosion of trust now extended to the Internet use of hyperlinks. He also believed security was key to building trust back up and companies may have to offer guarantees in the same way banks do when using their debit cards. Otherwise, he argued, “…that raw principal <hyperlinks> that the Internet was based on is now too dangerous to use”.

The defences that organisations or larger companies were primarily around forensics, logging, internal governance and the use of automation software. Respondent A was concerned about companies logging of data saying that “…a lot of businesses, the logging isn't up to standard or isn’t looked at”. The same respondent was scathing of any push to use attack as a form of defence for companies or organisations.

With regard to the future of defence against cyber attack, respondent B argued for a “…baseline in law on a minimum security standard” and also a law stipulating that cyber security had to be within risk management. The same respondent wanted to also see new cyber security regulations to complement existing data protection regulations. Respondent C wanted companies to inform the public of any risks in the products they buy with regard to cyber security. In terms of company responsibilities versus the governments, the same respondent wanted companies to take some responsibility for protecting their assets whilst recognising that the government, specifically the U.K.'s, has a lot of capability to assist.

The role of nation states was discussed by all respondents in terms of defensive and offensive capabilities. From the former subject, Germany was recognised as being “…hot on governance” by

respondent A who also cited the Dutch as having "…very good specialist skills". The UK government's belated but robust moves on creating greater cyber capability in defence was heralded by respondent B.

An area of importance for governments, according to the respondents, was national infrastructure. Respondent D included TV stations, power stations, water networks and health institutions as being vulnerable national infrastructure. He was also concerned that developed countries' reliance on IT left such infrastructure vulnerable.

Responding to a question on how the UK was set to defend against such attacks, respondent C stated they were optimistic that the next generation would have better skills in cyber security. He stressed how "… kids were now interested again" in how computers work rather than just being consumers of it.

Discussions were also directed to the capability of nations in offensive cyber terms. The combined view was that the following were very capable;

I. USA
II. Israel
III. China
IV. Russia
V. Iran
VI. Syria
VII. North Korea

It should be noted that none of the respondents placed the UK explicitly in that list. However, respondent B did mention UK and proxy forces whilst talking about the comparisons to rendition. The respondents generally better understood the term "proxy force" in preference to "patriotic hackers", and this was therefore used by the interviewer to ease comprehension. The use of such forces by nation states was raised by respondent B. He said that the following were involved "…Russia, Iran, Syrian groups, North Korea, China" though he admitted the latter would find it high risk. The differences between Russia and China hacking was explained by respondent C. He believed the latter were more interested in industrial espionage, giving three examples in industry of China hacking the UK for industrial gain. These examples were at a premier football club, a wind turbine manufacturer and a wave machine manufacturer. The latter two went into administration as a result. However, "…Russia is different" and is about "…causing political disruption and business disruption". In comparison, western countries would find it hard to use proxy forces due to the many restrictions in place. One way this could happen, though, was to use other countries to do the work for them, which is where the comparisons to rendition came in.

The advantages of using proxy forces for cyber warfare were discussed and their combined responses can be summed up by:

I. Plausible deniability
II. Cost-effective
III. Quick to stand up
IV. Force multipliers
V. Global reach
VI. Accuracy

Respondent D also stated that when hacktivism occurs in response to unpopular political decisions, patriotic hackers could be used to counter them. The cons of using them also came up. Respondent B commented that they opened up the nation to the risk of counterstrike, they had a certain lack of scale and "…you will probably lose control at some point". The same respondent also described how counterstrikes could get out of hand and a 'cold cyberwar' could become "…less proxy and more actual". The transition from an Obama lead USA administration to a Trump one worried the respondent in this context. However, they also countered this by saying proxy forces can be used as "safety valves" to release international tensions and this was better than fighting another "Vietnam".

Terrorism in the context of cyber warfare was touched on by the respondents; respondent B explicitly mentioned Hezbollah as using proxy forces for cyber warfare. However, respondent C also commented that terrorist groups, such as Islamic state, were the targets of hackers themselves with the example of Anonymous stopping them showing homophobic videos.

The subject of cyber weapons and in particular Stuxnet, was raised by three of the respondents. The Israelis and Americans were implicated in its creation and its target was Iranians nuclear processing plant machinery. Respondent D called it a "fairly slow burn weapon" and stated that such weapons could be used to target systems that physical weapons would not. Respondent B argued that Stuxnet eventually found its way back to the west, attacking targets it hadn't been intended to. This con was counted by respondent's D view by the pros "they are very powerful weapons" and "…the barrier to entry is so much lower than conventional weapons". He went on to say that this allowed countries with low resources to arm themselves with such weapons. Overall, cyber weapons were likened to their biological equivalents in warfare; cheap, easy to use but with the potential for deadly blowback on the users.

Respondent B turned their attention to the law in relation to cyber warfare and felt that new laws were required, both in the UK and internationally. However, he stressed that the latter would be "…futile absolutely futile", seeing it as "…too difficult and too complex" to achieve.

Finally, responded B talked about how cyber had become a new domain in the UK Armed Forces, sitting alongside the more traditional domains of air, land, sea and space. He compared this to the commercial world where it was called "the digital space". He added that proxy forces would have an increased role in cyber warfare going forward.

4.3. Summary

This chapter drew out the salient points from the four interviews with cyber security professionals. The main findings were that patriotic hackers were better known as proxy force hackers; that their characteristics and motivations were wide and varied; that their use by nation states were growing; and that the risk of cyberwar, due to the use of such actors, was real and present.

The respondents helped, in part, to define the toolkits and techniques that hackers use, which is one of the key objectives of the study. Respondents A, C and D all gave valuable insight on the toolkits and techniques used, whilst also giving some depth to how the threat landscape was changing.

In assessing the effective effectiveness of patriotic hackers in cyber warfare, another objective, respondent B was best placed to answer due to his role in cyber warfare for the UK Armed Forces. He laid out some of the shortcomings in using patriotic hackers, highlighting the possible loss of control when trying to field them and the risk of leaving yourself open to counterstrike.

All four respondents contributed to explaining the perceived motivations of patriotic hackers, thus helping to satisfy another of the studies objectives. This was invaluable as finding this in the literature was elusive. Respondent B summed up their motivations as ideological, national and political whilst respondent D gave an interesting comparison between patriotic hackers and hacktivists, arguing that they were the essentially same thing only with different motivations.

Knowledge of the future role of patriotic hackers in cyber warfare appear to be limited; only respondent B touched on this. This could be down to their professional careers with only respondent B being involved in cyber capabilities from a military perspective. The others dealings with patriotic hackers could be surmised as being on the receiving end of such attacks and trying to work out the most effective way of dealing with them. It would also be in entirely possible that such attacks could be mistakenly attributed to different attack vectors due to misattribution. It is noteworthy that none of the respondents placed the UK in the list of nations with capable offensive cyber warfare abilities. This could be down to a bias due to them all being British nationals; in their professional life they would never be exposed to offensive UK cyber operations.

5. Field diaries

Following the tenants of Fassin (2013), the field diary was used to explore an understudied terrain, or a ‘black hole’ as Fassin himself puts it. Attention was paid to the ordinary within the Dark Web and attempts were made to elicit perspectives from this world. The lack of any previous ethnographic approach to patriotic hacking was discovered during the literature review; this neglect is possibly due to the difficulty of conducting such research and its comparative newness.

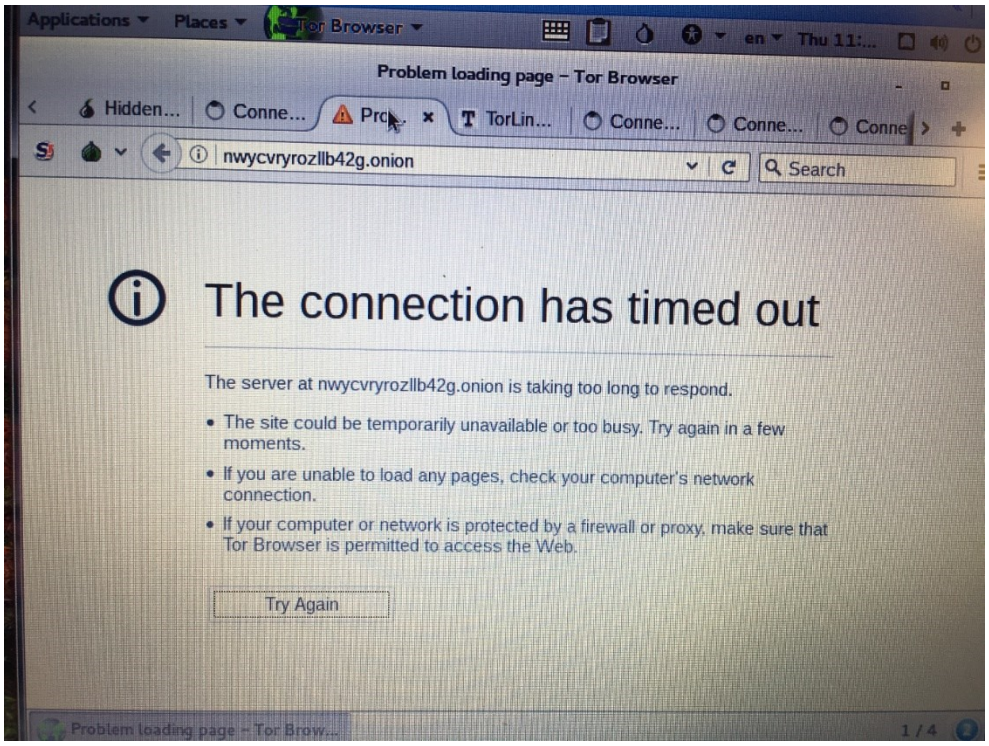
The reflections taken within the diary range from the banal (the constant checks against robotic incursions) to the extreme (the hitman and blackmail services). The former are captured within the diary by comments such as "to submit to Recapture security check to prove you're not a robot". This mundane security check was part of the ordinariness of the Dark Web but also gave hints of the paranoia ever present within its depths. However, this paranoid mind-set seemed to have some justification; the FBI were shutting down websites on a regular basis and a number of the forum members were engaged in clearly illegal activity. This feeling of being hunted by law enforcement agencies contributed to a recorded exchange of "don't trust nobody, feds are everywhere“. This vignette exposes the social texture present in the Dark Web and renders perceptible the vulnerability felt there.

Some of the nomenclature used in the Dark Web was revealing. The search engine ‘Not evil’ contrasts with the more combative ’Kick-Ass’ marketplace. A forum for hackers went by the moniker ‘Offensive community’; whether the group intended the adjective to be defined as ‘insulting/rude community’ or the more aggressive ‘hostile/attacking community’ was not clear. The noun ‘community’ seem to imply a cohesion of people having similar characteristics – a grouping on the Internet trying to self-define.

The lag caused by using the anonymisation software TOR/TAILS led to a rigid dichotomy between safety and speed. The anecdote captured by one group of posts complaining of the system slowness was counted by others chiding them as “newbies” or “noobs”. This exemplifies one of the characteristics forum members coveted; to be considered experienced and therefore not naive or unsophisticated. On a more prosaic level, the services offered on the Dark Web seem to expect payment only in Bitcoins (BTC). As Caffyn (2015) recounts, the Dark Web is the ‘1st killer app’ for Bitcoin and drug transactions were a large proportion of total transactions made.

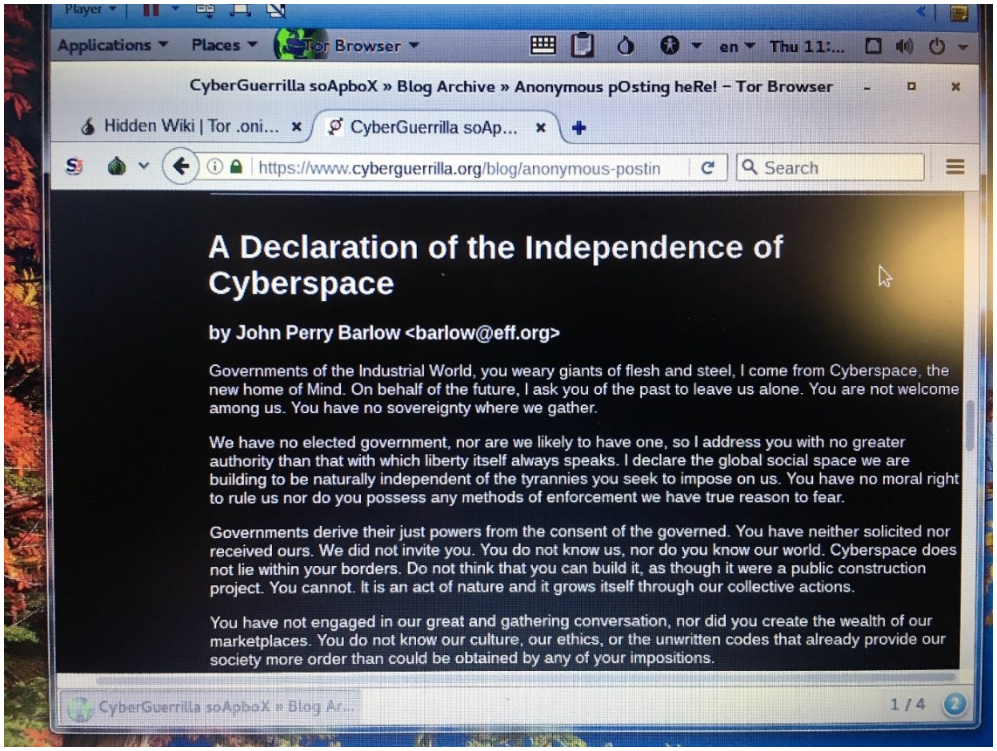
Screenshots could not be used due to the setup of the TOR/TAILS software so photographs of interesting webpages were taken instead and are shown in figures 2 to 18:

Figure 2 - Connection timed out



A constant occurrence during the field research was the timing out of connections (see figure 2). It could not be ascertained if this was due to the onion site being unreachable or the TOR/TAILS software latency causing the problem.

Figure 3 – Cyber Guerrilla manifesto



A political website called Cyber Guerrilla was accessed using TOR (though it appears to have an address indexed by Google). One of its pages contains a manifesto which appears typical of an

anarchist organisation; it is critical of existing governments and declaring such institutions obsolete (see figures 3 and 4). It demonstrates traits similar to those of Anonymous (Olson, 2013), stating that fairness and humane behaviour across the world are its objectives.

Figure 4 – Cyber Guerrilla manifesto continued

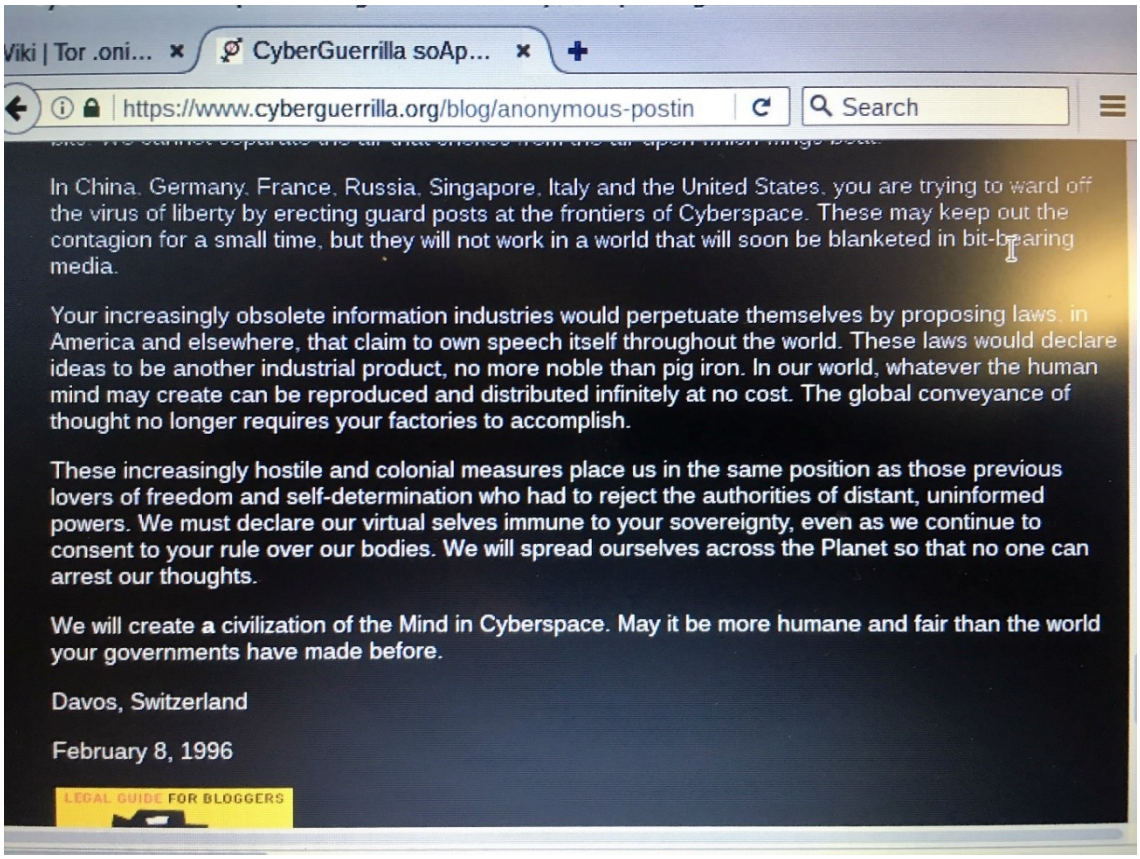
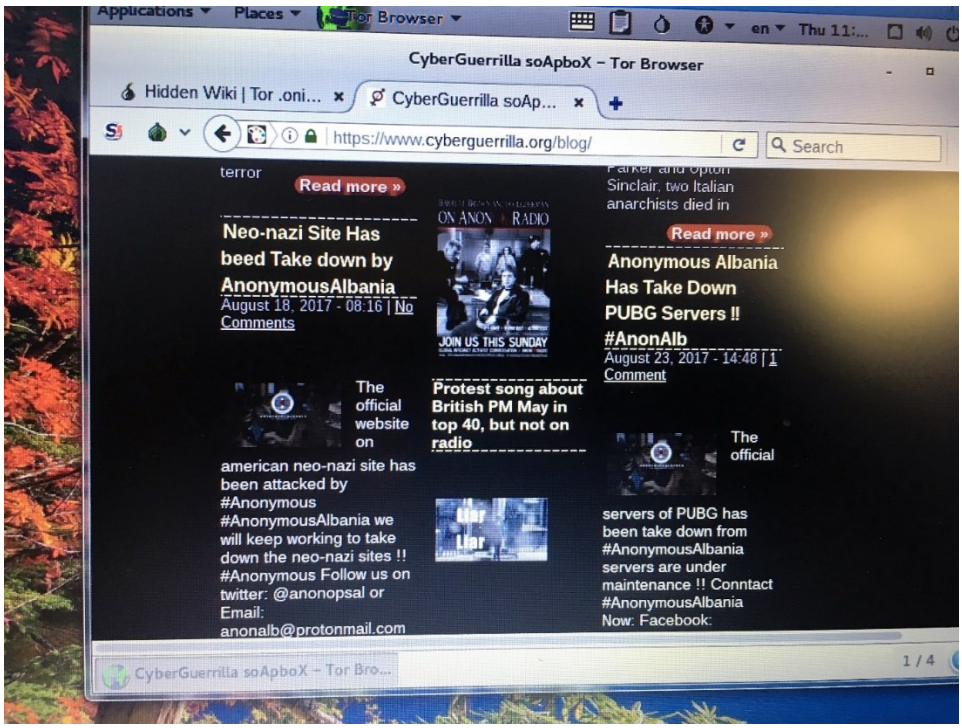
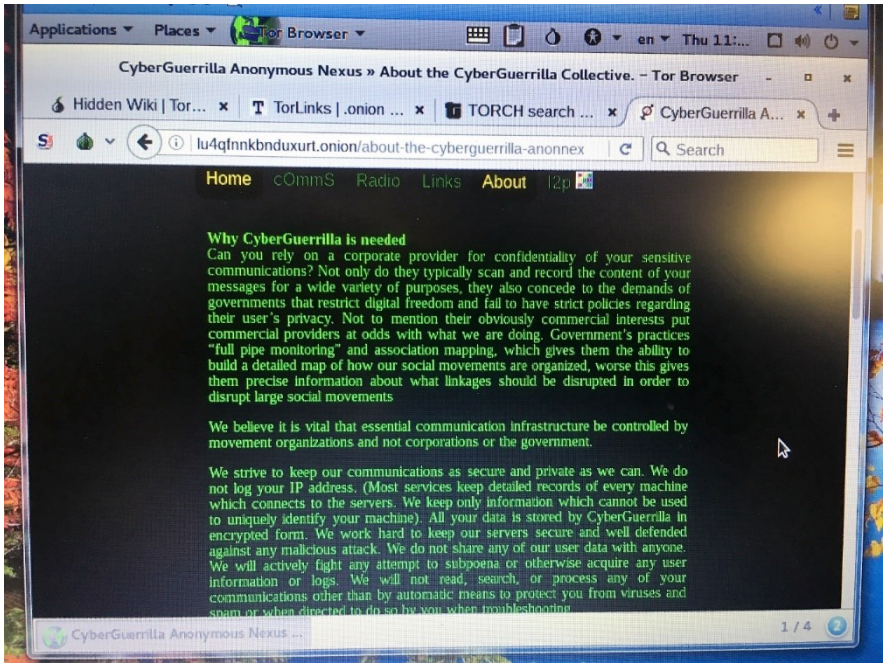


Figure 5 – Cyber Guerrillas; hailing Anonymous in Albania



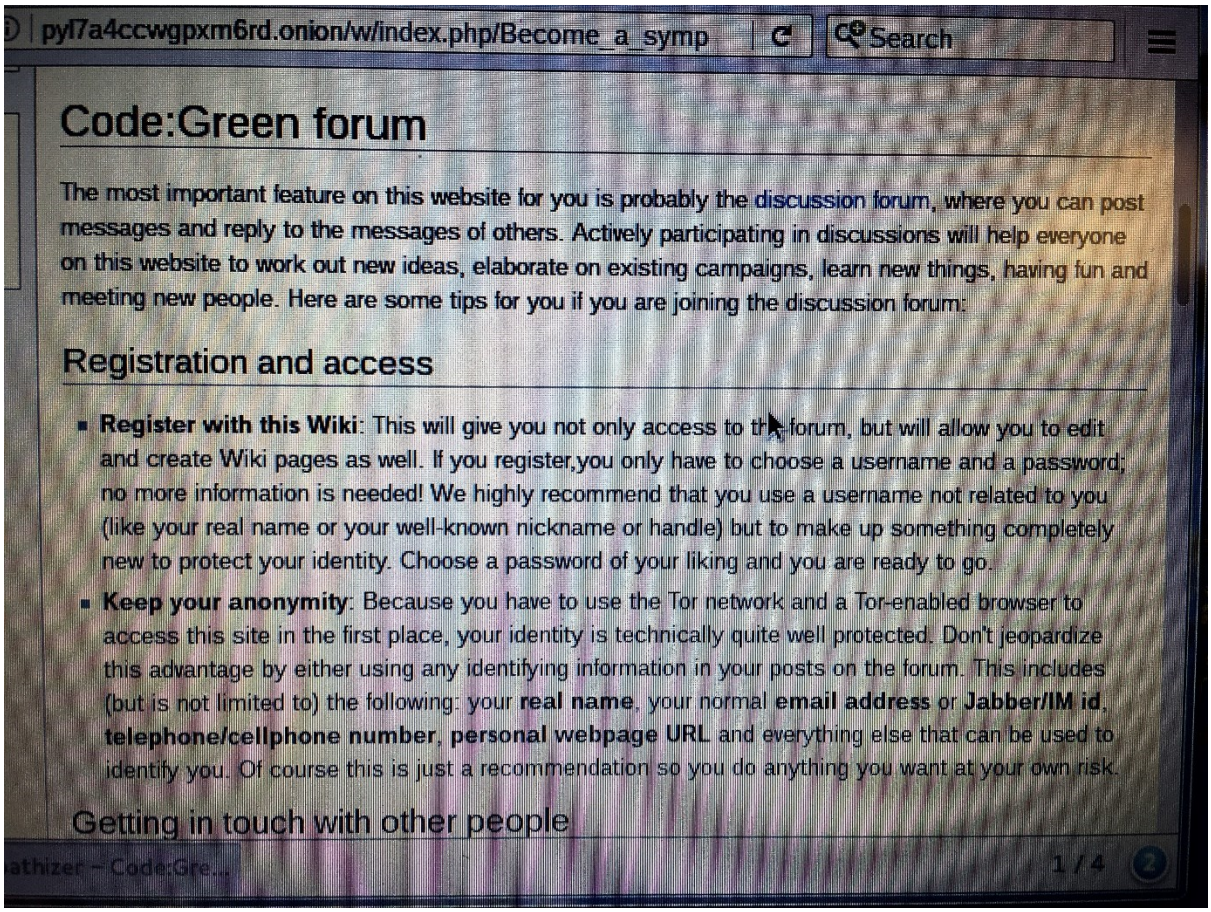
Another still from the Cyber Guerrilla website (figure 5) shows blogs celebrating the actions of Anonymous in Albania. One shown rejoices in the hacking of an American Neo-Nazi website. It is not clear whether this website is the official one of Anonymous or whether it is another organisation that merely celebrates them.

Figure 6 - Why Cyber Guerrilla is needed



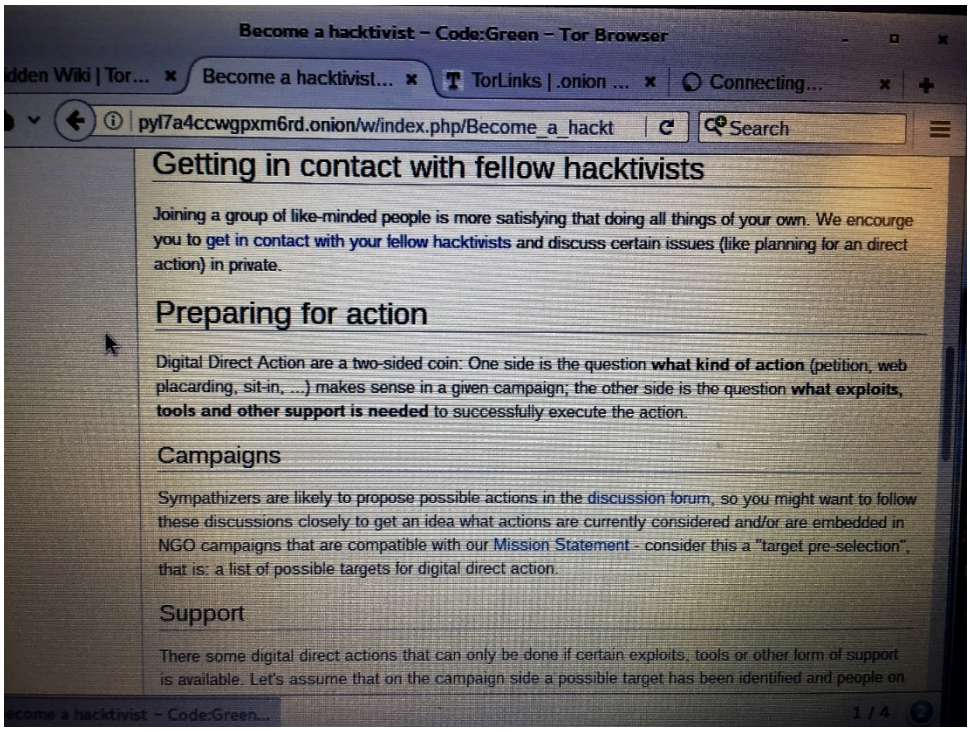
The Cyber Guerrilla website provide services for anarchists, including a confidential email service. Figure 6 shows a message to users declaring why and how to protect their identities, communications and movements. It also differentiate itself from mainstream email services by railing against "commercial interests". They also comment that the information stored there is encrypted and that user IP addresses are not logged. This is another demonstration of how the Dark Web parallels the regular world by offering the services that legitimate companies offer.

