
Article:
Bellaby, R. (2016) Justifying Cyber-Intelligence? Journal