Figure 7 - Green forum; codes



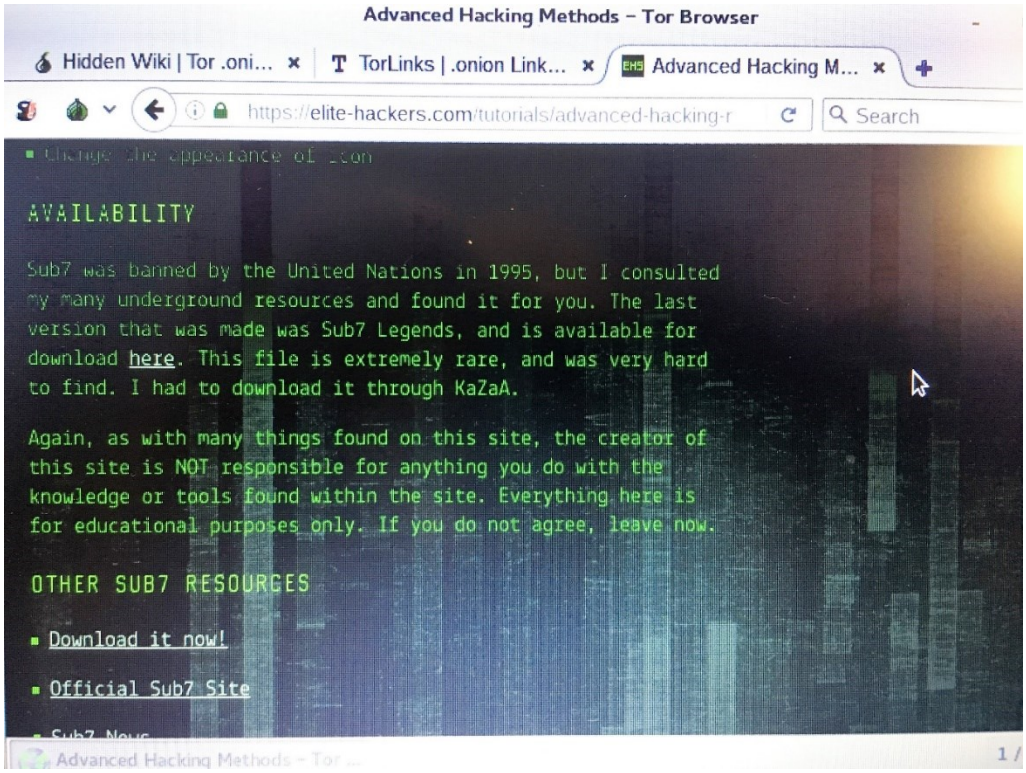
Another Hacktivist website was visited, called the Green Forum, and this allowed members to participate in discussions with other hacktivists. It encourages users to post messages anonymously though it adds that members' identities are protected by the TOR System they have to use to access the site anyway. It advises members against giving personally identifiable information such as their real names, well-known nicknames or mobile phone numbers (see figure 7).

Figure 8 - Green forum; preparing for action



A different page on the green form website talks about Digital Direct Action. They ask any potential Hacktivist what kind of action they are interested in (petition, web placarding, sit-in's) and what kind of tools they need to execute the action. This includes exploits, tools and any other support that's needed (see figure 8). It also indicates a “mission statement” that identifies potential targets.

Figure 9 – Elite-hackers; sub7



The Elite-hackers website purports to provide advanced hacking tools, including the sub7 Trojan horse which includes a key logging feature – this is shown in figures 9 and 10. Figure 10 also shows an email hacking tool that is available to download.

Figure 10 – Elite-hackers; email hacking.

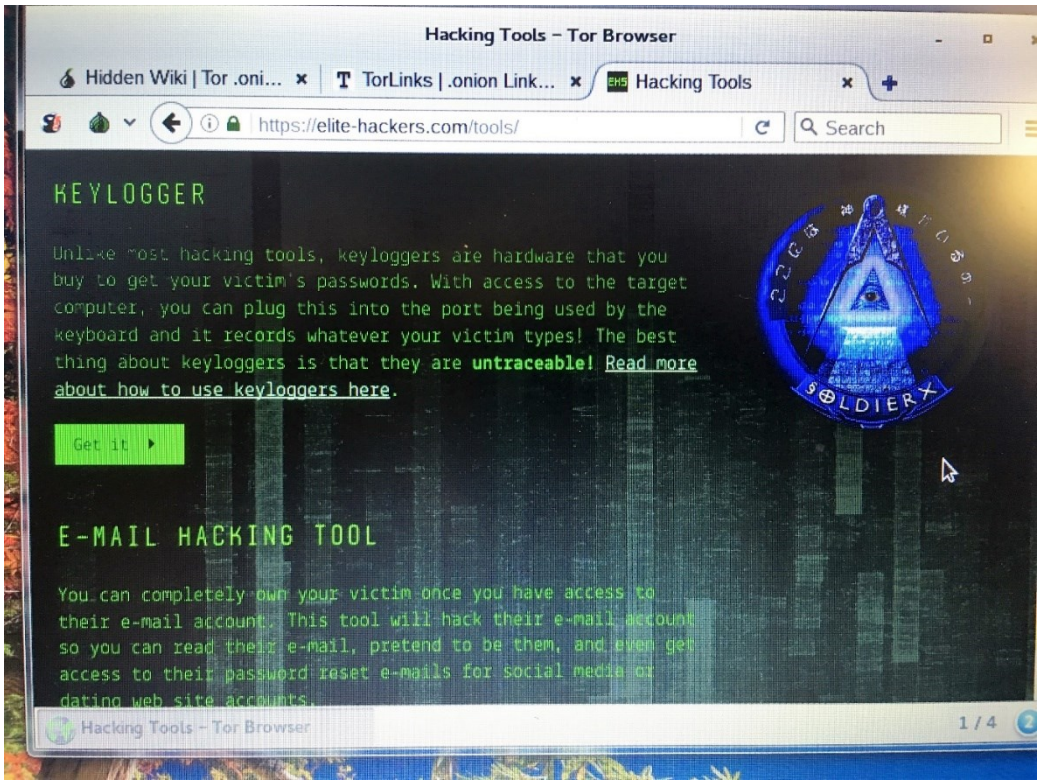


Figure 11 – Elite-hackers: who this site is for

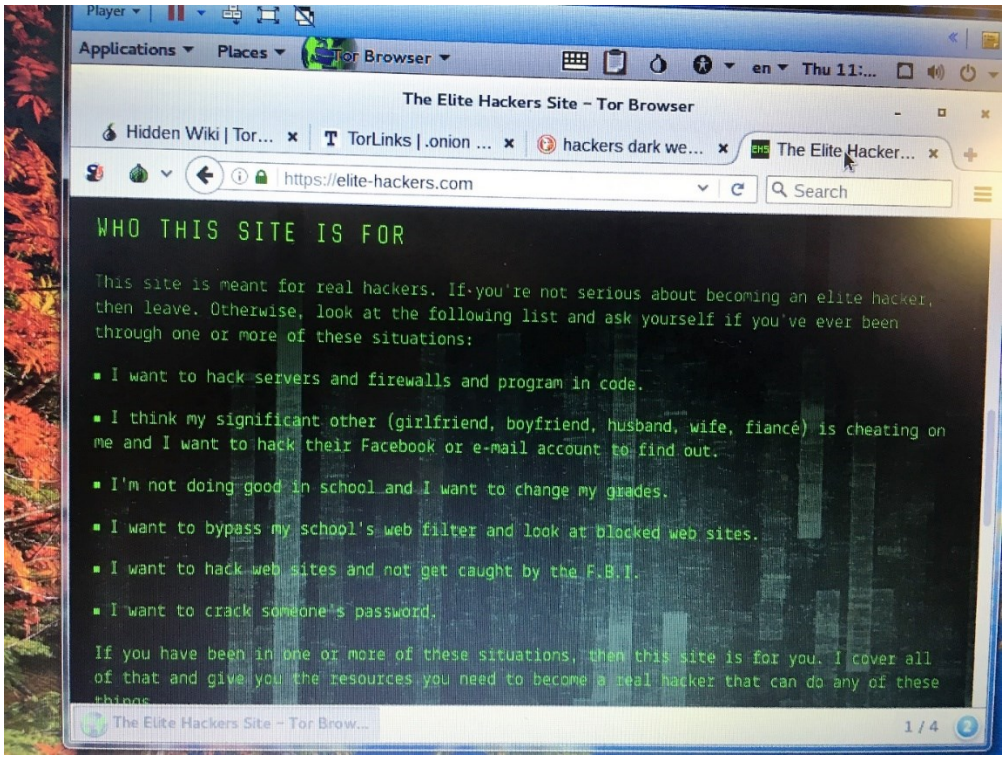
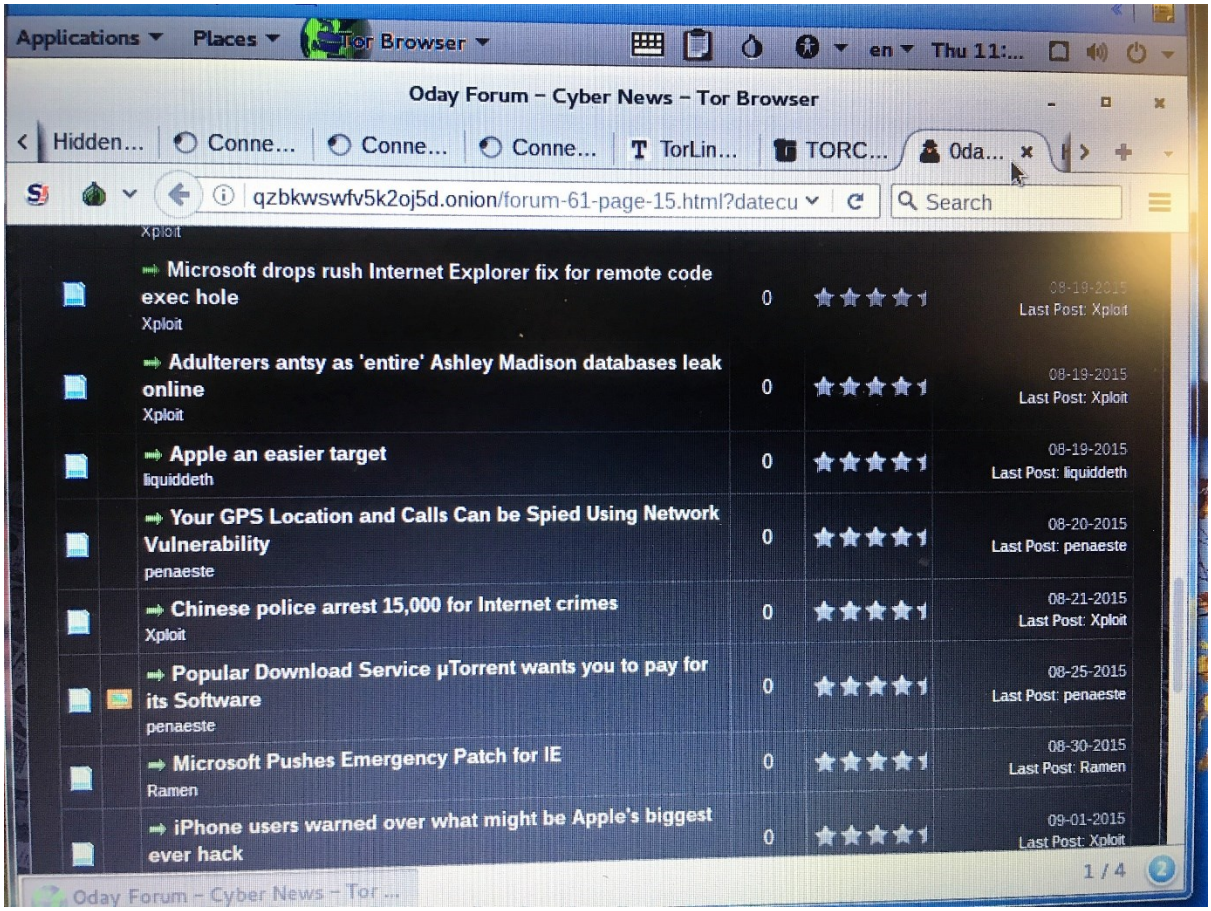


Figure 11 shows who the Elite-hackers site is targeted at and what they offer. This includes details and tools to hack firewalls and social media sites. It also purports to allow users to avoid the FBI, change exam marks and utilise password cracking. The voracity of this website is difficult to ascertain, these may be genuine services or something that is without foundation.

Figure 12 – 0day forum



A hacking website entitled “0day forum” takes its name from the term “zero day vulnerabilities”, which are undisclosed software vulnerabilities which leave the software’s author zero days to patch and make safe. This forum requires registration to post on and can only be accessed by using TOR. New vulnerabilities, general cyber news and Law Enforcement Action (LEA) are all discussed on the forum.

Figure 13 – Hackpartners; warning

Another hacking website called The Hackpartners invites people to join though it warns that “Our expectations are high” and that “if you fuck with us, we will fuck with you”.

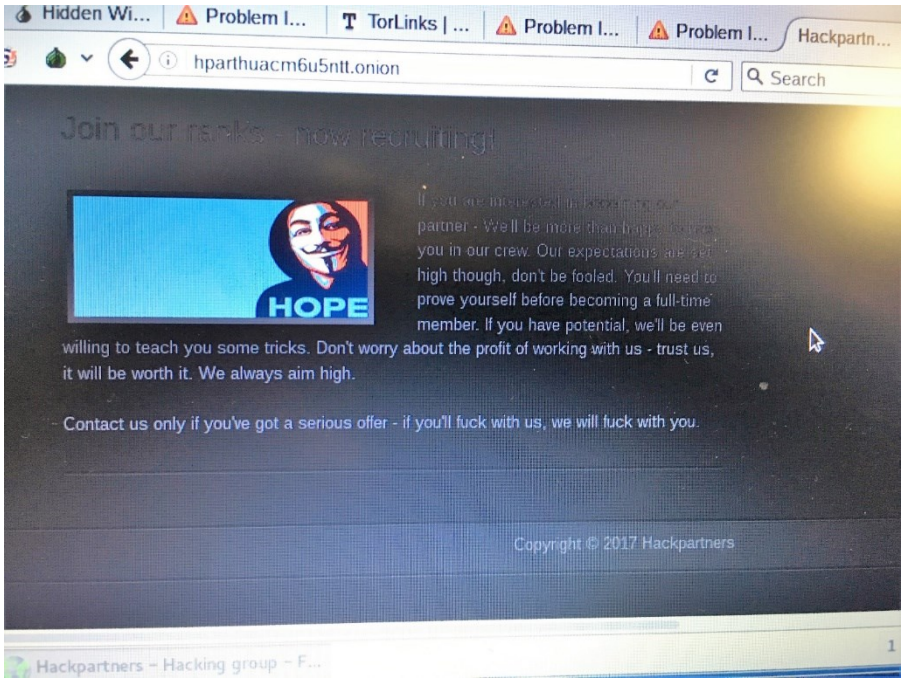


Figure 14 – The Hidden wiki; drugs

A common jumping off point on the Dark Web, the Hidden wiki is a website built collaboratively by the Dark Web community. It allows users to add and edit the links held within it. This particular wiki offers different illicit services, such as purchasing illegal drugs, as shown here. Note that there are also references to “Silk Road marketplaces” and “Silk Road forums” which are probably homages to the original, which was shut down by the FBI in 2013.

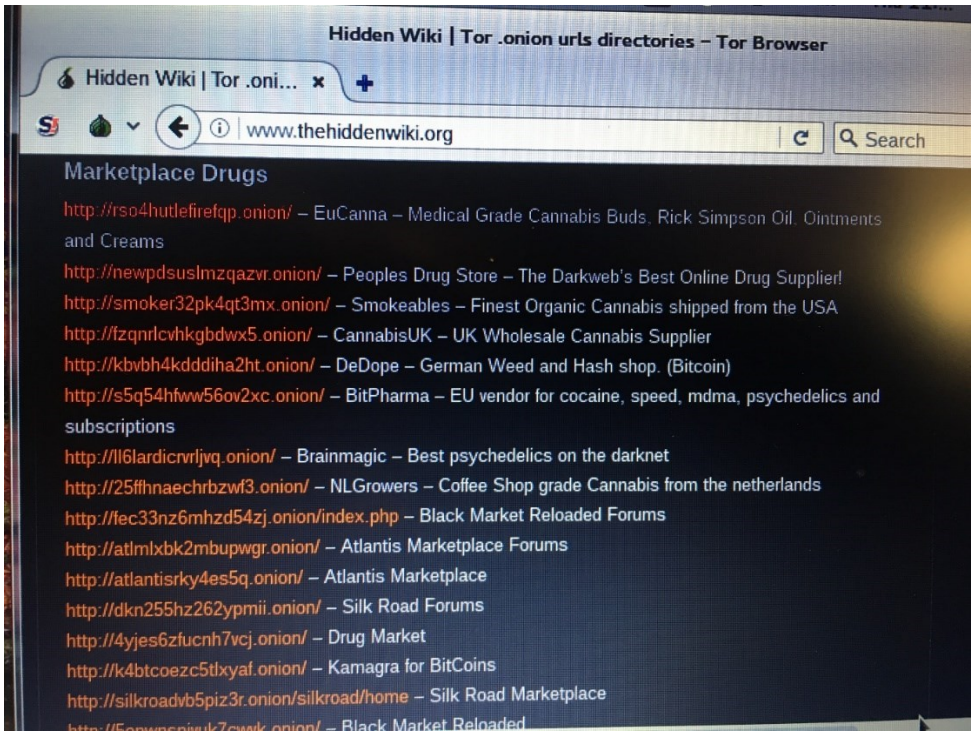


Figure 15 – Hidden wiki; political

Another part of the Hidden wiki concerns itself with political links; there are references to Wikileaks and some conspiracy theories. An atypical Link is that to a crowdfunded assassinations website, which appears to be incongruous next to the “Fairrie Underground” link.

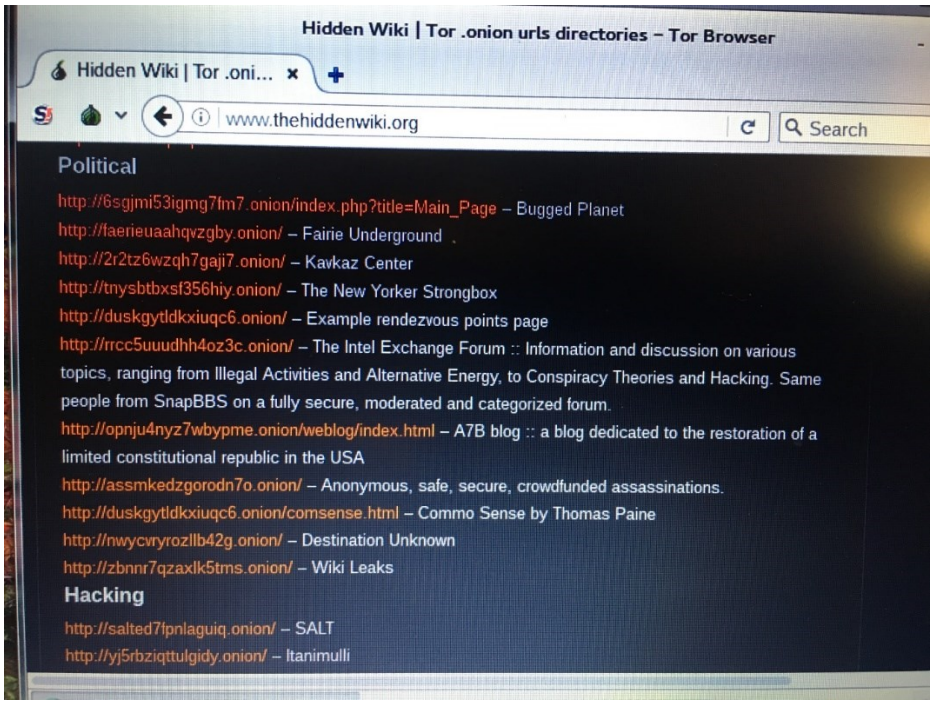
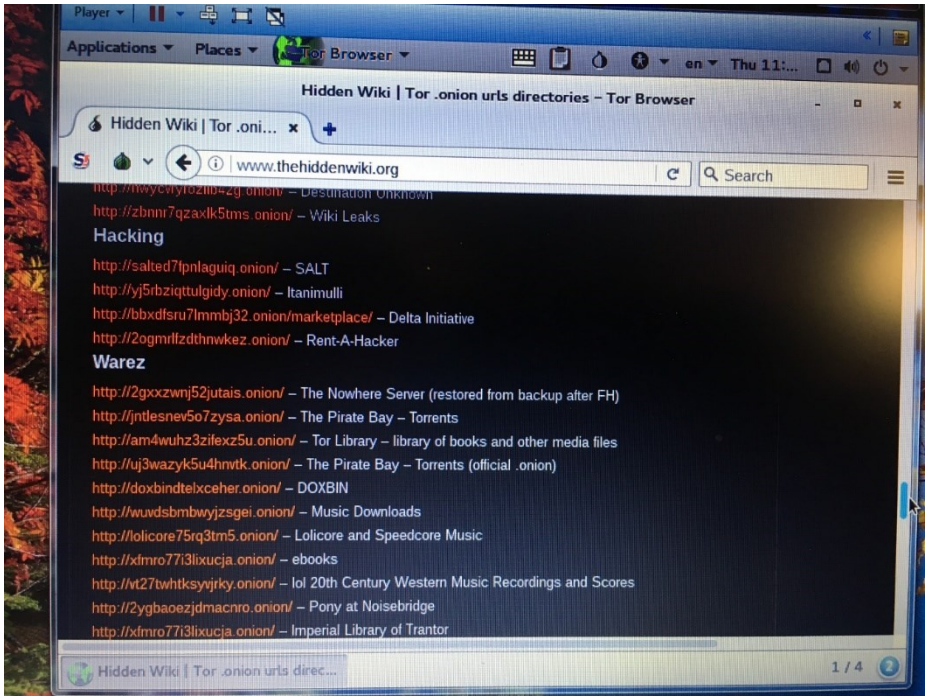


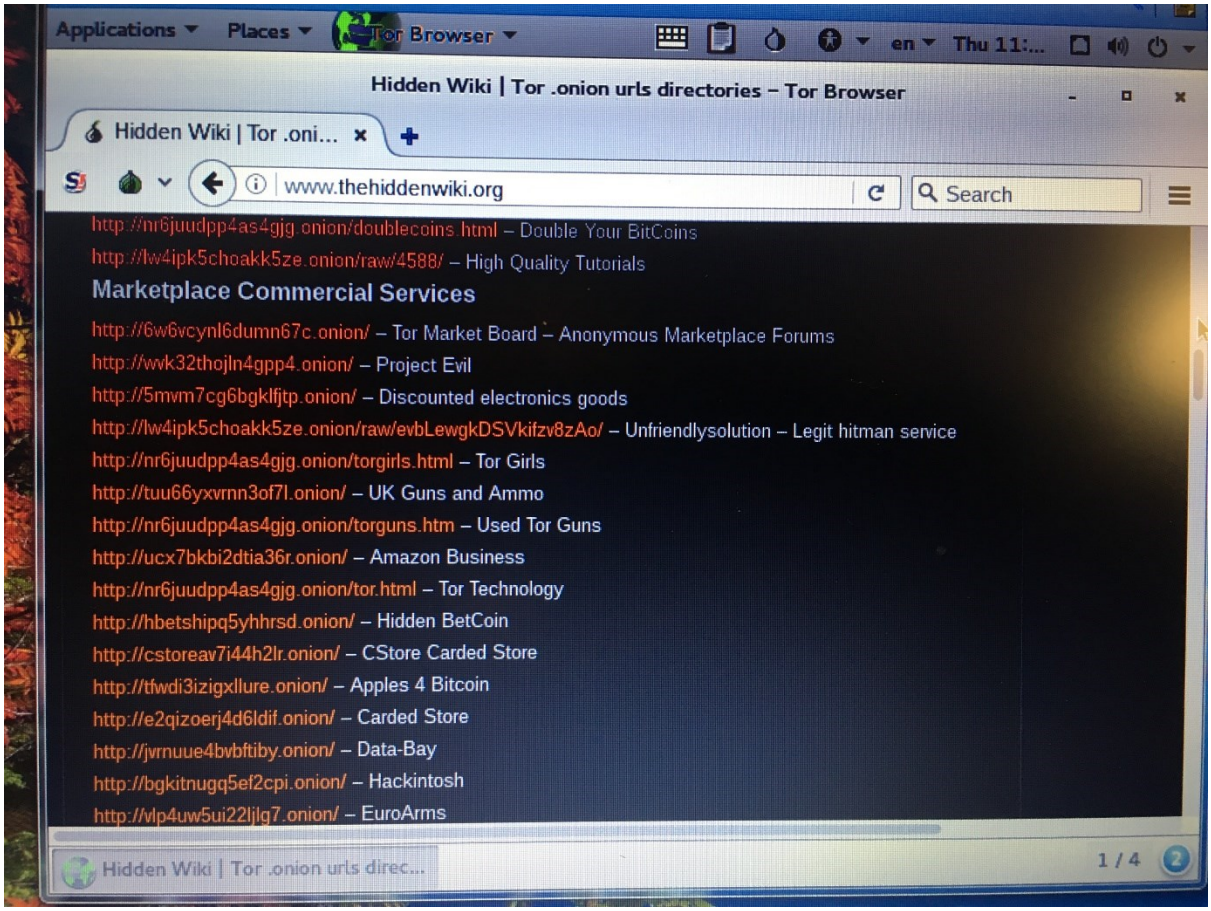
Figure 16 – Hidden wiki; hacking and warez



In this figure links to hacking and warez sites are shown. The first three links in the hacking section did not work for the author – this is fairly typical on the Dark Web as sites are badly indexed, taken down by LEA or are poorly maintained. The Warez section demonstrates the popularity of pirate software and streaming (torrent) services on the Dark Web and reinforces the findings of Seigfried-

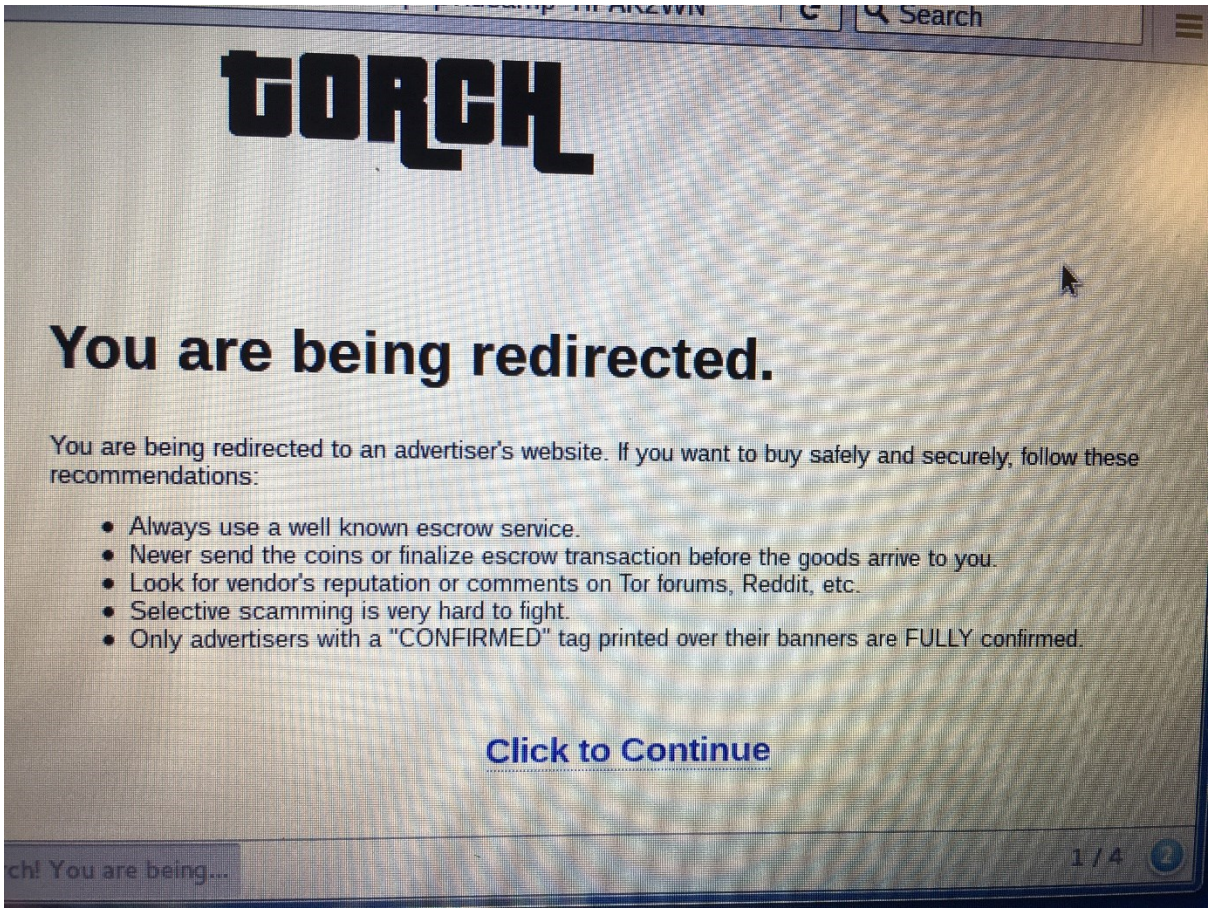
Spellar et al (2015) and Décary- Hétu et al (2012). These authors found that one of the first steps of cyber delinquency was for miscreants to involve themselves in pirating software and illegal downloads. This then could lead to more serious instances of online illicit behaviour, including hacking.

Figure 17 – Hidden wiki; marketplace commercial services



This section of the hidden wiki offers an eclectic range of links to Dark Web services. These range from something called “Project Evil” through “UK guns and ammo” and onto various carding sites. The latter is where recently stolen credit card details are offered for sale, usually using Bitcoin as a currency. There are also sites offering to exchange Bitcoins into other currencies, such as dollars, and illustrate the points Caffyn (2015) was making about the alt-currency scene.

Figure 18 – Torch redirect



When using the Torch Dark Web search engine, figure 18 is shown when any attempt is made to go to an advertiser's website. This shows some care for the community of the Dark Web by the search engines designers; however, it is probably also an attempt to encourage users to use advertisers that are "confirmed" by Torch and is likely to be a revenue stream for that organisation.

5.1 Informal discussion with a hacker

The following is a full transcript of an informal discussion held with a hacker that was captured in the field notes.

"A meeting was set up with a friend of a friend, someone who I had been assured was a hacker, at least in a previous life. We agreed to meet in an informal location, a city centre public house. The pub was only moderately busy, and there was room at the back where Tom and I could sit and discuss his experiences as a hacker. Tom was white male in his mid-40s and was dressed in standard office wear, shirt and trousers, but they were kept rather scruffily. His hair was unkempt, he had some stubble and was a chain-smoker. Once we had ordered our alcoholic drinks Tom insisted on us going to the outside space so he could smoke whilst we talked.

Tom began by describing his past, he had been to university and had begun his career in IT. He was now a well-regarded cyber security architect and had gainful employment. He was also a part-time DJ with all his own speakers and amplifiers etc, which he was quite proud of and described at some length.

After a few more drinks, and a bit of trust had built up, it came to light that Tom had a complex personality. He had a problem with excessive drinking, gambling in casinos and he even recounted

an attempted suicide some years earlier. Tom was also, however, an intelligent person who had a sense of humour laced with a lot of self-awareness; he recognised his flaws, which he ascribed to an addictive personality.

This frank conversation was allowed to develop due to the trust between us; this was based on our age, background and education being similar. We had also both worked in the same industry spaces and could relate amusing anecdotes to each other. The informal nature of our surroundings coupled with the shared laughter over the anecdotes was essential in Tom being comfortable and feeling able to give a frank account of his life to date.

When probed about his experience with hacking, Tom was still forthright and did not seem embarrassed in any way. He explained that these days he was on the good side, and was using his experiences as a hacker to help protect companies and organisations. He didn't believe his previous actions as a hacker invalidated his current work; in fact he indicated that it reinforced it.

He began hacking whilst at university. He was doing a computer studies course and had noticed various complaints about the database that the students were using to save their data on. The database language was SQL- 92 and, utilising an SQL injection flaw, Tom was able to gain access to the server. Once he had access he quickly ascertained that not only did it have all the students work on, but it also had a space where the lecturers stored the exam questions. With his final exams coming up, Tom took the opportunity to check the database regularly in an attempt to see his own upcoming exam questions. After repeated incursions Tom finally saw the paper he was after and transferred it to his own private server. Utilising this he was able to revise exactly what he needed and he stated he came out with a score in excess of 80%. He also admitted that he didn't try to answer the questions perfectly, as to not raise too much suspicion. He also had the benefit of being regarded as a bright student and therefore his high marks were not held under any suspicion. After his exams, Tom stated, in a fit of conscience, that he sent an anonymous warning to the University explaining their weaknesses in the server and a recommendation as to which IP ports to close to protect it better.

Thus began Tom's interest in hacking.

As it was approaching the end of the night, it was decided that we would have a more formal meeting at a later date where I would be allowed to record the conversation, Tom would also elaborate on what other hacking he had done since leaving university.

Unfortunately, after this initial meeting, Tom did not respond to any further requests; different channels were tried including texting, emailing, contact via LinkedIn and using a mutual friend to try and contact him. Unfortunately, Tom was not willing or able to respond and further exploration of his hacking were therefore not concluded."

Tom is a pseudonym.

6. Secondary research findings – FBI statistics

The IC3 (Internet Crime Complaints Centre) were set up in 2000 (then known as the Internet Fraud Complaints Centre) to allow the public in the USA to report cybercrime. The information gathered is disseminated to allow investigations and further analysis to be completed by other law enforcement agencies and industry partners. Information on Internet facilitated crimes is gathered and covers a growing list of misdemeanours from online extortion to money laundering and intellectual property theft, amongst many others. The worth of the IC3 concept is demonstrated by Canada, Germany and the UK using it as the basis for their cyber reporting since 2013.

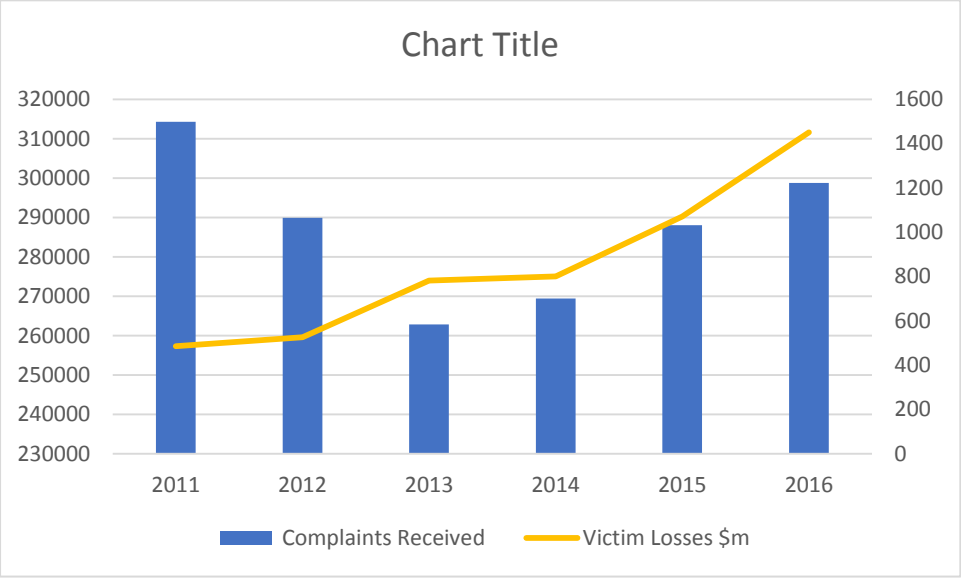
The 2016 Internet crime report was chosen to provide context for the study and was downloaded from the IC3 website. It is the latest full report available.

Two key metrics to drive out of the total number of complaints received and the total victim losses. These are shown for the last six years below in table 3 and graph 1.

Table 3

Year	Complaints Received	Victim Losses $m
2011	314246	485.3
2012	289874	525.4
2013	262813	781.8
2014	269422	800.5
2015	288012	1070.7
2016	298728	1450.7

Graph 1



The data shows complaints falling between 2011 and 2013 before picking up again. In contrast, the total losses shows an inexorable rise from 2011 to 2016 when over 1450 million dollars was recorded.

Other pull-outs from the 2016 report are the figures recorded for losses by crime types; those of interest to the study are shown below in table 4:

Table 4

Type	Victim Losses $m
Business Email Compromise	360.5
Corporate Data Breach	95.9
Phishing/Vishing/Smishing	31.7
Denial of Service	11.2
Malware/Scareware	3.9
Ransomware	2.4
Virus	1.6
Hacktivist	<0.1

The actual figure for hacktivism related crime in 2016 is approximately $55,000 – a possible indication that the motivation for hacktivism is not primarily financial. There are no figures in the above that can be directly linked to patriotic hackers, though they may be covered in areas like Denial of Service.

7. Discussion of research findings

7.1. Introduction

This chapter will discuss and contrast the findings of the research methods chosen; primary research in the form of interviews and the field diary, and secondary research in the form of the literature review and FBI statistics.

7.2. Current state of research into patriotic hacking

This section was mostly informed by the literature review as detailed in section 2.

The very phrase 'patriotic hacker' is a contentious one. None of the experienced cyber security specialists interviewed had heard of the term before; indeed, one correlated patriotic hackers to hacktivists (respondent D, section 4.2). However, patriotic hackers are referred to in both academic and non-academic literature. One of the earliest references is that of Denning (2000) who distinguishes them as citizens or expatriates involved in cyber state-on-state conflict. A more modern definition comes from Borghard and Lonergan (2016), who consider them within a typology of cyber proxies; here they are considered to be unorganised groups or individuals acting for political ends. The patriotic hackers as an unorganised person or group was given a more nuanced definition by Ottis (2011) who graded their organisational level based on three different models; the Forum, the Cell and the Hierarchy. Ottis stated that patriotic hackers were at the most unorganised in the Forum model and their organisational structure became more corporate/militaristic moving from there, through the Cell and eventually arriving to what he termed the Hierarchy, where the discretion and actions of the individual was subordinated to the collective group. However, that is not to say that the final stage is the most effective. As Ottis himself points out, the correct model depends on the situation a controlling state find itself in; different problems require different solutions.

The definitional waters are muddied by Aschmann et al (2015) who fuse patriotic hackers with religious fanatics. Whilst there are certainly cases in the Middle East where patriotic hackers have acted along religious lines, there are also numerous cases of them not doing so (Barata, 2015). A good example is the cyber conflict in Estonia in 2007, where the moving of a Soviet war memorial led to conflict between the state of Estonia and Russian patriotic hackers. Whilst there was an ethnic aspect to this conflict, there was not a religious one. The author Kshetri (2013) conflates patriotic hackers with online criminals; it is probably the case that some patriotic hackers are career criminals. However, with some countries organising patriotic hackers into cyber militias and with most not involved in actions for personal financial gain, Kenny (2015) suggests that the labelling of them as simply criminal is wrong. Organised groupings of patriotic hackers is explored by Borghard and Lonergan (2016) who labelled them cyber militias (or armies); they added that 'moonlighters' or mercenaries may augment these collectives.

All of this allows a definition of patriotic hackers to emerge via inductive reasoning. This is: "A patriotic hackers is an individual who involves him/herself in cyber conflict to further the perceived political aims of their home country".

The FBI statistics (section 6) show no reference to patriotic hackers and only a minor reference to hacktivists. Against a backdrop of rising victim losses (that is, the amount of damage victims of cyber malfeasance have incurred, estimated in $– see graph 1) it is apparent that the activities of patriotic hackers are not prevalent enough to warrant inclusion. However, care must be taken with this analysis as patriotic hacking operations may include DDoS attacks (and possibly other FBI recognised

types) which are collated without reference to the type of attacker. That is, patriotic hackers may indeed be affecting the figures but they are not directly visible.

Action by patriotic hackers has been recognised since at least 1999 when the USA accidentally bombed a Chinese embassy; tit-for-tat actions by USA and Chinese patriotic hackers followed. It is interesting that following the September 11th attacks in 2001, the USA decried its own patriotic hackers' actions in defacing Arabic websites, demonstrating that nation-states do not automatically value such action. This is possibly because such action was not only *ultra vires* but also may have led to a disproportionate counterstrike and hence further escalation.

The use of cyber weapons in cyber militias is commented on by Barata (2015), with states providing them when required to achieve a political objective. Supplying advanced code to such groups has inherent dangers as shown by the use of stolen Equation Group (a part of the NSA) cyber weapons that were then used to create the WannaCry ransomware. The authors Knopova and Knopova (2014) stress that such cyber weapons create a paradigm shift in warfare and foresee ominous results for society as a whole. Kenny (2015) is more sanguine, contending that such weapons are not widespread amongst malignant cyber actors and that terrorist recruitment via the Internet is a greater problem. In the fast moving world of cyber weapons, this view from 2015 already appears out of date as the WannaCry and NotPetya ransomwares demonstrate. The broadening of the attack landscape for cyber weapons is exampled by the advent of the Internet of Things. Multitudinous and exposed to poor security practices, they allow the creation of vast, zombie networks (botnets) that can be used for DDoS attacks.

Such botnets could be used if a cyberwar was to break out. There is some debate over whether an actual cyberwar is in progress: Breene (2016) believing that the USA is conducting cyberwar against the so called Islamic State. Knopova and Knopova (2014) conversely do not believe a cyberwar is in progress; they state that it would be highly visible if it were active.

Borghard and Lonergan (2016) stated that the use of patriotic hackers gives both benefits and disbenefits. The argument is that their key pro is the ability for the controlling nation to act at a remove by giving them plausible deniability. This is confirmed by Dahan (2013) in his paper "Hacking for the homeland: patriotic hackers versus hacktivists". One of the prime issues with their use is the way such forces can spiral out of control, possibly leading to punitive counterstrikes and escalation. An example with out-of-control cyber proxies is the 'Red Hacker Alliance', which had over 300,000 members in 2006. This cyber army was co-opted by the Chinese authorities to conduct cyber operations but it appears that it got out of control, with over 250 million people in China being victimised online by such groups (Beech, 2013). However, their low cost of use, coupled with the Internet's cloak of invisibility, means that they are still an attractive asset to military planners. Karatzogianni (2012) argued that future cyber wars would be waged by the two ends of the non-official cyber actor spectrum, the aforementioned patriotic hackers, and hacktivists; however, it is only the former that a state can effectively control.

Knopova and Knopova (2014) comment that the era of cyber warfare began with the discovery of Stuxnet in 2010; it was certainly the most powerful cyber weapon yet unleashed on the world and was sophisticated enough to only target the centrifuges in an Iranian nuclear processing plant. Variants of this weapon were used to develop Flame, Gauss, DuQu and WannaCry malwares; many companies/organisations across the globe were affected when these viruses were released against the public. This was arguably not what the developers of Stuxnet would have foreseen or wanted (Hejase et al, 2015).

Others suggest that cyber warfare actually began earlier; in Estonia in 2007, Lithuania and Georgia in 2008 and Kazakhstan in 2009 (Hejase et al, 2015). It is interesting that all these countries share geographical borders with Russia and almost certainly in the case of Estonia, Russian hackers were involved in the attacks (Michael et al, 2010). With a recent physical war in the Crimea and surrounds, the cyber attack against the Ukrainian power grid in 2017 also points to Russian, or pro-Russian supporters', involvement. The key problem with such statements is the difficulty of attribution in cyberspace. Whilst it is recognised that Russia is a cyber superpower and has the motivation to conduct such attacks, the difficulty of attribution (and, indeed, possible 'false flag' operations) means there is no direct evidence. It may be possible to deter such attacks if you have a powerful, offensive cyber capability (anonymous, 2016a); if not, cooperation with allied states may offer defence (Kostyuk, 2014).

Two other cyber superpowers, the USA and China, have both been accused of conducting cyber offensive operations. The USA was alleged to be behind the Stuxnet attack and has a powerful, secretive organisation with the moniker 'The Equation Group' which has developed new cyber weapons (Menn, 2015). It appears that the Chinese were initially happy to co-opt cyber militias (e.g. The Green Army) for offensive cyber operations (The Economist, 2013). However, this has now been superseded by PLA unit 61398, an actual entity within its standing army. This is an example of what Ottis (2011) calls a Hierarchy command and control set up and may have been a reaction to how the USA used information warfare in Iraq (Thomas, 2008). The creation of such forces in the USA and China (in addition to them both having powerful physical armies) has led to seemingly inevitable tensions between them. This manifested itself in 2013 with the then USA president, Barack Obama, warning the Chinese premier that Chinese hacks were damaging bilateral relations (Knake and Segal, 2016).

Military research has focused on how future cyberwars 'play out'. It is accepted that geographic distance from an enemy has no meaning in cyberspace and that reactive defence is not realistic (Butler, 2013). It could also be beneficial to have non-state actors (i.e. patriotic hackers) fight alongside state units (Aschmann et al, 2015) and, thus, the kinetic and cyber forces to act as one (Butler, 2013). Such concepts have led to military organisations, such as NATO, determining that cyberspace is a unique domain and have recognised it sits alongside the traditional domains of land, sea, air and space (anonymous, 2016b).

In contrast to Kostyuk's (2014) hopes for cooperative deterrence, it has been argued that deterrence does not work effectively in cyberspace (anonymous, 2016d). The argument being that you cannot prove that your offensive capability (acting in a counterstrike) is effective against all countries (as their networks are all different) and you cannot make a big statement in the same way as detonating a nuclear device and destroying a small, uninhabited island can. However, Henry et al (2010) are of the opinion that deterrence can be achieved through cooperation in building legal and theoretical frameworks to control cyber warfare. An attempt at doing this was sponsored by NATO and the 2009 Tallinn Manual was produced as a result (Schmitt, 2009). This tried to lay out the rules of engagement for cyberwars but it has not been adopted internationally (Aschmann et al, 2015).

This attempt at crafting a framework for cyberwar on which future legal regimes could be overlaid on has been welcomed by legal authors. However, Pool (2013) and Kirsch (2012) have both commented that a legal definition of cyberwar is first needed before additional frameworks are written. Legal definitions of proxy forces, such as patriotic hackers, are also required (Barata, 2015). This would allow a definition of cyber forces to be made that are within existing United Nations laws and would, therefore, have to comply with items such as the 1949 Geneva Convention. NGOs, such as the Red Cross, consider this, and other cyber warfare laws, to be urgent – as it is, existing laws do

not adequately protect civilians during a cyberwar (Droege, 2013). Such legal and linguistic delays demonstrate a shortcoming in international organisations' approach to cyber warfare; there is currently no specific cyberwar or cyber warfare legislation that can be applied internationally and yet cyber attacks continue unabated. This lack of action can possibly be explained by Chayes (2015) who states that nations do not want to self-limit the actions of their own cyber forces – largely because their hands are free if international laws are not in place. With four of the five permanent UN Security Council powers (USA, Russia, China, UK) having the greatest cyber capability, meaningful legislation may be some way off.

7.3. Toolkits and techniques

This section deals with what tools and techniques hackers could use to conduct attacks; these are universal meaning they are available not only to patriotic hackers but to hacktivists, script-kiddies, cyber terrorists etc. The tools to be described are not the prosaic physical hardware or simple software (for example, a laptop running VMware and utilising TOR/TAILS as the author describes in 3.3.2), but rather the sophisticated viruses, worms and Trojans used in the attack process and the way they can be delivered.

Viruses are malicious code that can execute themselves to affect how a computer operates without the original user's knowledge or permission. They are also self-replicating and can overwrite other files on the infected computer. Worms are different from viruses by spreading the malicious code without the need for a host file and generally exist within other files or documents. Trojans, or Trojan horses, claims to be desirable code but are in fact malicious. They do not replicate themselves and require an invite to operate, e.g. by opening an infected email attachment (anonymous, 2017).

Whilst writing sophisticated malware is beyond the capabilities of the majority of hackers, there is a minority who do so and were given the descriptor 'Coders' by Seebruck (2015). They may be talented individuals or, more likely, collectives such as The Equation Group (Menn, 2015). The majority of hackers use code written by others and utilise tools such as Kali Linux or Metasploit to deliver the payload (various respondents). Payloads may contain the aforementioned viruses, worms or Trojans. Whilst 'script-kiddies' (respondent C) would typically utilise ransomware such as WannaCry or NotPetya, patriotic hackers could have access to powerful cyber weapons typified by Flame and Gauss (Hejase et al, 2015). With patriotic hackers' *modus operandi* being to inflict as much damage as possible during a cyber attack (Dahan, 2013), it can be expected that they use malware that targets Critical National Infrastructure. Stuxnet is a prime example of such a worm but was originally only available to groups directly connected to the USA or Israel (Knopova and Knopova, 2014). However, it appears that powerful cyber weapons are now being leaked into the public domain, an example being the stolen EternalBlue exploit that came from The Equation Group and was used in the WannaCry virus (Thomson, 2017). Thus, whilst cyber weapons such as Stuxnet are undoubtedly potent, they can have deleterious side-effects and this can be considered a major flaw in their ongoing development.

Command and control is important during an advanced cyber attack and patriotic hackers have used RAT (Remote Access Tool) software to achieve this, notably during the 2016 email hack of the Democratic party of the USA by suspected Russian patriotic hackers (Alperovitch, 2016).

The techniques used by hackers to conduct cyber attacks is equally important. The first decision that has to be made before launching a malware attack is the identification and selection of targets. After weaponisation of the payload (e.g. loading a virus into a Microsoft office file), the next most important step is to understand how to deliver the weapon – this may be using cyberspace (e.g. a compromised website) or physically via a USB stick (respondent A). The latter method is typically

more expensive and complicated to set up (you need a covert operative in the same geographical area as the target), and is therefore usually only used by those with nation-state resources. However, as respondent A stated, this physical option typically targets the "soft underbelly" of an organisation and can be very effective. Once delivered by either channel, the weapon can exploit any vulnerabilities in the target and commence its attack.

Different attack profiles are used by hackers; sometimes theft of information can be achieved by simply farming passwords to unlock email accounts. A technique used to obtain this information can be phishing, where malicious entities disguise themselves as something trustworthy. This kind of social engineering has become a prime method of obtaining sensitive information (Mansfield-Devine, 2013), and victim losses in the USA ran to over $31 million in 2016 (table 4).

A technique that can cause widespread disruption is a DDoS attack, and has been used since the mid-1990s (Denning, 2015). This can temporarily disrupt the host's services and prevent it responding to genuine requests and can additionally be used for cover for other attacks; its distributed nature means stopping it is problematic. A good example was the Dyn DDoS attack in 2016 which caused major Internet platforms to be unavailable, primarily in North America and Europe (Etherington and Conger, 2016). The hacktivist group Anonymous claimed responsibility for this. Concerns were expressed by respondent A, B and D regarding the advent of IoT in the context of DDoS. With poor security (Weissman, 2015) a hacker could control a zombie army of tens of millions of compromised devices with which to launch a DDoS attack. Whilst the strengths of such assaults are clear, the weakness of a DDoS approach lies in its scattered line of attack – systems that an attacker may not wish to target can be affected anyway.

Whilst all of the above are available to patriotic hackers, their focus on trying to achieve political aims means that ransomware and other methods primarily for wealth generation are not likely to be used. Conversely, methods that might cause widespread distress, confusion and disruption, such as DDoS and powerful malware, are more likely to be used.

The field diary gave no direct insight into patriotic hackers' methods of operation; their secretiveness and unwillingness to be the subject of research terminated any direct understanding. However, the photographs shown in section 5 give some idea of the landscape habituated by patriotic hackers. Such sites as the Cyber Guerrilla website (figures 3 to 6) are unlikely to be a source of inspiration to patriotic hackers and are much more closely aligned with how hacktivists think and operate. In a similar manner, the Green forum (figure 7 and 8) appears to be set up for hacktivist groups, indeed they are directly mentioned (figure 8). However, the Elite-hackers (figures 10 and 11), 0day forum (figure 12) and Hackpartners (figure 13) offer more hard-line views that appeal to those of a criminal nature. Patriotic hackers could, nonetheless, utilise some of the software and services offered on such sites to conduct cyber attacks. Forums such as 0day could also be used to organise a group of patriotic hackers akin to the Forum or Cell, as suggested by Ottis (2011). The Hidden wiki shown in figures 14 to 17 gives a flavour of the illicit nature of parts of the Dark Web. Due to the vast scale of the Dark Web and the difficulties traversing it (see section 5), pinpointing sites aimed specifically at patriotic hackers was problematic. It is, however, reasonable to postulate that such sites exist.

The ethnography allowed another aspect of the landscape patriotic hackers operated within to be revealed. It became apparent to the author that all operators within the Dark Web, including patriotic hackers, have to choose between personal safety and speed of operation. This dichotomy was something that would have to be faced during every visit to this part of the web. Possible

exceptions to this would be reserved for those with direct state links; their methods for traversing cyberspace can only be speculated at.

7.4. Motivations of individuals involved in patriotic hacking

It is worth revisiting the definition of patriotic hackers; a patriotic hacker is an individual who involves themselves in cyber conflict to further the perceived political aims of their home country. This implies some risk to the individuals, albeit at a much lower level than a kinetic conflict, that they are acting for their homeland and that they are interested in things political. The literature review holds little insight into their motivations with the exception of Dahan (2013), who stresses that their motivation lies solely in their patriotism, with no visible manifesto. However, the interviewed respondents offered a view that their motivations would be wide ranging; a list was compiled from their collective views:

I. Monetary gain
II. Recognition and kudos
III. Being coerced
IV. Political and ideological
V. Nationalistic

Taking these in turn, the idea that money can motivate patriotic hackers is given support from Borghard and Lonergan (2016) who describes mercenaries or 'moonlighters' who would act for a nation for monetary gain. Kshetri's (2013) argument agrees that many Chinese patriotic hackers are financially motivated but adds that they should simply be called cyber criminals, not patriotic hackers. The idea that monetary gain is a motivation contradicts the finding in section 7.3, where patriotic hackers were found to be not using tools such as ransomware. The distinction may be that they are willing to be rewarded (by the supporting state) when undertaking political operations but they ceased to be considered patriotic hackers when using ransomware for personal wealth gain. In this latter example they are simply cyber criminals.

Any recognition or kudos that patriotic hackers may desire would have to come from other cyber warriors as it is unlikely the home nation would publicly recognise them. This would go against plausible deniability, a key concept of using proxy forces. Indeed, after the events of 9/11 the USA government disowned patriotic hackers' attacks on Arabic websites. However, Russia has a more sanguine view with President Putin describing patriotic hackers as "…free people like artists" implying that they cannot be controlled. He added that they were contributing to the "…justified fight against those speaking ill of Russia", which demonstrates at least some respect for them and attempts to justify their actions (Hille, 2017). Respondent C explained how recognition from other hackers might be a motivation by stating "kudos, I helped my country, I targeted my enemy, I help take down the enemy website".

The next listed motivation, coercion, can be considered to be an ever present possibility when you are acting unlawfully, as patriotic hackers are. Coercion involves the hacker being compelled to act against their will by the use of psychological pressure, threats or even physical force. Acting outside of the law, the hackers put themselves in a position where national security services can request that they act with them or face penalties. Some of the paranoia exhibited on the Dark Web "don't trust nobody, feds are everywhere"(See field diary, section 5) can be construed as an attempt to avoid a coercive outcome for the hackers.

In terms of political (or ideological) motivation, Borghard and Lonergan (2016) in their discussion about proxy forces comment that such forces are acting politically and Ottis (2011) and Barata

(2015) concur. Dahan (2013, p55) stressed that patriotic hackers were "parochial, generally to the right of the political spectrum and with little to no cohesive ideology". From the interviewed specialists, respondent B stated that they would have "ideological, national and political motivations". As can be seen by the breadth of illicit services on viewing the Dark Web (see figures in section 5), it can be postulated that kindred spirits for political or nationalistic ideals can be sought out fairly easily and safely. Like-minded individuals may then reinforce illicit online behaviour and make a hacker more receptive to delinquent moral guidance.

This segues into the final motivation to be discussed, nationalism. Barata (2015) states that patriotic hackers act on nationalistic grounds with respondent B agreeing with this sentiment. Dahan (2013:56) added that patriotic hackers "lacked any cohesive or identifiable ideology beyond nationalistic rhetoric". If we think of patriotic hackers acting as part of a more organised force aligned to a state's security force (towards Ottis' Hierarchy), then their nationalism defines them.

Overall, it is the nationalistic motivations of patriotic hackers that stand out as a class defining feature. The others can all be associated with other hacker types, such as recognition and kudos for hacktivists, and monetary gain for cyber criminals etc. No hacker types, except the patriotic hacker, operate out of a sense of nationalism.

7.5. The effectiveness of patriotic hacking in cyber warfare

American patriotic hackers were involved in cyber conflict after 9/11. Israeli and Palestinian patriotic hackers have been active during various Intifadas. Russian patriotic hackers brought chaos to Estonia in 2007 (Dahan, 2013). However, it is debatable whether an actual cyberwar has yet taken place, at least not between equally matched adversaries (Knopova and Knopova, 2014). Therefore, the effectiveness of patriotic hackers in a cyberwar has not yet been demonstrated; their actions have taken place in low intensity operations. Nevertheless, attempts can be made to assess their effectiveness by focusing on examining low intensity conflicts in which they have been involved, the countries operating them and the weaponry they have access to.

Patriotic hackers' capabilities depend on their structure; they can exist as nationalistic individuals with no set agenda through to highly organised units with a strong hierarchy (Ottis, 2011). Some authors term the latter group a cyber militia, though there is no set definition (Borghard and Lonergan, 2016). Whilst individual patriotic hackers acting on a purely nationalistic urge would add little to a nation's forces, more organised groups can pose a serious threat (Butler, 2013). Such groups, acting through some kind of command and control, would be difficult to stop; they could be distributed globally, even acting out of the target country and those of their allies, and the use of such software as TOR/TAILS makes tracking them difficult (Butler, 2013). As a precursor to a cyberwar they could also allow a country to utilise them whilst maintaining plausible deniability, as noted by the interviewed respondents. Depending on their structure, patriotic hackers would also be quick to stand up and be cost-effective, giving countries with low resources the opportunity to use them (respondent B). Conversely, as Ottis (2011) points out, the more structural units are, the longer they take to get in position and the larger overheads they run. As with other hackers, patriotic hackers have global reach and can strike a target at the speed of light (Butler, 2013).

The above capabilities all make patriotic hackers a welcome addition to the military standing of a nation (Aschmann et al, 2015). Conversely, using patriotic hackers in a cyberwar has some drawbacks. Respondent B picked up the risk of counterstrike stating that a 'cold cyberwar' could become "…less proxy and more actual". This would be an issue if patriotic hackers were used during a precursor phase to a cyberwar as hostilities may be triggered before the host nation was ready. Borghard and Lonergan (2016) concurred with respondent B when discussing the additional

disbenefit of the host nation losing control of the patriotic hackers, especially when they are in a less organised structure, and this could lead to unforeseen circumstances. Additionally, the respondents pointed out that continued hacking of this nature could lead to "the erosion of trust in IT", and especially in hyperlinks, with damaging repercussions for the future of Internet use. Such an outcome may not be intended when using patriotic hackers but the risk is there.

Respondent A also gave an insight to the capabilities of patriotic hackers in the commercial space. When queried about a state-level attack (patriotic hackers acting as a proxy force) he was blunt "…if you're in the attack category for those then you're going to get got no matter what". The implication being clearly that commercial entities have little defence against such attacks.

Whilst not a full cyberwar, the cyber attacks on Estonia in 2007 demonstrated some of the capabilities of patriotic hackers. Schools, media networks, government departments and banks were disabled by sustained attacks on their computer networks (Cizik, 2017). These attacks were DDoS in nature and were able to disable a wide variety of network dependent items such as Parliamentary email servers, credit card machines and other banking services (Kozlowski, 2014). In 2008, similar attacks against Georgia began with large scale DDoS outbreaks, followed by website defacement. Key sections of Georgia's Internet traffic was rerouted to services based in Russia and Turkey, where the traffic was either blocked or sent to Moscow-based servers. Georgia's office of the President and the Parliamentary website were defaced, with anti-Georgian articles and pro-Russian propaganda put in place (Lysenko and Endicott-Popovsky, 2012).

Countries suspected of utilising patriotic hackers, with at least indirect links to that state's security forces, include China, Russia, Iran, Syria, Israel and North Korea (Dahan, 2013, respondent B, Alperovitch, 2016). It is almost certainly the case that most countries of the world host patriotic hackers in the sense of nationalistic individuals acting without a government mandated agenda. However, it is the aforementioned countries that have some evidence pointing to state command and control. It is interesting that, with the exception of Israel, they are all authoritarian regimes. Additionally, they are all countries involved in recent conflicts or crises e.g. the Syrian Civil War, North Korean nuclear tests, the Ukrainian Civil War, etc. It can be hypothesised that countries with weaker accountability to independent media and press i.e. authoritarian states, can make use of patriotic hackers with a lower risk of exposure. It can also be hypothesised that countries who are battle or conflict hardened see value in using patriotic hackers, therefore, giving them some credibility as effective additions to regular state forces.

The cyber weaponry available to patriotic hackers can be greater than that available to hacktivists and the like. The latter should not have access to the latest nation-developed cyber weapons, whereas organised patriotic hackers groups do. However, this is not always the case. The stolen EternalBlue exploit is now available on the Dark Web and has already been used in various viruses (Thomson, 2017). Whilst such exceptions do exist, we can expect that patriotic hackers with strong state links would be allowed to access the latest technology (Barata, 2015). It follows that such weaponry makes the patriotic hacking groups more effective during cyberwars. In further assessing their effectiveness, Chansoria's (2012) writings are instructive; she states that China believes information superiority is so essential in any future war (note, not just *cyber*war) that they have integrated cyber warfare into the PLA and that they can call upon thousands of patriotic hackers when required. Russia also values patriotic hackers, with Putin an apologist for them (Hille, 2017), and cyber attacks in Estonia, Ukraine, Lithuania and Georgia all point to Russian patriotic hackers' involvement. If two such formidable cyber superpowers utilise patriotic hackers for their own ends, then their effectiveness is given further credence.

7.6. The future role of patriotic hackers in cyber conflict

Cyberwars may either be fought as a proxy to a 'real' kinetic war or alongside them. Cyber conflicts could be brought to bear, fought and brought to a conclusion much quicker than regular conflicts due to their unique nature. That is, with forces able to project globally at the speed of light, distance to target is of little relevance (Tennant, 2009). As developed or developing countries come to rely on their IT infrastructure more and more their threat exposure to cyberwar gets greater. Defending all these targets from cyber attack is problematic; there is no front and every target is equidistant to the enemy.

Some leaders believe that deterrence is key (anonymous, 2016a), whilst others are doubtful (anonymous, 2016d). What is clear is that with IoT gaining traction and Critical National Infrastructure becoming increasingly connected to cyberspace, the effects of any future cyberwar are becoming gradually more dramatic. This is recognised by the West (via NATO) and by Russia and China, amongst others, who are busy bolstering their cyber capabilities (Butler, 2013; Thomas, 2008).

The existence of non-state forces in future cyberwar is highly likely (Aschmann et al, 2015) and patriotic hackers, depending on their structure, will be used. There is a disconnect, though, between the West and more authoritarian regimes, with the latter being much more likely to utilise them. This is possibly down to the West's general disdain for irregular forces, or because the legal framework they operate within makes it difficult to sanction. The structure of patriotic hackers is important and Ottis (2011) lays out possible options as the Forum, the Cell and the Hierarchy. Each of these have better command and control but heavier overheads as you move through from the Forum to the Hierarchy. It is likely that Western regimes would find the latter more straightforward to justify.

Minor powers with low levels of resources may find patriotic hackers attractive as a Forum type setup; their cost effectiveness making up for weaker cyber capabilities that nonetheless compliment official powers.

Nevertheless, it is unlikely that any of the major powers will rely too heavily on patriotic hackers in a future cyberwar. The difficulty of commanding them coupled with the risk of them going out of control would preclude this. However, their usefulness would be more akin to traditional guerrilla forces. They would be used for conducting reconnaissance while maintaining plausible deniability and conducting nuisance attacks that are very difficult to entirely stop (Butler, 2013). They would also be used in combating other irregular forces such as hacktivists (Lysenko and Endicott-Popovsky, 2013). With the possibility of facing thousands of such attackers (Chansoria, 2012), defending nations must adapt; a possibility is that legal frameworks could be settled internationally to curtail their use. Pool (2013) and Kirsch (2012) both believe that agreed international laws to regulate a cyberwar are necessary, with the former in particular concerned of the consequences of failing to do this. Chayes (2015) and Droege (2013) both stress that proxy forces, such as patriotic hackers, should be identified as combatants in law so that existing statutes come into play, such as the UN's Geneva conventions of 1949. International agreement to limit cyber forces may be difficult to attain; Chayes (2015) compares it to the process of trying to control the proliferation of nuclear weapons – a tortuous process. Additionally, with most, if not all, of the UN Security Council having powerful cyber capabilities, their instinct to self-limit will not be strong. As respondent B stated, new international laws would be "…futile absolutely futile", seeing it as "…too difficult and too complex" to achieve. Until such laws come to pass, or attribution in the event of cyber attack becomes considerably more straightforward, proxy forces such as patriotic hackers will be a feature of future cyber conflicts.

7.7. Summary

This chapter has discussed key findings from the research undertaken for this thesis. In response to Objective 1, regarding the current state of research into patriotic hacking, it was found that there is no current, repeated definition of patriotic hackers. The author has attempted his own definition. It was found that, in contrast to hacktivists, there was not a wealth of research undertaken on patriotic hackers. However, by the author's own definition there are numerous, recent conflicts that have had patriotic hacker interventions. In relation to cyberwar and the legal framework surrounding it, there have been numerous studies conducted by military, legal and academic scholars.

Objective 2 intended to examine the toolkits and techniques used by patriotic hackers; although it found that they were common across all hacker types. It was ascertained that the majority of hackers used toolkits commonly available on the web with only a minority of gifted individuals who are actually writing the code that forms the basis of viruses, worms and Trojans. The techniques discussed included phishing, DDoS and physical delivery of viruses via a USB stick. The latter was found to be the preserve of those with non-casual links to nation-state security services due to its expense. It was decided that ransomware was not a typical tool used by patriotic hackers. The landscape that patriotic hackers operated in was touched on with reference to the field notes.

Objective 3 investigated the motivations of individuals involved in patriotic hacking. There was no discernible and existing in-depth research into motivations of patriotic hackers though some authors did touch on it as an aside. A list was compiled from the interview respondents and this was held up to inspection by the literature review. Each item in the list was investigated in turn. One contradiction inspected was the view that patriotic hackers would not use ransomware but one of their motivations was monetary gain. It was suggested that individuals utilising ransomware were cyber criminals, not patriotic hackers. Overall, the nationalistic motivations of patriotic hackers stood out as a class defining feature. The other ascribed motivations can also be found in hacktivists, cyber criminals etc. but nationalism is unique, in this context, to patriotic hackers.

The effectiveness of patriotic hackers in cyber warfare was the subject of Objective 4. It concluded that patriotic hackers were a part of Russia and Chinese military thinking and therefore must be considered effective by them, at least. Examples of patriotic hacker action in recent cyber conflicts (and 'real' conflicts) was summarised and an indication given of which groups would have access to the latest cyber weapons.

Objective 5 was looked at last and covered the future role of patriotic hackers in cyber conflicts. It summarised that their future use was highly likely; the pros of using them and the expanding number of targets ensured this. However, the distrust of the West in using such forces was also highlighted.

8. Conclusion

8.1. Introduction – The Aim

The aim of this project was to critically evaluate the current use of patriotic hacking. This chapter examines the objectives outlined in the introduction and determines whether the research succeeded in achieving these. Any important and pertinent issues raised during the research are also explored.

8.2. Meeting the objectives

8.2.1. Objective 1 - Analyse the current state of research into patriotic hacking

The literature review revealed a large number of papers and studies regarding hacking in general, but little pertaining directly to patriotic hackers. The lack of direct patriotic hackers studies demonstrate that more research in this field is required, especially when considered against the importance numerous studies place in cyber conflict, of which patriotic hackers are sure to play a part. The phrase patriotic hackers was shown to be a contentious one with different authors having different views on its definition and, indeed, the term itself. The dimensions of ethnicity, religion and political stance were all attributed as defining patriotic hackers during different studies but eventually the consensus emerging from the literature was that the key attribute was the political/national dimension.

There was a great deal of literature that dealt with cyber conflicts, cyberwar and the geopolitical risks involved. Such studies allowed the context that patriotic hackers operate in to be demonstrated. They showed the importance powerful countries place in prosecuting cyberwar (such as the USA and China) and exposed the vulnerabilities that were expressed by weaker countries (e.g. Estonia). The use of irregular cyber forces, and patriotic hackers can be considered as such, was studied primarily by research groups associated with numerous militaries. Various studies were shown to have highlighted how the effectiveness of such forces in any future cyberwar depend on how they are organised and controlled. This thesis also explored literature discussing the cyber weapons that hackers are using; such weapons can be considered universal and are open to all the different varieties of hackers, including patriotic hackers. Some studies were sanguine about this weaponry, but the field of cyber weapons is fast paced and such literature already appears out of date. Some research compares cyberwar with nuclear war and explores the parallels in the field of deterrence and legal frameworks.

A substantial body of literature focused on the legalities of cyber conflicts and the actors taking part in them. Such studies came from a variety of sources including defence specialists, charities and the legal profession. This section of the literature review appears comprehensive with a great deal of literature to study from. However, reflecting the overall review, it was again lacking in direct studies about patriotic hackers and more oblique references to them had to be gathered. Care had to be taken to ensure that the Western narrative of an aggressive China and Russia in cyberspace does not mean the actions by the West were ignored. Indeed, studies also showed that the USA was active in cyberspace and had a top-tier capability similar to that of China and Russia. It was also clear that NATO members are bolstering their cyber capabilities and take the cyber domain seriously.

8.2.2. Objective 2 - Determine the toolkits and techniques the hackers use, highlighting the flaws, strengths and weaknesses

Literature was considered, alongside the field studies and interviews, to meet this objective. The field studies demonstrated that there were numerous Dark Web sites available to download specific tools from. Such sites were found to be easily accessible as long as TOR was used. Field studies also found forums and websites where techniques could be discussed and learnt from other hackers. Such websites involved were part of the Dark Web and operated using secrecy and anonymity. This meant that information gathered from them could not be verified and had to be treated with caution. Nonetheless, it was clear that this study was only scraping the surface of what is a huge communications space. It can be assumed that within this labyrinthine structure, many cyber weapons or tools can be found and, if necessary, downloaded or purchased by the cognisant.

Tools available to hackers were also elicited from literature and interview respondents. Complicated and potent malware has now been derived from Stuxnet and is available in the public domain. Such malware can be used to spy on people, to steal personal details, to collect password via key logging or to cause damage to network attached infrastructure. This demonstrates a flaw in developing such cyber weapons by advanced military departments, in that they can be developed far beyond what was originally envisaged.

The strengths and weaknesses of another disruptive tool, DDoS, were discussed. Although a blunt tool, it is still much used by hackers to punish corporations or as cover for more covert attacks. Whilst is has been in use since 1997, effective defence against it is still limited and it shows no signs of abating.

Phishing is a relatively simple technique that hackers could utilise to gain unauthorised access to systems. Its popularity with hackers was shown in literature and the field studies and causes problems for organisations and individuals that training only partly mitigates. Cases using more advanced spearphishing techniques were also discussed.

Interview respondents indicated that with software such as Kali widely available, hackers do not need to be technically proficient in order to use powerful tools such as key loggers and password crackers. Additionally, if a patriotic hacker group is closely connected to a state's security services, powerful cyber weapons not otherwise widely available could be given to them. This premise is consistent with the actions of some Russian APTs.

8.2.3. Objective 3 - Explain the perceived motivations of individuals involved in patriotic hacking

Literature and interviews were considered to meet this objective. It was hoped that the field studies would allow a current patriotic hacker to be interviewed but events meant that this did not happen. This is likely due to their secretiveness and, possibly, that such hackers do not visit English language websites; evidence suggests they are more likely to be from the Ukraine, Russia, China or other predominantly non-English speaking countries. The motivations found in literature were focused on hacktivists or hackers in general. There was little available specifically on patriotic hackers. The research that was found viewed patriotic hackers' motivation as patriotism and little else. A more comprehensive view was given by the interview respondents who listed five different motivations, one of which was equivalent to patriotism; this was interpreted as nationalism. Four of the five motivations (monetary gain, recognition/kudos, political/ideological and nationalism) could be tied-in indirectly with the literature, however, coercion could not. This may be because the literature review did not focus on cybercrime and it would be beneficial if future research was able to

concentrate on this area. Even so, hints at coercion were found in the field study and were included in the analysis.

The most contentious motivation listed was that of monetary gain. A rejection of using hacking for personal wealth creation is at the heart of hacktivism. This self-righteousness can also be laid at the feet of patriotic hackers but only if they are hacking solely for patriotic reasons. Otherwise, they become mere mercenaries, hacking in pursuit of money. There is certainly evidence that some patriotic hackers are for hire. Examples, however, of patriotic hackers acting in conflicts, such as the Israeli/Palestinian troubles, suggest there is a patriotic action and reaction going on with the opposing sides. Actions such as the hacking of Israeli websites were not done for monetary gain, but rather as a visceral reaction, to be seen to be doing something. This also feeds into the idea that some patriotic hackers are after recognition for their actions. This could come from their home country or, probably more likely, from fellow hackers acting in a patriotic cause.

8.2.4. Objective 4 - Assess the effectiveness of patriotic hacking in cyber warfare

Judging the effectiveness of patriotic hackers engaged in a cyberwar is not easy. Their furtiveness and the difficulty of attribution means a lot of the literature is speculative and reliant on assumptions. However, using the available literature combined with the insights of the interview respondents allowed an assessment to be made. Focusing on the countries involved, the cyber weaponry and low intensity conflicts helped to validate some of the assumptions and give an indication of patriotic hackers' effectiveness. This was corroborated by the stance of two major powers who utilise such hackers; Russia and China.

A key determinant in how effectively patriotic hackers operate is their structure. Research indicated that loose collections of individuals would be quicker to stand-up when a crisis occurs whilst more organised groups would take longer but be easier to command and control.

Unlike physical forces, patriotic hackers' attacks operate at the speed of light and have global reach. They also operates under a cloak of secretiveness that means direct attribution to the sponsoring nation is problematic. Conversely, their use during a crisis could precipitate a kinetic reaction and lead to further escalation; similar to a 'cold' war leading to a 'hot' one.

An additional key factor in determining the effectiveness of patriotic hackers is the level of cyber weaponry they can deploy. Those with close links to the host nation's security services can expect access to advanced cyber weapons. A full cyberwar has not yet occurred and the capabilities of such weapons can only be extrapolated from examples in more minor cyber conflicts, such as Stuxnet's use against Iranian nuclear reactors.

Whether Western governments can sanction the use of patriotic hackers is an interesting point. Literature suggests that Western governments may find it difficult to avoid press scrutiny and whistle-blowers exposing such forces. Conversely, the use of instruments such as extraordinary rendition has been used by countries such as the USA in times of war. This demonstrates that making a decision on whether Western governments will utilise patriotic hackers difficult to do and further research would be warranted in this area. It is straightforward to find evidence for more authoritarian countries using such forces, specifically China and Russia.

8.2.5. Objective 5 - Discuss the future role of patriotic hackers in cyber conflict

The last objective was informed by all the research strands undertaken. The premise that cyberwars may or may not be fought with a corresponding kinetic action was made. Either of these options would likely see the use of patriotic hackers by one or more sides. With countries such as Russia and China having patriotic hackers integrated within their Armed Forces suggests that active

consideration of these irregular forces has been given by all advanced militaries. However, there is some doubt over whether Western countries will be able to utilise them. Authoritarian regimes will doubtless find it easier to justify their inclusion in the order of battle whilst countries with fewer resources will see their cost effectiveness as hard to ignore.

However, whilst their presence in a future cyberwar is likely, their overall impact may be limited. The difficulty of command and control means patriotic hackers would be best employed as cyber guerrillas, conducting reconnaissance and undertaking nuisance attacks. A challenge to any military who use them is how much to invest them with the latest cyber weapons. The CIA backed the Afghanistan mujahedin who turned against their original sponsors and morphed into Al Qaeda. There is a danger that patriotic hackers could undertake a similar journey if the political landscape changed during a conflict. These considerations should be at the forefront of any discussion on the structure of patriotic hackers. Whilst a more hierarchical structure takes time to form and has higher overheads, the level of command and control is greater. This means that such a structure could be invested with the latest technology and their effectiveness enhanced. Conversely, utilising loose groups of politically unstable hackers and equipping them with advanced cyber weapons has the potential to cause damage to the host nations' own forces or allies. This can be mitigated by not allowing troops access to such weapons and, recognising their limitations, using them differently. An example would be using small groups of patriotic hackers to instigate propaganda and respond to any challenges from hacktivist groups. This shows that patriotic hackers can be flexible depending on their structure and it is likely that any future cyberwar will showcase the different possible structures.

8.3. Summary

8.3.1. Contributions to theory

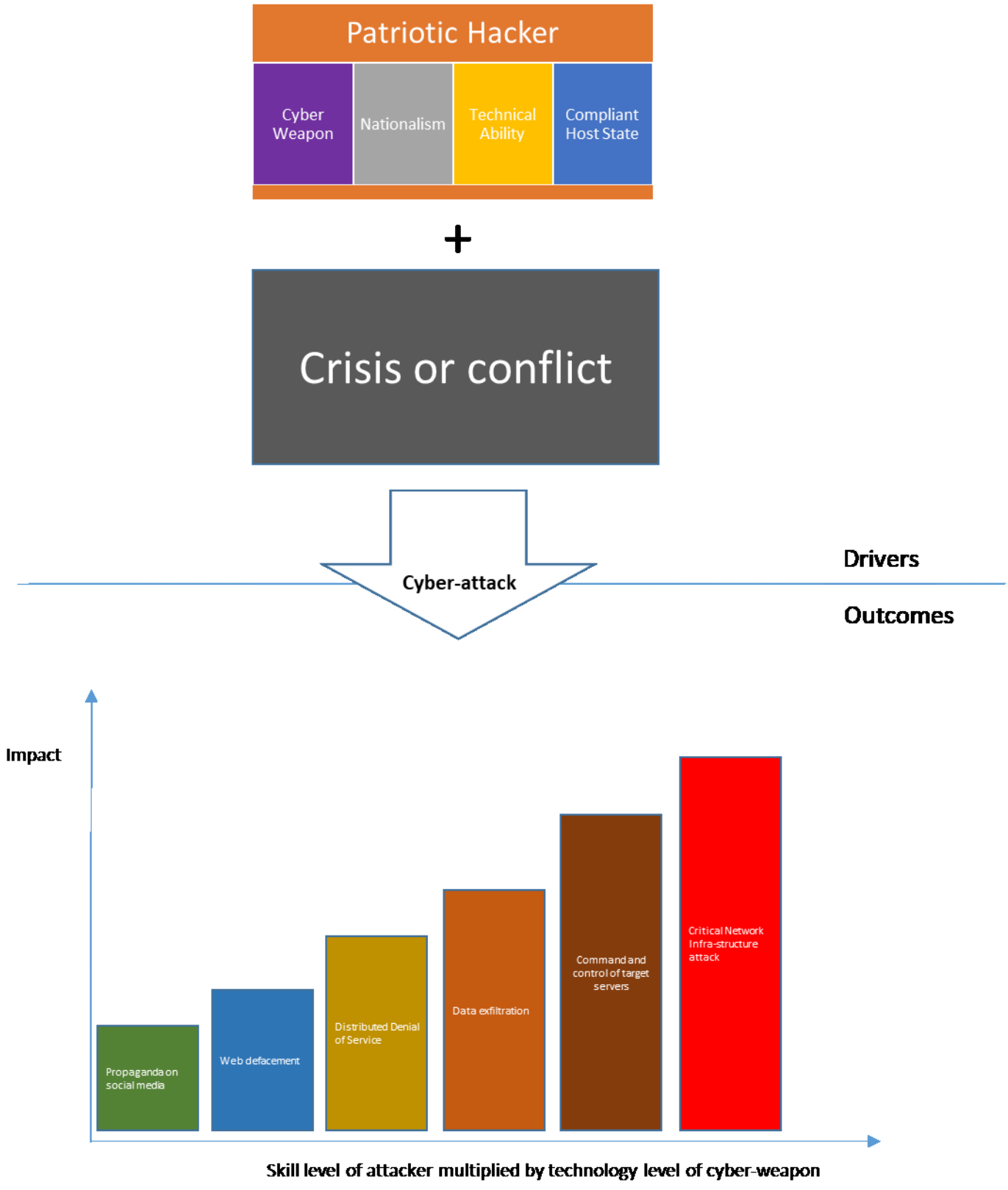
A lot of the literature studied covers the topics of cyberwar, hacktivists, cyber weapons and the law associated with cyberspace. However, none of the literature has focused on patriotic hackers and their effectiveness in future cyber conflicts. This study has concentrated on these elements, allowing a theoretical model to be synthesised.

The research has found that to be a patriotic hacker an individual would need a certain level of technical ability, an effective cyber weapon, a compliant nation to operate from and the requisite motivation. The defining motivation of a patriotic hacker is their nationalism and this is what separates them from other hacker types.

When patriotic hackers find themselves nationalistically associated with one side during a conflict or crisis then the likely outcome is a cyber attack. Such an attack would have different impacts on the victim state depending on both the attackers' skill level and the technological level of the cyber weapon deployed. As this multiplier increases then the impact would move from low-tier propaganda, through mid-level nuisance and disruption to top-tier CNI attacks that could result in death and injury. It should be noted that such attacks would follow the Power-Law tenets of Bibighaus (2015). That is, a large number of low skilled patriotic hackers would be less effective than one highly skilled individual.

The above findings allow a theoretical model for patriotic hackers to be developed and this is illustrated in figure 19 below:

Figure 19 - Theoretical model for patriotic hacking



8.3.2. Contributions to practice

It can be concluded that future conflicts comprising cyberspace elements are likely to see the use of patriotic hackers; though their use may not always be sanctioned by the host country. The ever growing interconnectedness of both developed and developing countries means that nations are becoming more exposed to cyber attack from such actors. This study recommends that the outlawing of patriotic hackers would be a good first step in the de-escalation of threats in cyberspace.

When patriotic hackers are closely aligned to state security forces, or otherwise have access to advanced cyber weapons, organisations targeted by them can do little to protect themselves. As such they should direct their resources elsewhere and not worry unduly about this type of threat. The organisation's host nation will be better placed to respond to such attacks.

The law surrounding cyberwars is thin and does not adequately protect civilians from the consequences of patriotic hacker action. Conversely, the will of major cyber powers to make changes to international law appears to lack leadership and motivation. Nonetheless, the United States of America and China, as the superpowers, should instigate proceedings to reach a universal treaty banning any effort to destroy cyberspace and the Internet of Things. This would be in their own national interests. Other nations should then follow.

The development of powerful cyber weapons has left nations exposed to cyberspace in a precarious position, which many have recognised. Numerous nations, large and small, are bolstering their own cyber forces, including recruiting patriotic hackers, as a result. If the tenets of deterrence work in a similar way to the nuclear Mutually Assured Destruction (MAD) theory, then these actions make sense. However, there are some experts and leaders who point out the deficiencies in this thinking, arguing that such an approach to deterrence does not work in cyberspace and a build-up of cyber capabilities will make cyberwar more, not less, likely. To counter this, nations, preferably led by the UN Security Council, need to control the use of cyber weapons by using new international treaties, in a similar manner to the non-proliferation of nuclear weapons' treaties already in existence.

8.4. Recommendations for further study

A further study is recommended to be undertaken to look at the subject of escalation during a crisis and how the use of patriotic hackers impacts this. This could focus on whether using such forces create the chance for misinterpretation, leading to escalation.

An additional study is necessary to explore the motivations of patriotic hackers and in particular whether coercion and religion are a consideration. The lack of literature found on coercion would, therefore, require investigation into online criminal activities to find similar situations. It is likely that online criminals could face similar pressure to patriotic hackers in circumstances of state action against them. The aspect of religion as a motivation has been touched on in this research project. Is it contained within the motivation of ideology or should it be treated separately? Religion plays a big part in the perceived motivations of different actors in the Middle East. Whether this is a defining motivational factor or whether it is subsumed by the political and ideological listed motivations is worth exploring further.

Finally, it would be beneficial to examine whether Western governments use patriotic hackers. The evidence uncovered during this research project was equivocal, and more time is needed to look into this area. During such a study, an interesting question would be: is Edward Snowden a patriotic hacker?

9. Glossary

IoT - Internet of Things. This is a system of linked computing devices that have the ability to transfer data over the network without human interaction

DDoS - Distributed Denial of Service. The intentional paralysing of a network by flooding it with requests for a response. Distributed means lots of different computers are used to conduct the attack.

USB - Universal Serial Bus stick. A small external flash drive

NATO - North Atlantic Treaty Organization

NSA - National Security Agency (of the USA)

CIA - Central Intelligence Agency (of the USA)

FBI - Federal Bureau of Investigation (of the USA)

HTTP - Hypertext Transfer Protocol

Warez - Pirated software

TOR - The Onion Router. An open source software program designed to protect privacy

Deep Web - a part of the Internet that is hidden from orthodox search engines, it may be encrypted or otherwise hidden from traditional search engines and is the aggregate of private databases, unindexed websites, and additional unlinked content

Dark Web - a part of the Internet that is hidden from search engines and is only accessible with a special web browser such as TOR

APT - Advanced Persistent Threat. A cyber attack that is launched by an attacker with substantial organization, means, and incentive to carry out an assault over a prolonged time

Cold war - a state of political hostility between nations categorised by propaganda, threats, and other measures short of open warfare

Hot war - open warfare usually involving loss of life

10. References

Abdallah, C. and Langley, A. (2014) 'The Double Edge of Ambiguity in Strategic Planning.' *Journal of Management Studies*, 51(2)

Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. (2000) Presentation at Washington,

Al-Rawi, A. K. (2014) 'Cyber warriors in the Middle East: The case of the Syrian Electronic Army.' *Public relations review*, 40(3) pp. 420 - 428.

Alaszewski, A. (2006) *Using Diaries for Social Research.* London: Sage.

Alford, L. (2001) *Cyber warfare: a new doctrine and taxonomy*. US Air Force. [Online] [Accessed http://www.crosstalkonline.org/storage/issue-archives/2001/200104/200104-Alford.pdf

Allen, P. (2003) 'The Palestinian-Israel: cyberwar.' *Military Review*, 83.2 p. 52.

Alperovitch, D. (2016) Bears in the Midst: Intrusion into the Democratic National Committee. In: Crowdstrike. Vol. 2016.

Anon. (2003) 'Cyber attacks accompany war in Iraq.' *Information Management & Computer Security*, 11(4) p. 201.

Anonymous. (2017) *What is the difference between viruses, worms, and Trojans?* : Symantec. [Online] [Accessed https://support.symantec.com/en_US/article.TECH98539.html

Ashenden, D. (2011) 'Cyber Security: Time for Engagement and Debate.' *In European Conference on Information Warfare and Security.* Vol. 11: Academic Conferences International Limited, pp. 11 - V.

Barata, N. J. C. (2015) "Patriotic Hackers: Non-State Actors Fighting Wars For States?" Web: University of Amsterdam.

Barbour, R. (2003) 'The Newfound Credibility of Qualitative Research?' *Sage journals*, 13(7) pp. 1019 - 1027.

Barbour, R. (2013) *Introducing qualitative research: a student's guide.* London: SAGE Publications Ltd.

Barnard-Wills, D. (2011) 'This is not a Cyber war, its a...? Wikileaks, Anonymous and the Politics of Hegemony.' *In European Conference on Information Warfare and Security*: Academic Conferences International Limited, pp. 17 - VI.

Barnhill, J. H. 'The Evolution of Cyber Warfare: International Norms for Emerging Technology Weapons.' *Air & Space Power Journal*, 30(3) p. 85+.

Beech, H.: [Online] [Accessed

Beech, H. (2013) *China's Red Hackers: The Tale of One Patriotic Cyberwarrior*. Time. [Online] [Accessed on 30/11] http://world.time.com/2013/02/21/chinas-red-hackers-the-tale-of-one-patriotic-cyberwarrior/

Bibighaus, D. L. (2015) 'How Power-Laws Re-Write The Rules Of Cyber Warfare.' *Journal of Strategic Security*, 8(4) pp. 39 - 52.

Blaxter, l., Hughes, C. and Tight, M. (2002) *How to Research.* Buckingham, UK: Open University Press.

Borghard, E. D. and Lonergan, S. W. (2016) 'Can States Calculate the Risks of Using Cyber Proxies?' *Orbis*, 60(3) pp. 395 - 416.

Breene, K. (2016) *Who are the cyberwar superpowers?* : World Economic Forum. [Online] [Accessed https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers

Buchan, R. (2016) 'Cyber Warfare and the Status of Anonymous under International Humanitarian Law.' *Chinese Journal of International Law*, 15(4) pp. 741-772.

Butler, S. C. (2013) 'Refocusing cyber warfare thought.' *Air & Space Power Journal*, 44

Caffyn, G. (2015) *Bitcoin on the Dark Web: The Facts*. Coindesk. [Online] [Accessed https://www.coindesk.com/bitcoin-on-the-dark-web-the-facts/

Campbell, L., Mehtani, S., Dozier, M. and Rinehart, J. (2013) 'Gender-Heterogeneous Working Groups Produce Higher Quality Science.' *PLoS ONE*, 8(10)

Cantil, J. K. (2016) 'Honing cyber attribution: a framework for assessing foreign state complicity.' *Journal of International Affairs*, 70, 2016 Winter//, p. 217+.

Carr, J. (2012) *Inside cyber warfare.* 2nd ed.: O'Reilly Media Inc.

Chansoria, M. (2012) ''Defying
Borders in Future Conflict in East Asia: Chinese Capabilities in the Realm of
Information Warfare and Cyber Space.' *The Journal of East Asian affairs*, 26(1) pp. 105 - 127.

Chayes, A. (2015) 'Rethinking Warfare: The Ambiguity of Cyber Attacks.' *Harvard National Security Journal*, 6 pp. 474 - 519.

Chen, T. M. (2010) 'Stuxnet, the real start of cyber warfare?' *IEEE Network*, 24(6) pp. 2 - 3.

Colarik, A. and Janczewski, L. (2011) *Developing a grand strategy for cyber war.*

Colarik , A. M. and Janczewski , L. (2012) 'Establishing Cyber Warfare Doctrine.' *Journal of Strategic Security*, 5(1) pp. 31-48.

Coleman, E. G. (2014) *Hacker, hoaxer, whistleblower, spy: the many faces of Anonymous.* New York;London;: Verso.

Cyber Warfare Challenges and the Increasing Use of American and European Dual-Use Technology for Military Purposes by the People's Republic of China (PRC). (2011) Presentation at archives, republicans, foreign affairs,

Dahan, M. (2013) 'Hacking for the Homeland: Patriotic Hackers Versus Hacktivists.' *International Conference on Information Warfare and Security - Journal Article*, p. 51.

Davies, M. B. (2007) *Doing a successful research project: using qualitative or quantitative methods.* Basingstoke [England] ; New York: Palgrave Macmillan.

Deibert, R. and Rohozinski, R. (2010) *Shadows in the Cloud*. http://www.tibetcorps.org/files/Resources/shadows-in-the-cloud.pdf: [Online] [Accessed http://www.tibetcorps.org/files/Resources/shadows-in-the-cloud.pdf

Denning, D. (2015) 'The rise of hacktivism.' *Georgetown Journal of International Affairs*,

Denscombe, M. (2002) *Ground rules for good research.* Buckingham, UK: Open University Press.

Droege, C. (2013) 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians.' *International Review of the Red Cross*, 94(886)

Dunn Cavelty, M. and Jaeger, M. D. (2015) '(In)visible Ghosts in the Machine and the Powers that Bind: The Relational Securitization of Anonymous.' *International Political Sociology*, 9(2) pp. 176-194.

Décary- Hétu, D., Morselli, C. and Leman-Langlois, S. (2012) 'Welcome to the Scene A Study of Social Organization and Recognition among Warez Hackers.' *49*, 3

Eddy, N. (2015) *Privacy Concerns Over Internet of Things Rises*. http://www.eweek.com/small-business/privacy-concerns-over-internet-of-things-rises.html: eweek. [Online] [Accessed http://www.eweek.com/small-business/privacy-concerns-over-internet-of-things-rises.html

Etherington, D. a. C., Kate. (2016) *Large DDoS attacks cause outages at Twitter, Spotify, and other sites*. TechCrunch. [Online] [Accessed https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

Fassin, D. (2013) 'Why Ethnography Matters: On Anthropology and Its Publics.' *Cultural Anthropology*, 28(4)

Fowler, F. J. and Mangione, T. W. (1990) *Standardized Survey Interviewing.* Thousand Oaks, United States: SAGE Publications Inc.

Fox-Brewster, T. (2015) *Equation = NSA? Researchers Uncloak Huge 'American Cyber Arsenal'*. Forbes. [Online] [Accessed https://www.forbes.com/sites/thomasbrewster/2015/02/16/nsa-equation-cyber tool-treasure-chest/#1447d5e0417f

Giesen, K. (2013) 'Towards a Theory of Just Cyberwar.' *In International Conference on Information Warfare and Security*: Academic Conferences International Limited, pp. 65 - VII.

Gilbert, D. (2015) *Equation Group: Meet the NSA 'gods of cyber espionage'*. International Business Times. [Online] [Accessed http://www.ibtimes.co.uk/equation-group-meet-nsa-gods-cyber espionage-1488327

Gillham, B. (2000) *The Research Interview.* UK: Bloomsbury.

Gompert, D. C. and Libicki, M. (2014) 'Cyber Warfare and Sino-American Crisis Instability.' *Global Politics and Strategy*, 56(4) pp. 7-22.

Government, U. (2015) *Developing our capability in cyber security.* UK: Department for Culture, Media & Sport.

Gutmann, E. (2010) 'Hacker nation: Chinas cyber assault.' *World Affairs*, 173(1) pp. 70-79.

Haraty, R. A. and Zantout, B. (2014) 'The TOR data communication system.' *Journal of Communications and Networks*, 16(4) pp. 415-420.

Harvey, L. (2011) 'Intimate reflections: private diaries in qualitative research.' *Qualitative Research*, 11(6), 2011/12/01, pp. 664-682.

Hejase, A. J., Hejase., H. J., Hejase., J. A., style="border-collapse: p. (2015) 'Cyber warfare awareness in Lebanon: Exploratory research.' *International Journal of Cyber Security and Digital Forensics*, 4(4) p. 482+.

Henry, W., Stange, J. and Trias, E. (2010) 'Pearl Harbor 2.0: When Cyber Acts Lead to the Battlefield.' *In International Conference on Information Warfare and Security*: Academic Conferences International Limited, pp. 148 - 155.

Heracleous, L. (2006) 'A Tale of Three Discourses: The Dominant, the Strategic and the Marginalized.' *Journal of Management Studies*, 43(5)

Hille, K. (2017) *Putin concedes 'patriotic' hackers might target foreign elections*. Financial Times. [Online] [Accessed on 04/08/2017] https://www.ft.com/content/f607ac6c-46e6-11e7-8519-9f94ee97d996

Holt, T. J. and Kilger, M. (2012) 'Examining Willingness to Attack Critical Infrastructure Online and Offline.' *Crime & Delinquency*, 58(5) pp. 798 - 822.

Holt, T. J., Bossler, A. M. and May, D. C. (2012) 'Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance.' *American Journal of Criminal Justice*, 37(3) pp. 378 - 395.

Iasiello, E. (2016) 'China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities.' *Journal of Strategic Security*, 9(2) pp. 45-69.

'Is cyber defense possible?'. (2016) *Journal of International Affairs*, 70, 2016 Winter //, p. 182+.

Jordan, T. (1998) 'A sociology of hackers.' *Socialogical Review*, 46(4) pp. 757-780.

Judith, B. (2006) 'Doing your research project.' *British Journal of Educational Technology*, 37(5)

Kan, P. R. (2013, 2013 Autumn). Cyberwar to Wikiwar: battles for cyberspace. *Parameters, 43,* 111+.

Karatzogianni, A. (2012) 'Cyberconflict and the Future of Warfare.' *In* Kobtzeff, H. G. a. O. (ed.) *Ashgate Research Companion to War*. Ashgate,

Kenney, M. (2015) 'Cyber Terrorism in a Post-Stuxnet World.' *Orbis*, 59(1) pp. 111 - 128.

Kesan, J. P. and Hayes, C. M. (2012) 'Mitigative counterstriking: self-defense and deterrence in cyberspace.' *Harvard Journal of Law & Technology*, 25(2) p. 520.

Kirsch, C. M. (2012) 'Science fiction no more: cyber warfare and the United States.' *Denver Journal of International Law and Policy*, 40(4) p. 620.

Knake, R. and Segal, A. (2016) 'How the next U.S. President can contain China in cyberspace.' *Journal of International Affairs*, 70, 2016 Winter //, p. 21+.

Knopová, M. and Knopová, E. (2014) 'The Third World War? In The Cyberspace. Cyber Warfare in the Middle East.' *Acta Informatica Pragensia*, 3(1) pp. 23 - 32.

Kostyuk , N. (2014) 'International and Domestic Challenges to Comprehensive National Cybersecurity: A Case Study of the Czech Republic.' *Journal of Strategic Security*, 7(1) pp. 68 - 82.

Kozlowski, A. (2014) 'Comparative
analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan.' *European Scientific Journal February 2014*, 3(ISSN: 1857 - 7431)

Krebs, B. (2016) *This is Why People Fear the 'Internet of Things'*. http://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/: [Online] [Accessed http://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/

Kryger, A. (2017) 'Strategy development through interview technique from narrative therapy.' *Journal of Organizational Change Management*, 30(1) pp. 4-14.

Kshetri, N. (2013) 'Cybercrime and cyber security issues associated with China: some economic and institutional considerations.' *Electronic Commerce Research*, 13(1) pp. 41-69.

Kvale, S. (1996) *InterViews: an introduction to qualitative research interviewing.* Thousand Oaks, Calif.; London: Sage.

Lysenko, V. and Endicott-Popovsky, B. (2012) 'Hackers at the State Service: Cyberwars Against Estonia and Georgia.' *International Conference on Information Warfare and Security - Journal Article*, p. 42.

Lysenko , V. and Endicott-Popovsky , B. (2013) 'Action and Reaction: Strategies and Tactics of the Current Political Cyberwarfare in Russia.' *In International Conference on Cyber Warfare and Security*: Academic Conferences International Limited, pp. 269 - VIII.

Mansfield-Devine, S. (2013) 'Interview: Joe Ferrara – fighting phishing.' *Computer Fraud & Security*, 2013(7) pp. 17 - 20.

Marks, P. (2011) *Dot-dash-diss: The gentleman hacker's 1903 lulz*. New Scientist. [Online] [Accessed https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/

Marshall, P. (2002) *Research Methods.* Mumbai, India: Jaico Publishing House.

Masters of the cyber universe; Cyber hacking. (2013, 2013/04/06/). *The Economist, 407,* 12(US).

Mattice, L. (2013) 'The NSA, Cyber Espionage, Hackers and More - A Frank Look at the World Today with Congressman Mike Rogers.' 50, p. 14. [Online] 10. [Accessed

McDowell, M. (2009) *Understanding Denial-of-Service Attacks*. Official website of the Department of Homeland Security: [Online] [Accessed https://www.us-cert.gov/ncas/tips/ST04-015

McMillan, S. (2013) 'Running a war by computer: cyber warfare and its dilemmas.' *New Zealand international review*, 38(3) pp. 2 - 4.

Menn, J. (2015) *Russian researchers expose breakthrough U.S. spying program*. Reuters. [Online] [Accessed https://www.reuters.com/article/us-usa-cyberspying-idUSKBN0LK1QV20150216

Michael, J. B., Sarkesain, J. F., Wingfield, T. C., Dementis, G. and Sousa, G. N. B. (2010) 'Integrating Legal and Policy Factors in Cyberpreparedness.' *Computer*, 43(4) pp. 90-92.

Noy, C. (2008) 'Sampling Knowledge: The Hermeneutics of Snowball Sampling in Qualitative Research.' *International Journal of Social Research Methodology*, 11(4)

Olson, P. (2013) *We Are Anonymous.* London: William Heinemann.

Ottis, R. (2010) 'Proactive Defense Tactics Against On-Line Cyber Militia.' *In Proceedings of 9th European Conference on Information Warfare and Security,.* Vol. J. Thessaloniki, Greece: Demergis,, p. 233.

Ottis, R. (2011) 'Theoretical Offensive Cyber Militia Models.' *In International Conference on Information Warfare and Security.* Vol. 307: Academic Conferences International Limited, pp. 307 - VII.

Owens, W., Dam, K. and Lin, H. (2009) 'Escalation Dynamics and Conflict Termination in Cyberspace.' *In Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington: National Academies Press,

P., C., D., L., D., C. and C., Y. (2012) On cyber warfare. Chatham House.

Pool, P. (2013) 'War of the cyber world: the law of cyber warfare.' *International Lawyer*, 47(2) p. 299.

Raether, R. I., Jr. (2008, 2008 September-October). Data security and ethical hacking: points to consider for eliminating avoidable exposure. *Business Law Today, 18,* 55+.

Rege, A. (2014) 'Digital information warfare trends in Eurasia.' *Security Journal*, 27.4 pp. 374-398.

Robinson, M., Jones, K. and Janicke, H. (2015) 'Cyber warfare: Issues and challenges.' *Computers and Security*, 49 March 2015, pp. 70 - 94.

Robson, C. (2006) 'Real World Research.' *Directory of Open Access Journals*, 3(1)

Sample, C. (2013) 'Applicability of Cultural Markers in Computer Network Attack Attribution.' *In European Conference on Information Warfare and Security.* Vol. 361: pp. 361 - XIII.

Scharf, M. (2015) 'A discussion on cyber warfare.' *Case Western Reserve Journal of International Law*, 47(1) p. 319.

(2009) *Tallinn Manual Process.* Tallinn: Cambridge University Press. (Schmitt, M. Report)

Seebruck, R. (2015) 'A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model.' *Digital Investigation*, 14 pp. 36 - 45.

Seigfried-Spellar, K. C., O'Quinn, C. L. and Treadway, K. N. (2015) 'Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students.' *Behaviour & Information Technology*, 34(5), 2015/05/04, pp. 533-542.

Sela-Shayovitz, R. (2012) 'Gangs and the Web: Gang Members' Online Behavior.' *Journal of Contemporary Criminal Justice*, 28 pp. 389 - 405.

Steinmetz, K. and Gerber , J. (2015) '"It Doesn't Have to Be This Way": Hacker Perspectives on Privacy.' *Social Justice*, 41(3) pp. 29 - 51.

Tennant, D. (2009) 'The fog of (cyber) war: cybermilitias, black hat hackers and other non-nation-state bad guys blur the lines on the virtual battlefield.' *Computerworld, Inc.*, 43 p. 28.

'The consequences of cyber attacks.' (2016) *Journal of International Affairs*, 70, 2016 Winter //, p. 175+.

'The risk of cyber war and cyber terrorism.' (2016) *Journal of International Affairs*, 70, 2016 Winter //, p. 179+.

Thomas, T. L. (2008) 'China's electronic long-range reconnaissance.' *Military Review*, 88(6) p. 47.

Thomson, I. (2017) *Shadow Brokers hike prices for stolen NSA exploits, threaten to out ex-Uncle Sam hacker*. The Register. [Online] [Accessed on 28/07/2017] https://www.theregister.co.uk/2017/06/29/shadow_brokers_threaten_nsa_hacker/

Weil, S. and Shalva, W. (2006) 'Review: Andy Alaszewski (2006). Using Diaries for Social Research.' *Forum, qualitative social research*, 7(4)

Weissman, C. G. (2016) *We Asked Executives About The Internet Of Things And Their Answers Reveal That Security Remains A Huge Concern*. Business Insider. [Online] [Accessed http://www.businessinsider.in/We-Asked-Executives-About-The-Internet-Of-Things-And-Their-Answers-Reveal-That-Security-Remains-A-Huge-Concern/articleshow/45959921.cms

Čižik, T. (2017) 'Baltic States - How to React to "New Warfare" in the Context of the Article V?' *Slovak Journal of Political Sciences*, 17(2) pp. 184 - 201.

11. Appendices

11.1. Appendix I Interview One

SW: Sam thanks very much for agreeing to talk to me. What's your background in cyber security, how did you come into cyber security?

SR: Essentially I enrolled in cyber security at <COMPANY X>, I had 5 to 6 years' experience building up in a range from the bottom end of the spectrum. I kind of ended up in it by chance via various job applications, I'm sure you're aware of the process.

SW: Yeah, most people don't set out to be in cyber security, they tend to fall into it.

SR: Yeah, it's an area where it is more a way of thinking, rather than a vocation. It's actually much better to be creative thinking rather than anything over technical such as computing, which means you get a very wide skill set with a wide variety of different types of individuals involved in it.

SW: So did you do any roles before this one that lead you into it?

SR: Well I've only been in <COMPANY X> for two years, I worked in a small firm for three years before that; I was taken on as a junior for three years in a small company before it went bust but that's completely different. It's a different matter. But, before that I was working in Homebase doing retail, completely different…

SW: Can I ask what your educational background was? Was it in computing or something completely different?

SR: It was a maths degree, obviously it was 2008 so just after the crash and so I ended up in a bit of a…

SW: It was tough times…

SR: Yeah.

SW: Did you ever sort of feel you are interested in cyber security or did this job just come up and you took it?

SR: It's sort of something that you have to have an interest in beforehand, it kind of comes about, it came about, kind of, at union when you start poking around with various bits and pieces. And then you kind of nurture it, I had a conversation with Ashley, and IT professional a company near Oxford and it kind of ran from there. And that kind of shaped the direction of where I was looking for.... and with various institutions being not that far from Cheltenham…

SW: GCHQ?

SR: One of them. There is a wealth of experience and lots of them come from the private sector into the public sector, and from private companies, means that that area is ripe for developing and nurturing those kind of skills. Rather than other background areas, for nurturing the skills…

SW: And what's your role now, at <COMPANY X>?

SR: Currently it's managing the cyber security, umm, cyber defence services which is essentially, (unintelligible) and specifically I have a role which is integrating those which are outside of London, working with (name at <COMPANY X>, redacted) working as a bridge between specialist technical services and…

SW: Is it a bit like pre-sales consultancy?

SR: No that's more <PERSON B's> role, I kind of take on from there, I do the technical scope and technical lead. One of the things about <COMPANY X> is that it doesn't have a sales model, it doesn't have a specific sales team, individuals are responsible for their own engagements. So the clients I work for, I have to manage the budgets, so it's after the pre-sales I have to work out who the most appropriate person or resource is, and then work out the strategy, to make, to improve them as a whole. To get them to understand where they can best, rather than a lot of firms where they commoditise them, actually that's one of the problems with the industry at the moment. It's that it's become very commoditised. It's they want to have this problem looked at, who do I go to?

SW: Yeah.

SR: Which makes it a very, er, messy place. And this means it's rife with bad consultancy because people, its chasing figures and it's chasing a result.

SW: And do you look at the large enterprises or SMEs as well?

SR: Yeah a lot of the clients I work for tend to be, yeah do work I do, I head up in London for UK defence as a sector. So have a lot of clients who are large multinationals in that respect. We have colleagues who work in all of the major sectors. That includes telecoms, um, retail, B2B, and....

SW: Do you find they are, um, are they spooked by the current market and therefore looking for guidance or it's just, do you think they have a proper strategy for cyber security or news stories are scaring them a bit into the arms of consultancies?

SR: It very much depends on the client. You get the whole spectrum, um, we tend to deal with the more mature, um, the larger organisations which is not necessarily very different. In that they tend to have that many hurdles to overcome before getting, um, there may be issues but they have to weather it and understand where they are going forwards. Where they are more concerned by things like acquisitions and mergers, where they have rapid changes in their infrastructure and…

SW: Exposure?

SR: Yeah. We deal with one or two smaller organisations, but as they are smaller organisations, we are probably pricing ourselves outside of these companies.

SW: So more the medium and larger ones?

SR: Yes. Because it's more strategy and oversight and that's where we're positioned in the market. People who are looking for the smaller organisations, there are a lot of firms out there looking for that and it's a very competitive space. And getting a big company involved in that would probably be negative for the industry as a whole. I suspect.

SW: And you see the market growing? For <COMPANY X>?

SR: That's definitely a lot more board awareness of the issues and risks. There's a definite steady and increasing amount of work but that doesn't mean people are getting more mature or switched on to it. It just means that they've been spooked by, er , or that they had problems and they're trying to do something. What you tend to find is when It gets to board level it's very much a question of they want an answer now. They want a very quick, easy fix to turn around and it's actually more the strategy and the development where the space is.

SW: Yes. Do you see companies being reactive to threats rather than having a long-term strategy?

SR: More often than not. There are companies that have strategies and they're looking at it, especially when they have a new CISO, taking on that role. Very often when they are new to the role and they've had experience before and they tend to get a benchmark and they want to look where they're at, um, strategy. That's more where the strategy comes in, when you can have a conversation, where our work tends to be, with looking at the benchmark, more than reactionary and ties in with the forensic response that we have. There is a lot of, there's been a problem and they want to understand it and try and improve going forwards.

SW: And do you see the position CISO, the chief information security officer, being more in demand now, or is it improving from a very low base?

SR: To be honest, there's a lot of very large organisations that you'd expect to have them and don't. But equally there is a lot of organisations that have them but they don't have board buy in to the roles and responsibilities. They don't necessarily report to the right people, so that's a structure issue and it takes time to get that to work.

SW: Yep.

SR: Whether that's, whether they're at the right level, and that's going to take a while and I think we are quite behind some nations with that kind of options.

SW: What kind of nations?

SR: It is, it is a difficult one but Germany is pretty hot, hot on corporate governance, but it doesn't mean they are any stronger but they have it at a, have much more legislation in place to take that on. And the United States of America is ahead in some ways, and in some ways it's a long way behind because it's very strict in the way it's enforced, there are very different rules in place. I think the prevalence of CREST, in the nations where it's heavily embedded, then it tends to be stronger because you have a certified level which is standard across nations. So places like the, er, Dutch are pretty good and they have very good specialist skills. We have a lot of multinational companies that are over many nations, and you find they're very strong but that they have a satellite office in Chile which has links to the rest of the organisation, so it's much.....

SW: So no country is perfect…obviously.

SR: No, no.

SW: Which is good news for consultancies I guess.

SR: Yes, anything that's got humans in the process is never going to be perfect. There's always going to be space for humans in the role, for that role may be different because there is a lot of automation software. Whilst there is a lot of firms which just use automation software there is an argument that the human effect will always best be analysed by a human than by a computer, always be areas that won't have it.

SW: Okay. I've just remembered something that I meant to ask you at the beginning about your educational background, do you have any post-university qualifications, such as CISSP…

SR: I've got, um, I've got two, and both are with (unintelligible) which is a governing authority which gives, which are ratified by CSG. I'm a checked in leader, leader of the group, qualifications which means I can work on government systems up to reasonable level.

SW: So, it's like a security clearance?

SR: No, that's security clearance, that's a separate area.

SW: Beyond your scope…

SR: I don't think it's where your research is…

SW: Okay. Thank you, I just remembered that. If I can move on through the questions, so we can get through them, so talking about hackers in general.

SR: Yeah.

SW: Do you have an understanding of what toolkits hackers use?

SR: They'll use whatever they can get their hands on, a lot of, you put through some of the toolkits on your questions, and they kind of just get split up, you get the, in reality you get the script kiddies, if you like, who are essentially going to run whatever they can find on the Internet which could be something simple. You got those that want to disrupt, using something such as DDOS, denial of service type tools which if you have more funding they're likely to include hiring botnets and level seven. You then got the knowledgeable individual, they've got a bit of understanding, probably doing it deliberately or accidentally, which will tend to be, if you're talking Internet then it tends to be intercept tools.

SW: Sorry, what tools?

SR: Interception tools.

SW: Oh sorry, interception tools.

SR: So basically proxy, running through proxy. And then you get the higher level, more organised criminal gangs which then use distributed botnets and they'd be paying a fair bit for those. Above that you've kind of got, kind of hacktivists, where you wanna change a website somewhere....

SW: Web face defacement?

SR: Yeah, they're high impact but not necessarily that skilled, though they have a similar purpose and depending on what their motivations are, will determine how we are going to do that. And then you've got criminal agencies who want to get a handle into the system, they want to get funding out of people and systems. Then you've got state-level....

SW: And I guess they've got the most comprehensive tools available?

SR: I'd assume so. If you're in the attack category for those then you going to get got no matter what. These instances are the ones that cause most concern in companies, and it's where the media hits, for example yesterday with the CIA toolkit leaks. The reality is if you going to be got by them you're going to be got by them, by the Russians et cetera.

SW: Is it a case of there is no defence against them.

SR: If you're law-abiding citizens then whilst you've got no defence against them equally you're not going to be targeted. Their skilled teams that go in for specific purposes, if you're concerned by them then you've got bigger problems....

SW: What about companies, for example in the West, who have IP that is at risk of being espionaged?

SR: In that case it's not likely to be across the Internet, there's a lot of bad sites but there's a lot of regulation with regard to front end websites. There is a lot more soft underbelly elsewhere which is not regulated and isn't maintained. A lot of companies we find have a great solution for their web front-end, hosted in a nice managed space, completely disjointed from their internal infrastructure, but you can just walk in and plug-in and get.....

SW: You mean they've got vulnerabilities on site, for example, there physically.....

SR: Yeah

SW: Plug into a UTP port and away you go.....

SR: Yeah, or by just paying a cleaner a fiver. Probably a fiver for a cleaner is enough, and they'll go and do something for you.

SW: Plug a USB?

SR: Yeah, and by that stage you got far bigger problems. And that's not a regulated industry, that's not a mature industry. And it's where a lot of nation states would be more inclined to pay a fiver, or pose and go and get a job for a week as a temp and get in that way rather than focusing on, on the hard target. And with that it's always the case you go for the easiest target.

SW: I'm interested that you're seeing that as the soft underbelly of companies as they will lock down their UTP ports for examples and.....

SR: There are all sorts of examples but, if they're lockdown, there are a million and one other systems. For a system to be completely secure, everything needs to be patched, everything needs to be brand-new well everything needs to be a generation before brand-new because brand-new have a problems. They need to be patched and maintained and companies don't have the budget to maintain that and they've got too high availability requirements. So you always have legacy equipment around, you always have a Windows NT 4 box in the corner that everyone's forgotten about. You always have a security guard that goes for a cuppa tea at 3:57 on a Friday afternoon. You will always have a gap there, now if that's where it is, you always have a third-party delivery and you can intercept that; if you're intercepting on delivery that tends to be state-sponsored, because the chances of individuals picking the right equipment are quite slim.

SW: So I understand state-level, they've got the time and resources, to pull someone in on the ground. It's expensive to do that rather than try and come in over the Internet. What about criminal gangs? Could they use the physical option or do they always come over the Internet?

SR: I don't know to be honest. I imagine gangs will be more likely to use ransom-ware from the Internet just because it's easier but I've got no evidence to support that. I've not been confronted with criminal gangs.

SW: Ok. Well you've already answered my second question about the different kinds of hackers and the different toolkits. So do you have a view on what the differences between hackers, hacktivists and patriotic hackers? Almost like a definition if you like...

SR: I'd say hackers is a generic term, which everything umbrellas underneath that. Yeah, it depends on what your dictionary is as to where and what comes under that because what the media portrays it as it is very different to what I imagine it is and what you imagine it is.

SW: Yeah. So if you had a definition of a hacker what would it be?

SR: I guess, an individual attempting to influence through unconventional means the operation of the system.

SW: Good, perfect.

SR: That obviously covers a lot of stuff which is non-Internet specific and there is the kind where are you add a button to a system to make it do what you want it to do....

SW: The legitimate side of hacking.

SR: Absolutely. I'd say hacktivists are those that use malicious means to then make a, generally political but not necessarily, statement.

SW: Pursuing a cause, would you say that?

SR: Maybe. They've got a specific goal in mind to deface or make a change to something. And then…

SW: Patriotic hackers?

SR: It's not really a term I've come across previously before I've seen the paperwork that you've got there. The way I've read it is that because it's patriotic they want to do something for their country which is unusual. It kind of conflicts with being a hacker because you're trying to do something for a cause. So it's kinda conflicting and because cyberspace is non-geographic in then becomes very much a grey area. It's a bit of an oxymoron.

SW: I think it's a fairly, relatively new term. It's something I'm interested in, and example would be the time of the last intifada between Israel and Hamas and the Palestine territories. Israel invaded Palestine in response to some terrorist attacks, and in response to that various hackers attacked Israeli websites. In response to this, and allegedly not at the behest of the Israeli government, Patriots rose up in cyberspace and attacked back, on behalf of their country.

SR: Yeah, I suspect that because it's Israel and Palestine means it's a kind of side-effect. I think it's effectively gang warfare or individuals who have a cause, example those that want to take out a particular server or those that want to take down EWS. It's going to be the same individuals and structures to do that. There is the state-sponsored side, which is the whole cyber warfare within the national interest, attack and defence kind of things. I would almost certainly say, given what you said there, that it would be led by Mossad on one side and Palestine on the other. Instilling the initial idea in there, I think very much it's a mercenary kind of behaviour.....

SW: You think they're for hire rather than acting patriotically?

SR: Yeah, almost certainly. Almost invariably, if you're attacking bits of Israel or bits of Palestine, they will end up attacking service in the US, bits of infrastructure that's halfway around the world and the consequences would be that be in a hell of a mess and not doing what they set out to do.

SW: Ok. Good. The next bunch of questions are about patriotic hackers, you may find them tricky and you may want to generalise. Do you have a view on the age, gender, type of person that would be a patriotic hacker or, a hacker in general?

SR: There are lots of stereotypes, it's probably an individual looking for extra money who has a particular skill or has some sort of disillusionment. And wants to be heard, either directly or indirectly and they want to get some kind of recognition for what they are doing despite the fact they are probably average Joe on the street. Very much the case. There's a kind of market in areas such as Eastern Europe, not Russia, such as Ukraine and Poland, which have very lax security laws

which means that a lot of individuals, who have a bit of skill, will play around. You find that a lot of this takes place in this informal space, they have a lack of national regulation, maturity, but have a lot of expertise in these skill sets. They're being used for programming, legitimately, and a lot of companies will push their data centres out to places like Bulgaria and they're probably doing a bit on the side.

SW: Could also be said, that given a good education and things such as computer studies that the jobs just aren't there for them?

SR: Yeah. Potential. Yeah it's a potential that one day they got bored, and they've got no formal qualifications but they managed to get on a PC, and are looking for money or looking for whatever they're after. There is a great site, which a colleague of mine, former colleague of mine, had which has a picture of mounds and mounds of cash that they got for hacking and for taking that kind of role. It's clearly a faked picture, but the motives behind it are very clear and it is clearly not restricted to a geographical area. It's stereotypical to say it was in the east, it's typically someone in their early 20s, quite affluent, in a rich part of the UK. It's quite often the case, and with the quite sophisticated ones too, that the parents are not giving the attention; they've got the skills but they've not got recognition for what they are doing so they don't understand where the law line lies.

SW: Would you say they are mostly male or female?

SR: The good ones don't get caught, so there isn't really a statistic; in my personal, stereotypical view they're probably early 20s male but there's no reason to assume that. That's for those who get caught and who historically have been identified.

SW: Okay good. The question I had, is do you know which countries actively use patriotic hackers? That is, use them as a proxy because they can then have deniable responsibility for the actions?

SR: The kind of wider question is, patriotic hackers is kind of the weird anomaly, those nation-states that have attacking militia forces which are not necessarily geographically located in their country with plausible deniability. From certainly all the major states ,major forces certainly have them and obviously the leaks yesterday, from the CIA documents, verify that, If it can be believed, that there are two offices within Europe, which were plausibly deniable, which they no longer are. And the Chinese, the great Chinese firewall, and Russia, certainly these are the big three. And I would not be surprised if there were another 30 or 40 countries on that list that are included. But have I got proof of that? And would I want proof of that?

SW: No. You've actually touched on the motivation of hackers already, do you want to expand on that?

SR: There are certainly large financial rewards for it, er, and every individual will have different motivations for it. A lot of them have a kind of reward from being recognised, for good or bad…

SW: A level of achievement, proving…

SR: Yeah, they see it as a computer game, they're after recognition of the skills that they use.

SW: And when you say recognition, do you mean from their fellow hackers?

SR: From the hackers, from the fact that you hit the news, it is a recognition that you are big enough to make it on the world stage. Or the fact that you can get into organisation X or the fact that you can stay in there for more than a week or every individual has a reason for doing it. Whether they can then say they have root at the box or that they have a zero day and they can then go and sell it

on the black market for that they have taken a server off-line and a competitor then has an advantage. A kind of one upmanship at a basic level.

SW: Do you think there's any revenge motive online?

SR: Very much, it's definitely a case of revenge, I took you off yesterday and then you hit me back and it builds and builds and builds. And whether that is petty revenge or more structured because there is a gang side and this has spread online. There will be echoes and reverberations around that which encourages online action, it will encourage revenge action. And there are outbursts such as, attacks, terrorist attacks, with individuals letting you know that they are not happy with something and you can write to local newspaper or you can hire a botnet, and attack Russia Today.

SW: Almost acting patriotically?

SR: Not necessarily, for example when Lee Rigby was killed then the responses were not patriotic necessarily in that that would be retaliated against. It is, how could that happen on my turf? It's kind of…

SW: Gang?

SR: Yeah, turf related. It's very much more gang warfare, the Internet is very disorganised. You go and see, you don't see the estate in particular, a gang or corporation or capitalism, which is one that a lot of people will fight against.

SW: Okay good, um, the next one is moving on a bit to cyber warfare and the future of cyber warfare. Do you think that proxy forces, that is nonofficial cyber forces, have a role in cyber warfare?

SR: If I knew the answer to that I would be a general or a strategic planner. Almost certainly they will do, as in general warfare, there will always be frontal assaults. You've got country A against country B, you've also got guerrilla warfare where it is all tucked in with everything else. And as we have seen in recent years, guerrilla warfare tends to last a lot longer and tends to be a lot harder to extinguish. So I would say that would be a role for proxy forces, whether they are aware about plausible deniability and command and control, and about using the Internet leaving themselves exposed is a different question. There will be logs and links that will show who they are eventually.

SW: Is that the case Sam, as the nation-state can you always find the route back? Or can a clever nation-state always hide themselves using proxy forces?

SR: I'm not a nation-state so I can't give you an honest answer to that. What I would say as a standard user there are invariably ways in which you can be traced. Whether that is directly or by a lack of anything being direct; logs that are being amended to hide something will be just as telling as logs that show you where they are. But equally there are tools that can be used to amend those logs and it will be hard to trace back, and with that kind of attack you are looking at the element of time. It will often be days, weeks, months, years later that things are finally resolved back. The Sony hacks took a long while to even vaguely work out what was going on. And that was with tools that can log reasonably well. A lot of businesses, the logging isn't up to standard or isn't looked at, there is a whole separate piece there.

SW: With the Sony hack, do you think the attribution to North Korea was proven?

SR: I don't really know what the honest answer is, I think there were several Sony hacks and I think that in reality a lot of them were very simple and straightforward and were probably an individual that was downloading the data and exfiltrating it. I think that the inclusion of nation-states in that

was more down to the media or was propaganda, whether that was states or individuals. Sony were trying to allude that it was something serious when in fact it was something much more straightforward. But it always takes time to digest what exactly is going on. I suspect that there are people who know the truth, but most people don't know what was going on.

SW: Would a nation-state, for example Britain, always be able to get the attribution of another nation-state if it was involved?

SR: Pass. I suspect that they might be able to, but whether they choose to announce or publicise the fact that they have is another question but, I know what I know but…

SW: On another level then, if a company has sufficient resources and the willpower to trace a hack, could they always go through the data and be able to attribute the attack?

SR: Almost certainly the systems and the logging that they have in place would not be enough but that's more because as a business you don't log everything because you don't have an infinite amount of space. And you are also only looking at certain points in that journey. The difference between the previous question is that as a company you only have certain points; if you had the resources of a state, then you could potentially look at the connections between infrastructure and that would be a lot more powerful. For a business, there are ways and there are forensics, and there are forensics groups out there. But you can't guarantee every time that you will get your man, there will always be an element of…

SW: Yeah and the question is, if you do get your man, what can you do about it as a company? If example, they are in a state that doesn't have an extradition treaty...,

SR: If you are a company then you wouldn't necessarily want an extradition. There are obviously a lot of grey areas in the Internet as a whole, and in cyber security, because it is non-geographic. There are areas that fall within, that can be challenged under that nations law but there is a determination at which point, because you have things like VPNs, which are allowed but other nations do not have that so is it the endpoint, is it the origination point or is it the target? And which point comes under, there isn't really an answer to that.

SW: Is it fair to say that, at a company level, they don't really care where the attack comes from, they just care how to stop the next one?

SR: That sounds fair, but to be honest they're not really caring about how to stop the next one because they will assess the risk, is it under X percent of our company turnover, if it is so what I don't care. Is there a fine if I don't do it, which is still less than X percent of the company turnover, then I still don't mind, is it going to rob me blind and put me into administration, yeah then I'll definitely fix it.

SW: Risk against cost.

SR: Yeah it's always about the financials.

SW: Okay, do you have a view on how hacking is going to develop, it’s a big wide question but have a go.

SR: There are so many areas, I think a lot of low-level, is going to become more commoditised as it matures. Which is not a good thing, there will be a lot of fore-runners who are able to make the most of that. Most of them are likely to be automation companies that provide a box or a solution that you can just plug-in and it's going to give you 70% of the findings that everyone else is going to

give you. But there is a need for an increase in the maturity level, so that people can actually understand where it is and where the risk really lies. I suspect that, I'm looking at more of the defensive side rather than the attacking side, just because of where I am, I suspect that companies will move towards that understanding of where the risk is and being able to change low risk findings. And they will be able to pull out what is rubbish and what is genuine risk. But I think that a lot of the small companies will fall out of the market, you can see a lot of the large companies squabbling and trying to fill up that space, they're buying out a lot of small companies to get that market presence. I suspect that is going to happen for a while, and then you are going to get more fallout and there's going to be a lot of uncertainty and I expected to get very expensive. Then the prices will drop, I think that's on the attacking side, it will continue at the low-level. I think there will be a few big things that appear, especially in the wake of the wiki leak scandals, it means that after 6 o'clock on the day of any release there will be a huge spike in activity. There will be a vulnerability in a release or a piece of software, and there will be a squabble to find a way to be able to use that. There will be big peaks and troughs, massive peaks with a lot of security releases, I imagine a lot of software coming off the back of the things in the last few days. Which means it's all got to be done quickly, so the code has to be rushed through, which means that there will be vulnerabilities in it. Whenever you have humans involved in that process, you always have to pick up the pieces. As long as there are issues, you always have individuals who want to exploit them. And there will always be the thrill of the chase to get that concept. And once you have a proof of concept you have to get it into a commercial way so that you can sell it to whoever - whether that's a gang or a state.

SW: Do you see the Internet of things creating an area for an attack?

SR: That's a very different question, I think in general it's taking us back to 1991 in that there is sadly a spike of devices that are cost produced with very little thought about the underlying security model. There are a lot of organisations out there that are trying to produce viable IOT devices, so it is a very sweeping statement to say that they are all bad. But generally because of how the market is, it is purely cost driven and people do not think there is a problem in trying to connect to the Internet. They all want to do the shopping on there, there's a big gap that people have overlooked and it's been overlooked for long enough for these devices to get onto the market. And they've exploded, and this means that there is this massive wealth of very dumb devices out there. As the IOT model develops, it's got to go through the whole process again. So they are going to be like this for a number of years.

SW: Do you see it as a problem of people's privacy and malicious attacks in the home, or do you see it is creating a zombie botnet for people to exploit and attack with?

SR: For the time being the maturity of the devices that are being compromised, then it's just the volume of them that is the problem. However as they mature I see that risk changing, the more intelligence that they have then the more that the risk becomes personal. And there's going to come a point when they have enough information stored on them for them to be order your milk for you, so you don't have to pay for it however by that point they'll have your android credit card or whatever, and at that point they've suddenly got personal information. This makes for a very different target.

SW: So you'd say at the moment they are more vulnerable to becoming a massive botnet than being used for personal attack?

SR: At the moment because they are essentially dumb devices with an IP address then the biggest threat is that all these devices suddenly point themselves at the same address at the same time and just brute force; whether that is proof forcing passwords or low-level attrition.....

SW: DDOS?

SR: Well there is that but more like neural networks working out how to brute force passwords, doing very low level, cheap work. Individually they don't have to do too much but pulled together they have this power. That kind of distributed neural network or distributed denial of service is the greater risk. But as that they become more powerful, and they go through their journey and life cycle, then that risk evolves. I see it as we are in 1991, turn the fridge on, turn the heating to hot, as they have more functionality, as developers get more freedom and realise what functionality they can deliver from it then the surface area will increase exponentially. There is a whole mountain there that could be an issue. Equally, if people take into account what they've learnt over the last 20 years on other platforms and put the time and the cost in to fix it before it runs away too far then it may be controllable. So I think it's with the venders to direct it.

SW: So a complete change of tack now, I've just remembered something that I wanted to ask. Do you think there is, currently the law in western countries does not allow a company to go on the offensive in cyberspace if they are being attacked from a particular source because there are lots of reasons. Do you think there is any justification for a change in the law to allow companies to go on the offensive against an attacker?

SR: I wouldn't have thought there was any desire, I wouldn't have thought there was any drive or directive to do that. The last thing you want to do is encourage fights effectively because it then becomes a competition of who will win. You also often find that IP addresses are shared, so you think you're attacking one of the hosting providers but you're actually attacking something completely different.

SW: So the collateral damage would be high?

SR: Yeah it would not be something that looked positive on them, If it started to happen I'd want to run away and find somewhere…

SW: Yeah. I don't see any companies agitating for that at the moment but it has been discussed in some circles.

SR: I don't think most companies would have the funding or the desire to do it and I think the only ones who might contemplate it would be the anti-DDOS providers. What would their role be? If you're attacked then I'll go and attack for you, we're your private army? Where you'd actually end up would be DDOS provider 1 would attack DDOS provider 2 and you'd end up with a war between them and because everyone is under one of these two providers then the whole world would go off-line. Yeah, realistically I don't think any company would be aiming for that, it's certainly not something as a consultant I would be suggesting.

SW: Well the law is against it at the moment, but laws do change over time. So that's all be questions covered off, is there anything else you'd like to raise that might be appropriate? That we may have missed or need to discuss?

SR: I don't know.

SW: That's fine it was just in case I've missed something obvious.

SR: I guess, the hackers' statement, is very general and people can be doing it for negative or for positive reasons. Whether that's online in that bedroom, they could be positive or negative. On the other side of the coin is the people who did bad things and got a lot of money for it and then went to the banks and sold their ideas which kind of goes in with what you were talking about earlier and their motivations. Similarly, bug bounties, is it a good thing or a bad thing? Because this is effectively subsidising people to become small time hackers, in effect. So is that a good thing or, effectively you've got to be aware of the problems. And you've got to get them out in the open and fixed and resolved. But does that mean you're creating a problem further maybe 10 years down the line? I guess there is also a question of how as a nation we develop things. For 5 to 10-year-olds, the cyber security challenge. For education, for getting people on the right track, which is obviously great for the UK but is something that should be done globally. The motivation for this is to ensure that the UK doesn't fall too far behind.

SW: Are you hinting that, by raising this awareness and education we might actually produce more hackers?

SR: We will produce those that are more aware of the situation; it means that industry and companies need to have the roles available for these people to go into. If you don't have support further up the chain then potentially this could happen but that is not what I was meaning. If you train people for 5 to 10 years and then when you get them to their early 20s you don't have any jobs for them and potentially you could have a situation where you have half a nation of hackers.

SW: I alluded to this earlier where some industry experts say that that's what's happened in Eastern Europe. When they have very good education for people in coding et cetera but they don't have the jobs for them to go into.

SR: In the UK, we have a strategy for this, with industry and the UK government working to drive things forward. Whether this helps us or not, with a lot of computers becoming automated then this potentially causes problems. But equally you need these individuals to help write these programs.

SW: Catch 22, eh?

SR: Yeah.

SW: Well thanks very much, was there anything else?

SR: No.

SW: Again thanks very much for all your help.

11.2. Appendix II Interview Two

SW: OK Sean, if we can start. Did you have a chance to look at the questions at all?

SLJ: Yeah, I saw them about a week ago, I'm happy to go with them.

SW: So, there is no right or wrong answer Sean, and it's perfectly okay for you to say I don't know. So, can you tell me a bit about what your history in cyber security is?

SLJ: Okay, so the long and the short of it is that I spent 20 years in the military, most of that was around operational risk. I was an intelligence officer, a planning officer and an Ops officer. Both in frontline roles and in headquarters roles. Also the air force and in national agency roles. I was also in Whitehall, with the national government both in military and in intelligence policy as well. I saw all parts of arms and risks, and I was also part of the countermeasure and solution planning. Towards the end of my career I saw the transition from electromagnetic warfare, and information operations becoming more grouped together, with the growth in the Internet, around the word cyber. Towards the end of my career, how can I say it, it was about fusing the effects of cyber with all the physical weaponry and the effects that they can bring to bear.

SW: Fair enough.

SLJ: It was an integration role really. We saw lots of new strategies coming out around cyber, one thing that you may want to get hold of, and it's available in the open domain, is the MOD cyber primer, a good little background read.

SW: Okay, yeah, yeah.

SLJ: It's a little document telling people what they need to do around cyber; it's about getting people who are non-security related to understand the wider angles of cyber. I.e. the non-technical bits. And the MOD, it's quite ground-breaking but very simple, the best ones usually are. There was air, land and sea and then there was cyber, and these were all the domains where warfare could happen.

SW: Yeah, I've read a bit about the US military, and it took quite a while for cyber to be accepted as a separate domain.

SLJ: Yeah, that's what we call in the commercial world the digital space.

SW: Yeah, and did you actively going to cyber, or did you fall into it?

SLJ: I was in joint effects, which is all about pulling together the different arms and making them work in unison, so cyber turned towards me rather than me choosing it. But I remember being given options about career moves, and cyber was definitely one of the better ones to be in. Because they knew I was either going to go stellar in the air force, or I was going to leave and this was a skill set that I knew was going to be key in a growing industry.

SW: Okay, thanks very much for that Sean, the next question is on hackers in general. Do you have a view on what tool kits hackers typically use?

SLJ: I don't have any detailed knowledge on that, I know that Sam and his team are all over that space. What I do know though is that they are becoming increasingly easy to get your hands on. Easy to use and therefore less training burden. More people are able to get hold of advanced tools and software, or rent them, rent the service as it were and let somebody else do it for you. So we're seeing a commoditisation of this.

SW: Yeah.

SLJ: There are favourites, but I think the guys that are doing the most damaging and having the most fun, it's often all about the challenge, are the ones developing their own or making a hybrid version of it.

SW: Okay, and do you see these tools widely available on the dark web?

SLJ: Yes, but they are also available on the open Web <laughs>. The better hackers are the ones using hybrid tools, a combination approach, and techniques and procedures as well.

SW: Do you see a difference between different kinds of hackers, for example hacktivists and coders, and the different tool kits that they might use?

SLJ: Umm, I don't know to be honest. I guess it depends on the target. You can reverse engineer the motivations of the hackers from the choice of target. I presume if you're going to attack a building control system or an industrial control system there will be a piece of kit that knows the vulnerability in the software, and the types of software that they can attack. If you're going to attack a bank, you need a different kind of tool, you know, different techniques in combination.

SW: Yeah. And on hackers in general, do you see a difference between hackers, hacktivists and patriotic hackers?

SLJ: Yes I suppose there are, there are a number of motivations for hackers. Whether it will be ideology, finance or illness. In some respects, a desire to be wanted. But with patriotic hackers there will be an ideological, national and political motivation. They may be proxies for a government or an agency; they may be doing it not because they are patriotic about a nation but because they don't like the other nation more. So they can use it as an excuse.

SW: Just going back a bit, just something you mentioned before, when you said illness do you mean like a mental illness?

SLJ: Yep, some of them are on the autism spectrum, and this is what they enjoy. They are obviously gifted at it, and they can be exploited, and sometimes there is a need to be loved about it. It's not all about autism, but there is an expressive need to belong or to show off or just to prove that they have particular skills. So this is then exploited, in particular by, Russian gangs.

SW: Ok. Would you also say Asperger syndrome, something like that?

SLJ: Maybe, yes. Maybe. And it's not just me, my thoughts on this, I've heard it mentioned officially with the discussions with NCA, and what they're learning around the prevent agenda.

SW: I've seen a paper on the correlation with Asperger syndrome, so there is definitely something there. With regard to patriotic hackers, do you have a view on their stereotypical look, in terms of age, gender, social status, job role?

SLJ: I don't, it's very easy to stereotype, with the disenchanted youth in the bedroom, with gadgets, a teenager. It's been going on a while, people are growing up, but I wouldn't be surprised if there is a big cluster in the middle that is teens moving up to middle to late 20s. They are disenchanted, disenchanted with society in general. They are playing around, playing around with things in their own space....

SW: Yeah, and would you say they are more male or more female?

SLJ: Definitely more male.

SW: Yeah, okay. Do you think they have a particular political leaning, in general?

SLJ: I think they may be apolitical, is what jumps into my head, they may have strong beliefs and strong opinions and strong motivations. Do they belong to a particular party? No I don't think so, they are more on the anarchist side. So they may be thought of as a movement like Anonymous, they won't be part of a political group.

SW: So, moving on Sean, that's a good answer. Do you have a view on what countries are using proxy forces in cyber warfare?

SLJ: Proxy forces I would definitely say Russia, Russian Bear is et cetera. I would definitely say Iran, various groups such as Hezbollah, or Syrian groups such as the free Syrian electronic army. Definitely North Korea, although a thin line between proxy and actual, I would suspect China to some extent, though this would be high risk for them.

SW: There are lots of the usual suspects on that list, would any of the less usual suspects' e.g. western countries use proxy forces?

SLJ: I don't think so, no. There are too many restrictions in place. They could use other countries, like they did with rendition, where US/UK can't torture them but a close ally such as Jordan can. So I wouldn't be surprised if, even though we can't do it, we can't see the output of someone else doing it. I'm not sure on the law on that one, I'm not sure if there's a law against it.

SW: Yeah, yeah.

SLJ: You've got countries like Estonia that might be able to do that for us. No evidence of course.

SW: Estonia is mentioned a lot, it's obviously at the front of cyber warfare.

SLJ: I think they've developed their own capabilities from experience with cyber attacks from Russia et cetera. It was about NATO expansion, so they managed to develop their own capabilities fairly quickly.

SW: Okay. With these proxy forces do you have a view on what their motivations are? These proxy forces.....

SLJ: It's partly political, so they can leverage political influence or financial gain, for instance political or economic contracts. I don't know, it might be a small piece in a large jigsaw. But sometime it's going to be about economic gain.

SW: So in the future Sean, if you could look into your crystal ball, what role will proxy forces have inside cyber warfare? Do you think they are going to have an increased or decreased role?

SLJ: I think we are going to see an increase, when I look at what is allegedly happening around the US election and Russia trying to block NATO expansion and trying to meddle where they can, getting quite boisterous. Yeah, trying to keep the Cold War lid on, the cyber Cold War. Yeah, proxy forces in cyber warfare could be a pressure valve, but without ramping it up too much into a physical hot war. So, allegedly, some of our NHS breaches recently have been delivered through Russian cyber proxies. This is to prove to the UK and influence other foreign policies. NATO expansion for instance.

SW: Do you see this as a classic extension of the Cold War in cyberspace?

SLJ: Yes, I think it is and it is a much better safety valve than going off and fighting Vietnam or whatever. Because they are not able to strike deniably but without crossing the red line of physical damage. But I worry that they don't know where the red line is for physical and economic damage, under Obama and especially now under Trumps rule, we may find a counterstrike which is less proxy and more actual.

SW: To be fair to hackers, even international law, I've read, doesn't know exactly where the line is where the use of force has been made in cyberspace. It's a very grey area.

SLJ: Yeah, yeah, it's a good point and I know the Americans have been thinking a lot about that and I guess it will depend on every political relationship they've got on where the line of aggression is. Or where they want to push, they can do lots but in North Korea where they have legacy equipment and lack of controls, they could do severe damage including physical damage if they wanted to.

SW: Okay, moving on. But still within cyber warfare, what do you think the pros and cons of using proxy forces are?

SLJ: Okay, thinking of Iran and Hezbollah, thinking of the free Syrian electronic army, they can ensure that Iran is kept out of things until they step over that line. They're still able to claim the credit even though it's deniable. So it's almost common knowledge that Iran is able to strike in Bahrain, in Saudi Arabia and Qatar and places like that if they want to using cyber and get away with it because of the Mickey Mouse organisation that is the proxy. There are a lot of advantages I suppose, there's the getting away with it, being able to do something where otherwise your hands would be tied, it's fairly cost-effective, fairly quick and fairly accurate, It's global reach.

SW: Are there any cons?

SLJ: Yeah, one of the cons would be you don't know where the line is, you're probably opening yourself up to something you might not be prepared for I.e. a counterstrike. You don't have scale for some of the targets that you are aggravating. You will probably lose control at some point, I mean who are these proxies and how well do you know them?

SW: Yep, yep, with a counterstrike is it a viable tool to use for the West, you may be targeting the wrong servers if they've hidden them, the path through the Internet and you will be striking at innocents by accident.

SLJ: Yeah, collateral damage. Yeah there's a risk of that all the time. It depends on what kind of effect you're trying to achieve, if you're trying to make some noise and be punitive then collateral damage is good. But what happens if it's one of your allies.

SW: Yes, yes.

SLJ: With Israel and Stuxnet, the initial target was hit but Stuxnet carried on and evolved, spread and eventually made its way back to the west.

SW: So this is the Stuxnet attack on the Iranian reactors we're talking about?

SLJ: Yeah.

SW: Okay, and how is the development of the Internet of things going to affect cyber warfare in the future?

SLJ: Well technically it should make it very easy because of instead of using steppingstones you now have a concrete runway to be able to go to where you're going. You're now able to attack through a

much greater threat landscape, threat exposure, you could say though that it also makes it more complicated and you can't see the wood for the trees.

SW: So are you saying that they can use of the Internet of things as a platform to launch off or as a target in themselves?

SLJ: So some attacks are direct and go through the supplier partnership chain and they may be three steps away from the main target. One of the greatest attacks in the US was finding a weakness in the air-conditioning supplier and working their way through the network that way. The more extended your environment, the more complicated, your threats are inside when you think everything is secure. Too many doors and windows.

SW: The development of IOT is going to create a lot of risk for people who use it?

SLJ: Absolutely, absolutely. You're broadcasting, you're sending out more beacons. You are leaving more windows and doors open. You're having a much bigger signature as well as footprint. If you're going to be socially engineered then you're going to be leaving a much bigger (inaudible).

SW: So generally in respect to cyber warfare is the west doing enough to defend itself?

SLJ: Definitely not, constantly surprised by the neglectful and wasteful approach to the challenge of cyber security by major organisations. In the commercial world they're not seeing any profit generated, investment, almost a deniability that it's even a problem.

SW: So do you think that is at a commercial level or at a governmental level as well?

SLJ: No it's at a commercial level. The government has finally woken up to this but has realise it doesn't have the capacity or resources to do anything about it. So they're trying to accelerate the catch up, which is why you're seeing expansion in the NCSC and an expansion in GCHQ and the NCO.

SW: Sorry Sean what was the first one?

SLJ: The NCSC, the National Cyber Security Centre. The website to look at is the CNI website. It's a national infrastructure, it's where the government has put all the crown jewels in.

SW: If you were dictator Sean, how would you better direct our efforts?

SLJ: If I were a dictator, I would instil a baseline in law about a minimum security standard. I would also instil an approach, in law, where organisations and companies have to have cyber within risk management. I would impose cyber security regulations to complement data protection regulations. There is quite a lot of overlap between the two, especially around technology, the operational security and the IT security overlap. Firewall, DLP, all that good stuff. So there is plenty of efficiency there you could already leverage on. And I would help propagate a reward for that, by getting the message to customers that they should expect security in their products and that they should be made aware of things like cyber essentials so that they ask for it. And in response, companies could charge an extra levy for that. So that helps repay their investment.

SW: So do you think the public needs to have much more awareness?

SLJ: Absolutely. I think the public is aware of cybercrime and what it means for them with regard to threats. But what they also need to understand is, are the big brands looking after them? I think they are getting there but the customer should help drive this. But I think this should be hammer and anvil, the big organisation should be hammered to do this, so that they meet in the middle.

SW: So do you see the market for cyber growing rapidly, I know there's a bit of a stall couple of years ago, and it's now picked up again?

SLJ: Yes, I can only talk locally, but what I've seen is the market picking up. We see a lot more interest from boardrooms, partly because of privacy, but also because of liability. Also there are more and more companies suffering from ransomware and DDOS attacks. Particularly last year.

SW: So we rattled through all the questions there Sean, is anything you'd like to add, something that I may not of asked?

SLJ: For me, companies need to make more use of ethical hacking. War gaming, diligence, so that they know what an attack might look like. And almost go through it themselves, on their own terms. I think the challenge for me, is how do we build an ethical hacking force, and get them to work for the blues rather than the reds. So we can train them up and skill them up in school, if we have a national training plan, how do we keep them on the right side of the law. Ultimately, the only thing that stops them going off to earn vast amounts of money with Russian and Chinese hackers, is their ethical code. Now that is okay in a way, I can see how western culture can act as a bit of a buffer to stop them moving over the line to a certain extent. Law-enforcement, and maybe a religious element. But what do you do for the Nigerian family, who have four boys who are technically gifted, and they are being exploited. They are being paid £10 a day, let's say, by a call center, and are sub-contracting to a multibillion-dollar criminal gang. What is to stop that family from doing this, when they see no real damage, they just see zeros and ones and think it's a bit of a game? But, the kids, are managing to keep the wider family in food. This is the big challenge, as law progresses it just displaces the work out to where the labour market is and where regulation is less so. It just displaces the criminal work out to where the labour is cheap, in south Asia and Africa and parts of China. I don't know how we are going to do this.

SW: I don't know, I think the only way to do this is to lift everyone out of poverty which is a massive task.

SLJ: Yeah, here we are focused on the technical aspects, pen testing, the tools, but maybe there needs to be a social aspect to it all.

SW: Do you think international law needs to be strengthened around cyber?

SLJ: Yeah I do but it is futile, absolutely futile. Yeah they tried with drug trafficking law, normal warfare, and what I would call common law, but I can't see them doing something along cyber. I think it's too difficult and too complex. There are small pockets, such as the EU, but I think they are few and far between.

SW: Ok, Great, I think that is it. Was there anything else Sean?

SLJ: No, I think that's it.

11.3. Appendix III Interview Three

SW: Thanks very much for agreeing to talk to me Frank. I appreciate it.

FM: No worries. I've done a phone interview that lasted about half an hour, and face-to-face interview lasted about an hour. The face-to-face is different isn't it? So hopefully we should be closer to half hour.

SW: So a couple of things, ground work really. I've got a list of preset questions, but we can go off and talk about anything really. So they are just a guide. Also, there is no right or wrong answer, so don't worry about what you're saying, you're not being marked on it or anything.

FM: (Laughs)

SW: And it's just your view I am after, so it's not the company's view, it's just your view as a cyber security professional.

FM: No problem. What's the purpose of this? What the end goal of this research?

SW: So, I'm doing a Masters in patriotic hacking. It's a Masters by research. So, I choose my own subject, I research it, I write it up, I explain it et cetera et cetera. It's purely for me and it's very altruistic of yourself to help out. The reason for doing it is, know thy enemy. By better understanding hackers and their tools, motivations, who they are, then will be better placed to defend against them.

FM: Yep, I agree.

SW: So I'm going around and interviewing cyber security professionals, and asking their views on hackers, and their toolkits and any interesting nuggets that I can pick up. Trying to see if there is any correlation between everyone. And I'm also going to talk to a hacker. I've got one lined up, so I hope to be able to talk to them and then I have both sides of the fence.

FM: That will be interesting, I started off that side of the fence. Before it was popular or common. You know at my age, before or around the time of the Internet, but my view is that the techniques haven't changed. It's just the technology that has.

SW: Yeah. So the things that used to be done are still valid?

FM: Yeah, pretty much. Absolutely.

SW: One other thing to mention is that you are being recorded and what I do is, record the interview, transcribe it and then send it back to the interviewee so they can see that they are happy with it and if there's anything that needs redacting then I'll take that out no problem.

FM: Sure, okay, go for it.

SW: First question is, what's your history in cyber security?

FM: Okay, thinking about it I've been in cyber security for the last six, seven years. In a cyber security, information security related job. I started off as an ISO, the Information Security Officer, in the welfare to work sector. Then I moved on to finance, a company in Telford called Admin Re, they do insurance, pensions, that kind of stuff. They are part of Swiss Re. But before that, I was interested in IP. I was interested in IP since I got my ZX81 at age 11. You can probably guess my age from that.

SW: Yeah, I had a ZX81 so you are in good company.

FM: Yeah, 16K of RAM, and I learnt Z80 as you could get more in memory. So, then I worked at <COMPANY A> in Cyber security, but I've been interested in computers and IT all my life. So I moved from IT to Cyber security where it's more about service delivery, ITIL, Service management than the actual tech, which is what I actually enjoy and I still get to deal with this on the security side.

SW: Great stuff and did you make a conscious effort to move into cyber security or did you just kind of fall into it?

FM: Conscious effort? I recognised that there was something to do, and something that I was interested in, and when the opportunity came up I said I wanted to do this. At the time, it was like chicken and egg, you could move into information security if you had the experience but if you didn't have the experience then how could you get it, so how could you get the experience? So when we won a contract to deal with a company that wanted information security, I jumped at the chance.

SW: Okay, okay. Good, thanks for that. So moving on in the questions, the next one is about hackers in general and the toolkit they use. Do you have a view on what kind of toolkit they use?

FM: So, generally it's open source kit, things like Kali, lots of people will use whatever is out there, and then maybe tweak or use their own exploits. There is a variety of open source tools out there but I would say that Kali is the most commonly used.

SW: So open source then. And do you find that you have to, they are easy to find or do you have to go delving into the dark web to find them?

FM: Oh God widely available. Literally if you do a search on google or YouTube. Google you will find the tool, YouTube you will find the manuals of how to do it.

SW: So widely available then?

FM: Yeah, yeah. When I started there was nothing like that. You had to do it yourself, you had to work it out or read the manual. These days it's a lot easier to find out how to hack. The positive side of that is that more people know how to defend.

SW: Okay good, and the negative of that is that it's much easier to get into?

FM: Yes, you still get the script kiddies who don't really understand what they are doing they're just following other people scripts. But yeah, it's a lot easier to get the tools now.

SW: Talking of script kiddies, and coders and hacktivists, the different kinds of hackers, do you think that they use different tools or that they all basically use the same thing?

FM: I believe they would use the same. On the forums that I've been on in the past, everyone is basically using the same tools. Hacktivists wanting to get onto a system versus cyber criminals wanting to get onto the system, they going to do different things but basically they're using the same way of getting on there. Your goal may be different but basically you're still trying to break the security of a system.

SW: So moving on in the questions now. Do you think, in your view, that there is a difference between hackers in general, hacktivists and what I've called patriotic hackers or proxy force hackers if you like?

FM: What do you define as a proxy force/patriotic hacker?

SW: They are hackers who hack on behalf of the nation-state, but not necessarily with the understanding or the nod and the wink of the state, although that is often the case. They are doing it's out of patriotic, although may be misplaced, feelings for the state that they want to defend. So for example during the intifada between Israel and Hezbollah, Israeli hackers stood up to defend their nation even though the Israeli military didn't ask them, probably, to do so.

FM: Likewise with IS, you get hackers hacking IS websites to stop them showing homophobic videos and the like on there. Sorry, what was the original question again?

SW: It was not about toolkits any more, it was about whether there were any differences between the different kinds of hackers.

FM: In terms of the people, I don't think there's much of a difference. They're all doing hacking, they're just doing it for a different motivation. Why are they doing this?

SW: So they are all hackers, just their motivation is different.

FM: Yeah. You hear about cyber criminals who are now doing it for money, when I was doing it it was about the knowledge. Now you hear about during war, that they can help by hacking into sites and finding documents or by defacing websites. So it is purely about the motivation, what motivates someone to do it.

SW: Picking up on what you said there then there are people who are doing it to prove their abilities, there are people doing it to make money, and there are people doing it patriotically, that is to defend whatever they believe in. Do you think there are any other motivations other than those?

FM: Knowledge and your own kudos, if you look up on the forums it is about I managed to break into XYZ company, I managed to hack the FBI, it's about those sorts of claims.

SW: It's an ego boost?

FM: Absolutely.

SW: Ok great. Moving on, to talk a little more about patriotically hackers, do you think there is a certain view on who they are? For example, their age, gender, social status, job role?

FM: I don't know is the honest answer to that. There is a stereotype of a hacker, but I don't believe it, anyone can become a hacker.

SW: Ok. The stereotype is maybe young males, who are a bit bored…

FM: Yeah maybe socially inadequate, they spend more time on their computers than socialising. But is that always the case? I don't think so at all. And the reason I say that is because of the proliferation of hacking tools that are out there.

SW: So because it easier to get into attracting a wider base of people?

FM: Absolutely. Especially when you consider that the companies out there or not moving at the pace. This is why consultancy such as us are needed because companies are not protecting their cyber goods. Because of the ease with which people can pick up hacking and attack them with it.

SW: Okay great. So continuing with the theme of patriotic hackers, do you have a view on which countries will utilise them? So I mean where a country has a government with which has an active state of mind to support such groups.

FM: I think there is probably, it's something that I've gathered from news sources, like the Chinese, and the Americans, Israel and the groups out there, absolutely.

SW: So do you think it's just the norm for governments to engage with these types of hackers?

FM: I think it is becoming the norm because it is easier to engage with these people than to try and train people up to do this; and of course you've got that old phrase, plausible deniability.

SW: Yeah, yeah, absolutely. That comes up a lot in the literature. So we talked about the groups and the countries engaged in this kind of hacking, but what about the motivations of the people involved? So those proxy force hackers, what are their motivations?

FM: I think it comes down to what they believe in, yeah, it could come down to the country, their religion, and it could go back to kudos, I helped my country, I targeted my enemy, I helped take down the enemy website.

SW: Do you believe they will be paid by the governments involved, or do you believe they're relying on their nationalistic spirit?

FM: I don't know is the honest answer. It could be money or it could be we will not prosecute you for the crimes we found against you. I don't know is the honest answer, it could be payment or it could be other motivations that we've talked about.

SW: Yeah ok. So broadening out the topic a little, do you believe that in cyber warfare patriotic hackers or proxy forces will have a role going forward?

FM: Oh God yeah, when you get these forces of course you'll use them. So, absolutely, yeah. It depends on the capability of the group, but you see groups in the past, but yeah it depends on who's attacking and who is defending. Each group will have their strengths and weaknesses, like mercenaries themselves; it's who are they attacking, what's their target, which specialists.

SW: In your travels through cyber security, have you come across any groups who are acting in the national interest or are they really hard to find?

FM: I've never personally come across them, no. I've read about them in the press, I can't remember any of their names, I've read about the groups in Egypt against ISIS. There was another army one, wasn't there?

SW: Free Syrian army?

FM: Yeah, that's the one. These are the groups that are in the press. I don't come across them, I just hear about them second, third or fourth hand.

SW: Focusing on a couple of countries now, there's been a lot in the press about the cyber capabilities of Russia and China.

FM: Yeah, yeah.

SW: How do you see it? How do you see their cyber capabilities at the moment somebody use it for?

FM: Of Russia?

SW: Well of Russia and China if you can.

FM: Russia and China. Okay, let's start with China. I can use some examples with that. So China is interesting, I've come across a couple of examples of companies with my time at <COMPANY A> that

been affected by China. One is a Premier League football club where they had a Chinese dignitary come and visit, did Sean tell you this one by chance?

SW: No, it is a new one on me.

FM: Okay, whilst the dignitary was here, he had an entourage, and the entourage split up, and one of them was caught trying to put a USB key into a PC. There is also the case of the UK company that had been affected by Chinese hackers, they were designing a new wind turbine blade. One of the problems with wind turbines is that they can't be placed anywhere because of the disruption to radar. So this company has designed a new kind of turbine blade that didn't disrupt radar. So this would prevent a fighter jet from entering UK airspace, or any other kind of jet. The company went bust before they went into production. The reason for this is of a Chinese had hacked them and produced their own blades at a fraction of the cost.

SW: So that sounds like a case of good old-fashioned industrial espionage.

FM: Completely, and this is typically where I hear about the Chinese; industrial espionage. There was another one up in Scotland, a similar thing …

SW: The wave machine?

FM: Yeah that's the one. And you just think, umm , okay… and another one I've heard about is graphene. Have you heard about this one?

SW: Oh yes.

FM: I thought you might. So you know about the graphene?

SW: Yes, yes.

FM: So the Chinese is all about industrial espionage, how they can use their low-level cost of production and to reduce their cost of development. Basically, developing a product is expensive.

SW: So they are using it as a surrogate for their own R&D…

FM: Exactly, exactly. So, Russia is different. Obviously corruption is a lot higher level there. I believe that in Russia it's about breaking into banks, causing political disruption and business disruption, it's all about the criminal oligarch over there and expanding their power over the world basically.

SW: So it's more geopolitical?

FM: Absolutely.

SW: And do you think there's any money in it for the criminal elements?

FM: Oh God yeah, for Russia absolutely. When I read about Russia in the press it's always about them having a very good cyber capability. And they're using this for monetary gain.

SW: Hear a lot about the criminal gangs in Russia don't you?

FM: Absolutely.

SW: So those are two classic examples of big countries using the cyber capabilities, are there any other examples of maybe small countries doing it?

FM: Have you looked at Israel? Israel was meant to have a particularly good level of cyber capability.

SW: I've looked at them peripherally, I've looked at Stuxnet which was developed by the Israelis and the Americans. And I've read about the intifada and attacks on Israeli websites and the counterstrikes back but other than that, no.

FM: Yeah, I've been reading up about them and it's apparent that they have a very good cyber capability.

SW: Yeah I can well believe it and there are the kind of country that thinks actively about these kind of things.

FM: Yeah, in cyber security it's not the size of the forces involved that matter, unlike in conventional warfare.

SW: A small country can have a big impact…

FM: Exactly, exactly.

SW: I think in military parlance it may be called a force multiplier or some such.

FM: Yeah.

SW: I read about the hacks against Sony a few years ago and it was believed, but never proven, to be the work of North Korea. Do you see North Korea being very active in cyber warfare?

FM: I find it very hard to believe, with all the publicity about it it turns out that North Korea has a very poor IT infrastructure. So have they got that level of capability? Highly unlikely. But if you look at the ties they have with the Chinese, are they operating out of China, then possibly yes. They could be the source.

SW: So, coming back to the west, and the UK in particular, how well set is the UK to defend against these kinds of threats?

FM: I think we're getting better, we've had this multimillion touted for vetting in cyber security, Digital, and where you've got schemes like cyber essentials which is where the government says you can stop 80% of the attacks, that's a good start. I think also with the government pushing that Britain is a safe place to do business with, I think we'll see it getting better. And the other thing that I'm now seeing, and this was worrying me up until a couple of years ago, is the skills. We are now trying to push the skills that will mean the kids will have the skills and will get them into the sector. For example when I grew up we had something like the BBC micro computer.

SW: Yes, I remember.

FM: That was great. We are now seeing things like the raspberry pi go out and we are now seeing kids interested in how the basics of how computers work and not just being consumers of technology.

SW: Yeah, that means the skills coming down the line will be better.

FM: Yep, I firmly hope so. I see a lot of people who think they know IT when they're just consumers of IT. There's a big difference. It's only over the last couple of years I've began to see that gap reduce. Which is good because we're always going on about how little skills we see in cyber security.

SW: Ok. So that's the general population of the UK and the government, what about companies operating out of the UK, are they well set?

FM: When I first started here I have said yes. But after working here for 2 1/2 years I can say that I was shocked and surprised at how poor they are. What I see is management, top level management, and they focus on the governance. They see that they have a policy on information Security governance, cyber security governance, and that will stop people. But they are criminals, they are not abiding by the law; whether that's the law or a policy in your company. I don't think so. Historically we've seen that management haven't seen the risk. Over the last couple of years we seen all these threats out there and businesses need to do something about it. I'm in danger of getting on my soapbox there.

SW: No, no. It's ok. Actually we've now covered all the questions, the pre-set questions I had. Is there anything else that I've missed or you think is of particular interest that we need to talk about?

FM: I think one of the key things is about how motivation on hacking has changed. It's moved on from historically being something of interest, to very much doing it for money now. That seems to be the key motivator for doing all the hacking. Yeah, how can we monetarise a crime, how can we make money out of companies.

SW: And do you think that, unfortunately, they've made great strides in doing that, the criminals?

FM: Definitely, companies seem to think of one line of attack, APTs have been out there for a while now, and companies forget that when someone is knocking on your front door, and you're answering the front door, they're actually breaking in round the back. The companies fail to see that, a lot of organisations but I work with, they can only deal with one thing at a time, they don't seem to have multiple defences and are not looking out for other things going on. So that's about monitoring and saying that whilst we are being attacked here we're also being attacked over here.

SW: Do you think within businesses that they are saying that it isn't their job, and it's the job of government and the police to sort out?

FM: Yeah, I'm fairly certain there is a recent report out where companies are saying that the government needs to do this and do that. And I'm thinking, really? Hang on a second, it's your information, it's your data and you need to take some responsibility. If you were a manufacturer, you won't go to the government and say you need to protect this widget that we made. I think there is an expectation that the government has to do things for him. On the one hand the government can help because it has a good capability. On the flipside, it's organisations that need to take some responsibility for protecting their assets.

SW: Interesting that we just talked about corporate responsibility, but what about individuals? Do they understand the threats that they are under?

FM: God no. It always surprises me how ignorant the average user is to be honest. But again, the expectation is if you buy a product, like a car, you expect it to be safe. You don't expect the wheels to come off, or you don't expect the brakes to fail. If you are a consumer of IT, you expect the organisation that supplied it to make it safe.

SW: Interesting analogy with the car industry there. I think what you're saying is that whilst users are a bit ignorant of what they need to do to protect themselves, they have an expectation that the supplier will make the product safe to use.

FM: Yeah absolutely. I think that's a fair expectation to have as well. However, the supply can only do so much, the end user has to be relied on to not have a stupid password or to do anything too daft. That's where I think that education, business and government education, to the end user will

make it safer. That is why when I'm in a corporate environment, and I've done some awareness campaign, I will try to make it personal rather than, for example, say that company XYZ need you to do this. I talk about what it means for them. How would you feel if your daughter's pictures are online? It soon gets their attention.

SW: Yeah good point. To take your motoring analogy a bit further, the manufacturers can make a very safe car but you're still responsible for not driving it in front of a 20 ton truck.

FM: Correct. That goes back to you have to take a driving test, have driving lessons and learn how to drive safely. So yes, the manufacturers to make safe car but you still need to know how to drive it properly. At least for now, I await with interest how Tesla and Google get on with the driverless cars.

SW: And I worry about the hacking element of that, for the driverless cars.

FM: It's really frightening. I'm following it with interest, we had our marketing team here at <COMPANY A> go isn't this great, driverless cars. And I said I don't want to be a party pooper but we've already had a case about a car being hacked. How would you feel if I cut the brakes at 80 miles an hour?

SW: Yeah, the potential for mischief is huge.

FM: Yeah. Worryingly, the car manufacturers have only realised in the last two years about the need to be big on cyber security.

SW: Yeah for definite. I'd want some pretty good guarantees before I was happy for a car to drive me around.

FM: Absolutely. You're happy for a plane to do it though?

SW: True, true. Though they do have two fully trained pilots on standby. I guess it would be like having a fully trained Formula One driver alongside you in case they had to take over.

FM: My hobby is flying drones at the weekend. I do it a lot, taking pictures and video, and I was thinking about the cyber capability. How many people fly them manually or use all the safety features built-in automatically? On the form I was on I asked this question, a lot of guys who have flown model aircraft for years, fly them manually. They've got that level of skill i.e. a racing driver. The others who are just coming into it, it's literally as simple as connect up the controller to your iPhone and program it to fly automatically. You don't have to do anything.

SW: So it's a lower bar of entry?

FM: It's a lower bar of entry but the risks are not any less. To be honest this is where you hear about my drone flew away, the software failed. And you think, that's a kilogram device that can fly at 40 miles an hour, what happens when you hit something?

SW: And they've had near misses with aircraft haven't they?

FM: Don't believe the press. The last one I was laughing at was a drone had been spotted at 10,000 feet. I was like, okay, only military drones can get that high. If I try flying mine at 10,000 feet, it would run out of battery before I got anywhere near that. You read these and you realise that the press are just doing scaremongering.

SW: Fair enough.

FM: And I think as a result there is a love hate relationship with drones.

SW: I'm still waiting for Amazon to deliver the goods to me via drones, it'll be great.

FM: I think they will but there is so much bureaucracy to get through to do it. It will get there though. I'm waiting for someone to try and use these for warfare. I read recent reports where people were saying that look, there are people trying to use these to carry grenades. And I just laughed, because if you try to put that size grenade are on a drone it wouldn't be able to take off.

SW: But going back to the hacking, if Amazon do try and use drones to deliver expensive goods, then there is a motivation to try and hack that drone and deliver it to yourself instead.

FM: And I am sure that's going to happen. They're all going to be automated and there's gonna be weaknesses in the system. Crikey, if you can get into that system you can get the drone to deliver the diamonds to yourself instead.

SW: It's a whole new avenue of crime.

FM: Absolutely, they got away with my jewels, where did they go?

SW: So that's it Frank, that's all the questions answered. Was there anything else?

FM: I'll be interested to see what the results are and what the trends are, if any.

SW: No problem.

11.4. Appendix IV Interview Four

SW: So, Mike thanks for coming. Can you tell me a bit about your background, your history, in cyber security?

ME: Yes, so, I started way back when, in mechanical engineering. So CAD/CAM. Working for companies that were manufacturing aircraft components. There was a fork in the road that took me down the computer route, so I dropped the engineering. So that was much more IT infrastructure management. So over the years I've built up my experience in service, networks, infrastructure and how things worked. Usually in opposition to security teams, especially as I was working more in an exploratory role trying to find new solutions for the company I was working for. Trying to break into new markets, that kind of stuff. There was a lot of opposition from IT security to things like robotic devices, or bring your own device. So that got me interested because I believed that security could play a more constructive role rather than just blocking all these new solutions. So I switched my focus to more IT and cyber security roles, gained a couple of qualifications, and I've been working in that area for three or four years now.

SW: What were the qualifications?

ME: Primarily it would've been the CISSP qualification. That is certified information system security professional. Which is great, it was quite an intensive piece of training.

SW: Yeah, I've seen the manuals and they're very thick.

ME: Yeah, in hindsight, I come from architecture teams and, in hindsight, they should all try and get this qualification. Even if they don't focus on security, the information gained should be used in everything that they work on. Whether it's storage, networking, whatever.

SW: And do you consider yourself staying in cyber security?

ME: For the time being, yeah. There is plenty of work and it's pretty interesting. I don't focus exclusively on cyber security, there is a lot of fringe work around that that I work on. I have an interesting mix of theoretical IT security, and more hands-on IT security, which I quite like. So for the time being, yes I'm staying.

SW: There's lots going on in the world, so it's in demand, absolutely.

ME: And it's changing regularly, which I like. There would be nothing worse than a skill that stayed the same for 30 years. The technology is changing, and therefore the risk is changing, and you have to stay on top of that from a security point of view. Which keeps it fresh.

SW: Okay, cool. So moving on, to talk about hackers now. As I said in the email, there is no wrong answer, if you don't know the answer just say so, and it's your opinion not the opinion of a company or whatever. So, what toolkits do you see hackers using today?

ME: There is a couple that I'm aware of. I think it's greatly influenced by coders. I think most people are not coders, and these people use existing tools such as Metasploit.

SW: Sorry, what was that called?

ME: Metasploit. It is a popular one. It's used by security auditors but also by a wide variety of hackers. The reason for that is that defects and vulnerabilities are published for this thing so you don't need to be a coder with a massive amount of skill. You can go shopping in the right part of the Internet to get it for yourself. So my opinion is, the vast majority of people work that way. They will

use the Metasploit, use someone else's expertise, and build an attack and then use that attack for whatever reasons.

SW: Yeah.

ME: And I believe there is a small section of that community that can create that code in the first place. Developers that have the right knowledge to be able to exploit those things.

SW: Are they using Python as a language?

ME: I would doubt it. I don't know, is the simple answer. But I doubt it. I don't think the language Python gets you to the right depth. I would imagine that the coder is writing software in exactly the same way that a software house is. So they are going to be using C, C++. You know, low-level programming languages, and they're writing proper applications. I think where Python might come in, is where someone has developed a vulnerability and attack for that. Building that may take the form of a python script, or some kind of script.

SW: Yeah, that makes sense. We talked about different hacker types, do they correlate with different toolkits? I think you hinted that they do, coders use C++, whereas Hacktivists and criminal gangs exploit those codes that have been developed.

ME: Yeah, I think it depends on the type of hacker, and the type of hacker that you are depends on your motivation. I can see a way where you could be employed, in whatever way that may be, and you are given the tools to perform the attack. You just use them, you execute them.

SW: Yeah.

ME: But I would say that the vast majority of people, without that developer skill, just buy the best that's available.

SW: We touched on the different hackers around, hacktivists, coders and patriotic hackers or, if you like, proxy force hackers, and the way that they differentiate themselves by using different toolkits. Do you think there are any other special cases that we need to be aware of? In the hacking community, who differentiate themselves by their use of toolkit?

ME: I don't think so. I think that the tool that is used to perpetuate the crime is just one part of a longer chain. Around that you are limited by the vulnerabilities that exist and the tools that can be used to attack them. In the NHS example, there is a vulnerability that needed to be attacked in a certain way; it almost determines the tool that you use. Additionally, you've got the method that they used to trick the user into triggering the software. Whether that's phishing, social engineering etc. This is separate to the technology that you use, you have to have the skill to trick the user into triggering the malware.

SW: There is certainly evidence out there that most successful attacks rely on social engineering, phishing rather than a technology lead attack.

ME: I think of hacking, certainly in an organised way, as being like an industry. Whether this completely aligns with what you call a patriotic hacker, or I would say whether it's related to the aims of the government, either intentionally or paid for, I think that starts to determine the types of attack. A Government is going to attack in very specialised ways, maybe over massive periods of time, instead of very short pieces of time. Slipping a packet into your network every couple of weeks, you're never going to notice it, rather than a full blown attack. I think that kind of thing goes on, but it's in a completely different way to what you call script kiddies. They have a much shorter

period of time in which to exploit something. The NHS attack was a good one, in that I think it was financially motivated, It could've been a distraction, I could be wrong. In the same way that junk mail gets pushed out, it's a broad attack, in the basis that you might get a couple of people to respond and pay you, job done. I think that's what happened.

SW: Just for my notes. When we talking about the NHS, which talking about the Wannacry virus?

ME: Yes. I posted on Twitter the other day that people are thinking this is the first time this kind of virus has been released. And it's not. Far from it. These are been happening for 15 to 20 years, when I've not been focused on cyber security. These things are not new, they've happened for a good long while. It's an indiscriminate weapon. It's deployed, without any real focus, and attacks wherever it may be, and that is the Wannacry virus.

SW: I've been amused by some of the newspaper reports, saying that the NHS has been targeted, but it hasn't. It's hit all over the world, it's not been aimed at the NHS. Some of the newspapers picked up that it had been targeted at the NHS, and it simply wasn't.

ME: I agree.

SW: Talking of these kinds of viruses, what do you think are the most prevalent and/or dangerous attacks that our society faces today?

ME: I think one of the same for that criteria are phishing attacks. It's the kind of attacks that are focused on people who are not that IT literate. The general population at large, it's fair to say, is not that focused on these kind of attacks as much as, say, an IT management team will be. So it's the general population who are more at risk. And I think that's where the prevalence for these phishing attacks is. People are completely unaware of the fact that they are being attacked. They almost have no capability to determine what is dangerous and what is not dangerous. Part of the danger is that people had money stolen and their identity stolen, but I think a longer term risk is that there will be an erosion of trust in IT systems generally.

SW: I was reading around about the Internet of things the other day and it was an interesting report saying about 80% of businesses are saying it's the next big thing, whilst 70% of that same population also believe that the level of security risk in there is very high. It's almost like they expect that it's coming but that they also expect it to be rubbish at security. It's an interesting position. It's like they can't stop it happening, even though they are really worried about it happening.

ME: Yeah and over time will it change the way people do things? On a thread I was on the other day someone was advising that if you are in a cafe like this that you don't do any shopping on the Wi-Fi. For example, don't Internet shop. Which I don't necessarily agree with, but at the same time, if that train of thought spreads you end up with…

SW: Inhibits business growth on the Internet?

ME: Sometimes businesses may move away from the Internet because of things like that, unless we can find a different kind of technology that makes things easier and more secure.

SW: So the security of it is key to building the trust.

ME: Absolutely. I was reading about something a number of years ago where people were not trusting cash machines; what if their card goes missing? It was only when the banks came up with new policies and procedures saying that they would take up some of the responsibility for that that people started to trust the machines.

SW: That is very true. For example, if your credit card get stolen and is used in Bolivia, the bank will cover your losses. And it may take this kind of thinking to secure trust in the Internet.

ME: Yeah, I think it might. But that is yet to emerge.

SW: So moving on, to proxy force hackers or patriotic hackers. Do you know what I mean by that term?

ME: My interpretation of what that would mean, would be someone who, with the agreement of their government or without the agreement of their government, is carrying out malicious IT acts on behalf of their country.

SW: Yeah, that is exactly it. Sometimes there is an explicit agreement or sometimes just an implicit agreement. A nod and a wink. Or sometimes there is genuinely none. But they are still acting on what they think is the good of their country. So talking about them do you have an idea of what a typical hacker would look like.

ME: So it's an interesting one, I would be tempted to go with the stereotype of a younger person who is interested in IT but I don't necessarily buy into that, given my own age. I don't think you can pin it down exactly. It's more to do with the type of person rather than the demographic. People who possess the right skills, the motivation, the right attitude to a particular cause. So you might be able to align it with a political alignment. Interested in a particular political action, I don't know, Brexit for example. Leavers versus remainers for example. Or Scottish independence, that kind of thing. So where someone feels particularly strongly, and I don't think you can put that down to a type of individual. It would be political or ideological alignment with a particular topic which would define them rather than their age or gender. If that makes sense…

SW: It does make sense and it sort of feeds into another of my questions, what are the motivations of these people?

ME: Are we talking about the political side or Hacktivists?

SW: They can be whatever you want it to be.

ME: The political side are aligned with their country's aims or what they think their country's aims are. Or in some way related to the benefit of their country. Whereas a hacktivist, that you wouldn't consider to be a patriot, is more likely to be against the government rather than being in their favour. So I guess they are really the same thing, it's just their motivation goes into different directions.

SW: You are exactly right, there are Hacktivists, for example anonymous, who almost attack their own countries; a political process or a reaction to something. And they are typically quite liberal minded people. Whereas the patriotically hackers tend to be more narrow-minded, less liberal, more nationalistic. They see threats to their country, they're not trying to change the country from within but trying to protect it from without.

ME: It's interesting because it's in their opinion what the country needs or wants. Every country is split in all different ways. What is interesting is that a group of patriotic actors could do with support from the government in some way. Let's say the government supported what they were doing, they could provide them with funding, people, technology. But if the government didn't support them, then a foreign government might well do the same thing. It's whoever has the benefit for that particular cause I guess.

SW: From what I've read, there are lots of hackers who are available in Eastern Europe or the Far East, they have the skills and will either act politically or are for hire. Governments can get the ones that are for hire and use them and arm them with the cyber weapons of their choosing. And then point them at a particular target. However they are a tough weapon to wield; yes they give you plausible deniability but those weapons can be turned against you or sold on et cetera et cetera.

ME: It's really similar to supplying arms to a group.

SW: Yeah. Whilst they are in your favour it's great but then 10 years later they turned against you. The CIA armed the mujahidin in Afghanistan in the early 80s and eventually that turned round and bit us all.

ME: It is the same for IT. The differences is that IT has a much lower barrier of entry. You can hire zombie botnets, there is very little to stop those with little finance from using these things.

SW: And you can do it all over the world, your target can be anywhere in the world. To get us back on track, although we don't have to follow the questions exactly, talking about patriotic hackers. Do you have an idea which countries would utilise them?

ME: I'm not really thought about it before, every year on the news there will be some new topic comes up that you didn't expect. For example, the USA. If you have asked me a year ago I wouldn't have thought it, but now you have a president who has a sizeable portion of the country against him. Might that motivate people to do this kind of thing? Should kind of depends on what's going on in the world. There are countries in the world that perhaps don't police these actions as robustly as other of countries do. Or even don't care. These people are allowed to operate much more freely than they would otherwise. But also there are volatile parts of the world which would motivate people to do these kind of action. Brexit might not motivate hacktivists but in volatile parts of the world, which have bad leaders or dictators running things, then the motivations will be much stronger to do these kinds of things; there is very little to stop those with little finance from using these things.

SW: So you're talking about Hacktivist there, people who rise up against their own country....

ME: I see them as roughly the same thing, it depends upon the topic and that topic can change. So the topics can change, but I think there are certain topics around the world which make motivations much stronger I think that's what I'm saying.

SW: Yeah. So, part of what I'm studying is the relationship between these hackers and geopolitics, so, for example, North Korea has a strong cyber capability and, allegedly, was involved in the Sony hacks. A few years back. So, which countries do you think use cyber weapons as a regular part of their arsenal?

ME: I would think that most of them do this. I think the difference is whether it's visible. Does North Korea do this? I would bet my house on the fact. Does the US? Yes. Does the UK, yes. So kind of depends on your political allegiance. He gets onto the topic of terrorists versus the army, what's the difference, one is funded and one is not. But they still have ideology that they follow. And with IT it's the same kind of thing. In North Korea I would bet that it was government backed. But in the US and UK and other developed countries where you think that it wouldn't happen, it does go on but it's a lot more covert. But with the definition of a political activist, at what point do they start being considered part of a government. There is a grey line between them being a separate entity and actually being part of the government. So government can take advantage of someone for their

political aims, I think in the west then maybe a distance there but in North Korea they can be considered to be employed by the government. It's controlled and paid for by the government.

SW: In terms of future conflict, how do you think these cyber weapons will be used?

ME: Well, last week's example was probably unintentional but when you think about it, national infrastructure, TV, power stations, Health institutions – destruction of those would be much more effective than the say bombing a motorway. There is now so much reliance on all kinds of IT in the developed world that they would be very powerful weapons to use. If you can turn off countries power or their water or their oil, stop its cargo from leaving, any of these things. Before long, it would be massively disruptive.

SW: I guess with the cyber weapons we seen today, they are fairly short acting, they might disrupt something for hours or days where is if you blow up a motorway with a tomahawk it could be weeks or months.

ME: But look at Stuxnet for example. That was a fairly slow burn weapon; it was you to destroy part of a nuclear plant. That had to be politically motivated.

SW: Allegedly developed by Mossad and the Americans.

ME: These kind of things are very capable of doing something that you couldn't do physically. You wouldn't bomb a nuclear plant, no one is going to do that. So they are very powerful weapons and, as I've said before, the barrier to entry is so much lower than conventional weapons. A country with low resources could arm themselves with cyber weapons much more easily than physical weapons.

SW: Yeah worrying times. I guess as you become more developed then you rely more on IT you become more vulnerable to this kind of attack.

ME: Yeah.

SW: So talking of which, the Internet of things is something that I've been reading an awful lot about. Do you see that as being positive or negative for cyber security?

ME: I wouldn't say it's positive or negative, rather it introduces a new area which cyber security should focus on. So the number of nodes on the network increases, then the risk increases with it. I think on a positive note, there is a lot that can be developed technology wise by industry. I don't think it shouldn't be used, what it does do is expose bad practice. And that bad practice already exists. Haven't really thought about this topic much but if you put a cheap device on the network which hasn't had much development in cyber security terms then it will be a risky product. I think everything should have cyber security in mind, otherwise if you buy a cheap product it will have poor security. The bad angle is, these things are gonna exist on the network and they can be taken advantage off. It provides an organisation with a botnet of 10 million WebCams which didn't exist before. The other downside is that when these products are purchased they can't be easily changed. Well whereas with a PC you can patch it to improve security…

SW: But patching your fridge?

ME: It's doable but has anyone really thought about it. The focus will be on what the consumer wants from the fridge rather than the security of it.

SW: Absolutely. I've been thinking about driving, I like my cars, and the rise of autonomous electric cars has got me thinking about the possible hacking of these.

ME: Yeah. Intentionally or by accident. If something was to spread unintentionally, it could just as easily knock out a car as someone's laptop.

SW: When you think of it like that it's almost like a biological weapon, you intend to target one country but then it spreads.

ME: Yeah.

SW: Cyber weapons are like that, they don't know when to stop at the geographical border.

ME: Same again, I think the development of malware is a professional, organised industry. You get good quality software, you get good quality malware. Valley is, it was built for the target it was intended for whereas others… Target things we didn't mean to.

SW: And spread where you don't want them to.

ME: The other thing about car system is who's got expertise in security for a car? You can see whether your car is locked with a key, but it's much more difficult with software. Whose fault is it when your car disappears? Was it a bug, did I leave the car open.

SW: Or did someone hack it and remotely drive it away. Going to be interesting isn't it.

ME: So I don't know where that industry is going to go. I had a car stolen recently; I had all the keys, I don't know how it was done.

SW: So can we come to the end of all the questions I had down. Thinking about what we discussed Mike, is there anything else we should have a quick discussion on?

ME: Related to hacking?

SW: Yeah.

ME: With all the phishing attacks and what happened to the NHS last week, I think what's interesting is what we think of as the Internet - as in providing a hyperlink in a message or an email is becoming dangerous. It's becoming something that you wanna stop people from doing. The very thing that allowed the Internet to become popular and widespread is becoming a risky thing to do. I think we need to have some thoughts about how we going to do that, how are we going to be able to provide a link to some sort of resource on the Internet? How can you make these things visible in the way that the user can trust what they see on their screen? It's going to be a very difficult thing to do.

SW: I guess it's already changing behaviour, how does an internal IT department communicate with its staff. They've got to think about how to make sure it doesn't look like a phishing attack.

ME: Totally. We've just developed a system around enrolment, and a 2 badge authentication system sends an email as you enrol. But the link takes you to the vendor. Which we don't want them to click on. It's the basis of the Internet, hyperlinks are used to embed in a document that took you to another resource on the Internet. That raw principle on what the Internet was based on is now too dangerous to use. I think we almost need to start providing signpost that people can read for themselves rather than giving them hyperlinks. Start from that portal or use this Google search term or something like that where the user has to do it rather than you automating it for them. But it's going to fundamentally change how technology works.

SW: It's true of Internet banking now, they say don't click on the link, just use a Google search and find the correct site and trust the padlocks.

ME: It also comes back to this concept of human error, I don't necessarily believe in human error. We are humans, and we do predictable things, we need to change the technology to avoid those weaknesses. So we need to tell them how to find the item or which portal to use rather than automating it for them. To the point where hyperlinks become unreliable. But where does that leave technology and websites?

SW: Some big things to think about there. Great, was there anything else?

ME: I don't think so.

‹ V Interview consent form

Manchester Metropolitan University

Date 15/05/2017

Name Steven Wood
Course Masters by Research
Department Business School
Manchester Metropolitan University
Tel: 07717 030930

Title of Project: Patriotic Hackers

Name of Researcher: Steven Wood

Participant Identification Code for this project: PH/ME

Please initial box

1. I confirm that I have read and understood the information sheet dated 08/03/2017 for the above project and have had the opportunity to ask questions about the interview procedure. ☐

2. I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason to the named researcher. ☐

3. I understand that my responses will be sound recorded and used for analysis for this research project. ☐

4. I give/do not give permission for my interview recording to be archived as part of th research project, making it available to future researchers. ☐

5. I understand that my responses will remain anonymous. ☐

6. I agree to take part in the above research project. ☐

7. I understand that at my request a transcript of my interview can be made available to me. ☐

_____	_____	_____
Name of Participant	Date	Signature
_ Steven Wood _____	_____	_____
Researcher	Date	Signature

To be signed and dated in presence of the participant

Once this has been signed, you will receive a copy of your signed and dated consent form and information sheet by email.

11.6. Appendix VI Research ethics form

ETHICS CHECKLIST

This checklist must be completed **before** commencement of **any** research project. This includes projects undertaken by **staff and by students as part of a UG, PGT or PGR programme**. Please attach a Risk Assessment.

Please also refer to the University's Academic Ethics Procedures; Standard Operating Procedures and the University's Guidelines on Good Research Practice

Full name and title of applicant:	Steven Wood
University Telephone Number:	07717 030930
University Email address:	steven.j.wood@stu.mmu.ac.uk
Status: All staff and students involved in research are strongly encouraged to complete the Research Integrity Training which is available via the Staff and Research Student Moodle areas	Undergraduate Student ☐ Postgraduate Student: Taught ☐ Postgraduate Student: Research ☐x Staff ☐
Department/School/Other Unit:	Faculty of Business and Law
Programme of study (if applicable):	Masters by Research
Name of DoS/Supervisor/Line manager:	Professor Dominic Medway
Project Title:	Patriotic hackers; their role in future Cyber conflicts.
Start & End date (cannot be retrospective):	10/09/16 to 10/09/17
Number of participants (if applicable):	n/a
Funding Source:	Self funded

Brief description of research project activities (300 words max):

A literature review will be performed to find any relevant reading on the subject of patriotic hacking. Current thinking is that this review will fall somewhere between a systematic and a narrative review. The review will also discuss any limitations of a study into patriotic hacking, why research in the area needs to occur, and how much empirical evidence on the subject is already out there. The literature review will utilise journal articles, books, conference papers, web blogs and any other relevant discourses that can be unearthed. The literature will be critically evaluated, a discussion will be made on areas for further research and a bibliography created. Problemitisation will be made by discovering whether the following apply:

* Confusion – i.e. contradictory evidence

* Neglect – i.e. little robust research

* Alternative perspectives – i.e. other scenarios which may have indirect relevance and/or implications for the subject of patriotic hacking

In parallel with this, contact will be made with the hacker community on the web. It is envisaged that this will take the form of an ethnographic study, using grounded theory. The ethnographic study will have the usual challenges around it: bias, selective perception, error, ethics, achieving and maintaining access. Observational preferences in this research endeavour will also be decided: up close or maintain your distance?

A field diary will be kept and a decision on what form of transcription to be used made.

The field diary will comprise of:

* Record of places, the day-to-day routine and situations

* Observation of behaviour * Personal reflections on situations and feelings

* Post-fieldwork reflections

As the research is developed, the data sources to be used will be considered and may include:

* Participant diaries

* Video/audio recordings * Photography

* Various forms of art

* Ethnographic fiction science * Memory

* Interviews

Depending on the level of access granted (see key challenges), interviews will be conducted with industry and academic experts in lieu of the hackers themselves providing information. The methodology used will ensure the safety of the researcher and the hackers researched. The capabilities of the Computer Science Department at the University will be leveraged to ensure the safe set up of any computer devices used to make contact with the hackers.

	YES	**NO**

Does the project involve NHS patients or resources? If 'yes' please note that your project may need NHS National Research Ethics Service (NRES) approval. Be aware that research carried out in a NHS trust also requires governance approval. Click here to find out if your research requires NRES approval Click here to visit the National Research Ethics Service website To find out more about Governance Approval in the NHS click here	☐	☐x
Does the project require NRES approval?	☐	☐ x
If yes, has approval been granted by NRES? Attach copy of letter of approval. Approval cannot be granted without a copy of the letter.	☐	☐

NB Question 2 should only be answered if you have answered YES to Question 1. All other questions are mandatory.	**YES**	**NO**
1. Are you are gathering data from people?	x	
For information on why you need informed consent from your participants please click here		
2. If you are gathering data from people, have you:		
a. attached a participant information sheet explaining your approach to their involvement in your research and maintaining confidentiality of their data?	x	
b. attached a consent form? (not required for questionnaires)	x	
Click here to see an example of a participant information sheet and consent form		
3. Are you gathering data from secondary sources such as websites, archive material, and research datasets?	x	
Click here to find out what ethical issues may exist with secondary data		
4. Have you read the guidance on data protection issues?		

a. Have you considered and addressed data protection issues – relating to storing and disposing of data?	x	
b. Is this in an auditable form? (can you trace use of the data from collection to disposal)	x	
5. Have you read the guidance on appropriate research and consent procedures for participants who may be perceived to be vulnerable?	x	
a. Does your study involve participants who are particularly vulnerable or unable to give informed consent (e.g. children, people with learning disabilities, your own students)?		x
6. Will the study require the co-operation of a gatekeeper for initial access to the groups or individuals to be recruited (e.g. students at school, members of self-help group, nursing home residents)?		x
Click for an example of a PIS and information about gatekeepers		
7. Will the study involve the use of participants' images or sensitive data (e.g. participants personal details stored electronically, image capture techniques)?		x
Click here for guidance on images and sensitive data		
8. Will the study involve discussion of sensitive topics (e.g. sexual activity, drug use)?		x
Click here for an advisory distress protocol		
9. Could the study induce psychological stress or anxiety in participants or those associated with the research, however unlikely you think that risk is?		x
Click here to read about how to deal with stress and anxiety caused by research procedures		
10. Will blood or tissue samples be obtained from participants?		x
Click here to read how the Human Tissue Act might affect your work		
11. Is your research governed by the Ionising Radiation (Medical Exposure) Regulations (IRMER) 2000?		x
Click here to learn more about IRMER		
12. Are drugs, placebos or other substances (e.g. food substances, vitamins) to be administered to the study participants or will the study involve invasive, intrusive or potentially harmful procedures of any kind?		x
Click here to read about how participants need to be warned of potential risks in this kind of research		
13. Is pain or more than mild discomfort likely to result from the study? Please attach the pain assessment tool you will be using.		x

Click here to read how participants need to be warned of pain or mild discomfort resulting from the study and what do about it.		
14. Will the study involve prolonged or repetitive testing or does it include a physical intervention?		x
Click here to discover what constitutes a physical intervention and here to read how any prolonged or repetitive testing needs to managed for participant wellbeing and safety		
15. Will participants to take part in the study without their knowledge and informed consent? If yes, please include a justification.		x
Click here to read about situations where research may be carried out without informed consent		
16. Will financial inducements (other than reasonable expenses and compensation for time) be offered to participants?		x
Click here to read guidance on payment for participants		
17. Is there an existing relationship between the researcher(s) and the participant(s) that needs to be considered? For instance, a lecturer researching his/her students, or a manager interviewing her/his staff?		x
Click here to read guidance on how existing power relationships need to be dealt with in research procedures		
18. Have you undertaken Risk Assessments for each of the procedures that you are undertaking?	x	
19. Is any of the research activity taking place outside of the UK?		x
20. Does your research fit into any of the following security sensitive categories: • commissioned by the military • commissioned under an EU security call • involve the acquisition of security clearances • concerns terrorist or extreme groups If Yes, please complete a Security Sensitive Information Form		x

I understand that if granted, this approval will apply to the current project protocol and timeframe stated. If there are any changes I will be required to review the ethical consideration(s) and this will include completion of a 'Request for Amendment' form.

x☐I have attached a Risk Assessment

x☐I have attached an Insurance Checklist

If the applicant has answered **YES** to **ANY** of the questions **5a – 17** then they must complete the MMU Application for Ethical Approval.

Signature of Applicant: _____Date: 24/11/16
(DD/MM/YY)

Independent Approval for the above project is (please check the appropriate box):

Granted

☐ I confirm that there are no ethical issues requiring further consideration and the project can commence.

Not Granted

☐ I confirm that there are ethical issues requiring further consideration and will refer the project protocol to the Faculty Research Group Officer.

Signature:_____Date: (DD/MM/YY)

Print Name: ___Position: _____

Approver: Independent Scrutiniser for UG and PG Taught/ PGRs RD1 Scrutiniser/ Faculty Head of Ethics for staff.

n 6. October 2015

11.7. Appendix VII Possible interview questions

Possible interview questions: 15/05/17

Themes

Background

- What is your history in Cyber Security?

Hackers – general

- What took kit do hackers use today?
- Do the different hacker types (e.g. hacktivist, coder et cetera) correlate to different toolkits?
- In your view, what is the difference between hackers, hacktivists and patriotic hackers?
- What types of hacking are, in your opinion, most prevalent and/or most dangerous to society?

Hackers – patriotic

- In your opinion, what does a typical patriotic hacker look like in terms of age, gender, political affiliation, social position and job roles?
- Which countries utilise patriotic hackers with either explicit or implicit government support?
- What do you think the principal motivations of patriotic hackers are?
- How are these motivations different to hacktivists and coders?

Cyberwar – the future

- In future cyberwars, what role do you think patriotic hackers have to play?
- How effective do you think patriotic hackers can be in cyber warfare – what are their pros and cons?

11.8. Appendix VIII Participant information form

Participant Information Sheet for Patriotic Hacking 08/03/2017

I would like to invite you to take part in a research study. Before you decide you need to understand why the research is being done and what it would involve for you. Please take time to read the following information carefully. Ask questions if anything you read is not clear or would like more information. Take time to decide whether or not to take part.

What is the purpose of the study?

Primarily the purpose of the study is educational, it is being undertaken as part of a Masters by Research (MRes) higher degree.

Why have I been invited?

Your background in Cyber Security means your opinions and views carry weight and can be taken, with others, to be a representation of the wider Cyber Security community.

Do I have to take part?

It is up to you to decide. We will describe the study and go through the information sheet, which we will give to you. We will then ask you to sign a consent form to show you agreed to take part. You are free to withdraw at any time, without giving a reason.

What will happen to me if I take part?

You will be asked to take part in a semi-structured interview of up one hour's duration where a voice recorder will be used for the purposes of transcription. The interview can be face to face or over a telephone.

Expenses and payments?

No expenses can be claimed and no payments will be made.

What will I have to do?

You will be given the questions in advance and then asked the same questions in the interview although further sub-questions may be asked if warranted. There are no right or wrong answers; just try to answer them as best you can.

What are the possible disadvantages and risks of taking part?

There are no foreseen risks in taking part in this study.

What are the possible benefits of taking part?

We cannot promise the study will help you but the information we get from the study will help to increase the understanding of Patriotic Hacking.

What if there is a problem?

If you have a concern about any aspect of this study, you should ask to speak to the researcher (Steven Wood) who will do their best to answer your questions (07717 030930).

If you remain unhappy and wish to complain formally you can do this through contacting the Director of Studies, Professor Dominic Medway. (Institute of Place Management

Journal of Place Management and Development| Academic Editor; Manchester Metropolitan University ¦ Faculty of Business and Law

Room 6.12 ¦ 6th Floor ¦ All Saints Campus ¦ Oxford Road ¦ Manchester ¦ M15 6BH)

Will my taking part in the study be kept confidential?

All information which is collected about you during the course of the research will be kept strictly confidential, and any information about you which leaves the university will have your name and address (if given) removed so that you cannot be recognised.

What will happen if I don't carry on with the study?

If you withdraw from the study we will destroy all tape recorded interviews, but we will need to use the data collected up to your withdrawal.

Further information and contact details:

Researcher Steven Wood

Contact: 07717 030930

steven.j.wood@stu.mmu.ac.uk

11.9. Appendix IX Field diary

21st October 2016

Connect to freedom hacker.net to find list of secure/private email addresses. Attempted to set up an account using a free service that didn't require phone numbers or new software being added. Attempt failed.

Concurrently, there appears to be a major cyber attack on going in America. Appears to be a DDoS attack against Dyn, a DNS provider, and some are speculating that it's to do with the hacking group Anonymous and Wikileaks.

23rd October 2016

Cyber attack against Dyn looks like it was caused by corrupted devices on the Internet of Things (IoT). It appears the devices were compromised by malware called Mirai, and involved tens of millions of IP addresses. It shows the importance of IOT and cyber security.

18th November 2016

Went to an independent cafe with free Wi-Fi to access the Dark Web. No registration with the Wi-Fi provider was required, therefore keeping anonymity.

Used the locked down laptop to access the Dark Web. Found various websites using the "hiddenwiki.org".

Attempted to join the "crack hack forum".

Request for registration was rejected.

Attempted to register with the "offensive community" – another hacker forum. This was blocked due to the user name or IP address suspected of being a known spammer.

Repeated registration after restarting TOR (to refresh the exit node and therefore the IP address) and had the same result.

An apparent issue with any Wiki links is that they are often old (i.e. no longer valid) or have been taken down by law-enforcement action.

Attempted to join the "darknet forum" and sent a message to the administration team explaining my position. Awaiting a response.

20th November 2016

Whilst reversing the dark web it's apparent that I must retain a professional detachment; some of the subjects and titles presented to me are disturbing. A great deal cover financial misdemeanours which aren't too worrying; far worse are the sites for paedophiles – I decide immediately that none of my research will involve such sites. Other morally dubious web links advertise drugs, blackmail or hitmen for hire. I do go on one of the latter sites out of professional thoroughness (and I guess morbid curiosity). The site offers regular blackmail, extortion, DDOS attacks against competitors to, yes, the hitman service. I get the impression it's probably some teenagers wet dream; maybe just a rip-off where someone takes your money and does nothing/threatens to report you to the police – but it is troubling nonetheless. Looking under the blackmail tab (website appears professionally constructive) give some sub options including one for ruining a business/romantic competitor by

getting them added to the sex offenders register (possibly indicating a UK site?). There is a post alongside a price (£250, payable in bitcoins) that they can do this within a few hours of payment being received.

As I wade through this morass it becomes more apparent as to why any genuine, miscreant hackers would not want to be interviewed. They're anonymity is their cloak and they protect it vigorously.

21st November 2016

Went to a nearby cafe to access free Wi-Fi. It was a Costa Coffee house. However, the Wi-Fi provider required you to provide a mobile number to access the Internet there. I didn't do this for fear of losing anonymity.

Tried to do the same at the nearby McDonald's restaurant, and had the same result (the same provider).

To provide better opportunity for research, a SIM free cheap and basic mobile phone was bought from Argos. No registration details were required. Likewise a free SIM was picked up from a newsagents. I'll be using these to enable myself to access the free Wi-Fi that large chains of coffee shops et cetera have. I suspect that the reason you have to register some details with them is something to do with the Prevent terrorist legislation.

26th November 2016

Bought a mobile phone with cash and no personal details were given. A free SIM card was obtained from a local newsagents, again, with no details given. Used the website "duck duck go" as a search engine to find "darknet forms". To get onto the form to you first have to submit to a recapture security check to prove you're not a robot.

There was no reply to my mail on the 18th of the 11th, except for a generic "welcome to darknet forms" type message. Most of the posts on the forum appear to be carding messages from sellers. The forum is meant to be both a hacking and carding site but it is the latter that stands out. Posted a reply to a thread saying "...." simply to see if posting works. The forum doesn't seem very active; though there were a few complaints from users on the slowness of using the forum – these were countered by some responses calling them ‘newbies’ or ‘noobs’.Trying to get an accounts on the "offensive community" forum again but got the same spammer message.

Decided to create a new email address on “Yahoo.mail” using a new username. The registration was allowed to happen after I gave the mobile number of the newly purchased phone. However using this new account I still failed to get onto the “offensive community" website - the usual message came back about spamming.

Contacted the "deepdotweb" administrator to see if I can help with contacts, it appears to be a news site dealing with the Dark Web and marketplaces and have done interviews with hackers themselves.

12th December 2016

Went to Sainsburys cafe, no extra security was needed to log in. Looked at “the Reg” article on 360° cyber security game, interesting and maybe need to add to the literature review.

Logged into my new mailbox, there was an answer from the “Deepdotweb” administrator saying “ I will try asking on forums, no one I could think of will be helpful”

Attempted to login to “darknet forums”, the site appear to be down for an unknown reason.

Found a site called “Dark Web news” that list 3000 Dark Web links, all apparently tested.

From the above I went to “hacker place” using an onion address. There is a long list of magazines and books for example “the basics of cyber warfare syngress 2012”

Also tried using the search engine "not evil", similar to duck duck go the more basic looking. Also tried "torch" and "ahmia” search engines - The latter was much more usable than the former. Convert to the anarchist forum and from there to Kick-Ass marketplace and forum. To register here I needed my PGP public key, time to read up on PGP!

Began looking at 2017 cyber/hacker conferences, checkout rant/contacts page for Manchester details.

30th December 2016

Interesting opinion piece in the Guardian by someone called Martin Belam. He believes that we are living through in the first world cyberwar but it just hasn't been called that yet. As a historian he's interested in when wars start and end, with the proviso that you can't see the exact moment at the time.

Again to the dark web. There is an abundance of carding forums; I had to look this up but it's where you can buy and sell stolen credit card details – the newer the theft the more the card details were worth. Those that were more than 48 hours old were available for nominal fees.

8th January 2017

Email to Guardian journalist with regards to a Russian hacker they've been interviewing. I've asked if I can be put in contact with them.

13th January 2017

Another big Cyber attack – this time at Lloyds Bank. 20m accounts were hacked or compromised. DDoS again.

19th January 2017

Sent a follow-up mail to SLJ at KPMG to see if he can help with contacts with hackers.

Also sent a chasing email to one of my supervisors re-his contacts at the Greater Manchester police have been in contact with him before.

18th January 2017

Arrange the meeting with a friend of an old work colleague to see what contact he has. Going to meet him in Manchester on 25 January.

25th January 2017

Had an informal meeting with a hacker – see separate entry “Discussion with hacker”.

3rd February 2017

Logged into my Dark Web mailbox, no new mail despite sending out lots of emails the previous week.

Attempted to login to “darknet forums”, the site appears still to be down.

20th February 2017

Regular visits to the forums for hacking/carding sites was usually fruitless. The sites were often down/missing (sometimes with FBI statements as to why they had been closed down), and the forms were often sparsely populated. A large number of the posts on these forums were simply adverts to buy credit card details. There were specific request from ‘newbies’ as to how to ‘card’ successfully. Occasionally, there would be a long, courteous and detailed response to these which was surprising. Posting messages requesting to interview hackers was a dispiriting process. They were never sensibly replied to; a few responses of the ‘no chance’ variety or obviously false promises. One exchange led to a comment back of “don’t trust nobody, feds are everywhere”.

10th April 2017

Good piece in The Register by Mark Pesce – will the costs of sharing (i.e. the basis of the Internet) outweigh the benefits? If Cyber attacks become too great then it could be the end of the Internet as we know it.

15th April 2017

Traversing the dark web using TOR/TAILS gave an insight into the community. It must be a slow and frustrating experience with the lag from TOR. Often the sites were missing or closed down, broken links abounded and the various wikis were often out of date – therefore, more broken links. This must be par for the course in the dark web. Bitcoins (BTC) appear to be the preferred currency and as a result there were a lots of currency converter sites; there are also currency sites purporting to be for money laundering purposes.

24th April 2017

Attempting to find hacktivist sites lead to a lot of misdirection; however, some were discovered and appeared to be functioning. A few of them listed possible targets for hacking, asking the readers to choose where to hack next based on the view of the community. Some of the more genuine sites gave coded instructions, directing potential hacktivists to other websites where they would gather; but to do what? Plot and plan or to launch an attack? This remained unanswered.

7th May 2017

Emmanuel Macron was targeted by a “massive and coordinated” hacking attack, hours before the voters went to the polls – loads of emails and documents released.

13th May 2017

A massive new Cyberattack - Wannacry ransomware has burst onto the world's computers. The attacks are becoming more and more public, which I guess is good for raising awareness.

28th May 2017

Michael Chertoff, former Homeland Security chap, suggests Wannacry ransomware originated from North Korea as a means for the state to make money; they’re that hard up!

From February 2017 to May 2017

Repeated attempts to contact hackers via the Dark Web proved fruitless; however, the industry contacts were yielding good results and I decided to focus on these fully.

28th June 2017

The NotPetya malware attack (27th June) maybe a test of a future Cyber weapon; it wasn't designed to make money but to damage IT systems – interesting.

23rd August 2017

Report in The Guardian on how dissidents and neo-Nazis alike are utilising TOR to escape detection, calling it a "controversial technology that provides protection for dissidents in oppressive regimes at the same time as harbouring Nazis, illicit marketplaces and child abuse rings". It highlights the difficulty of attempting to regulate it.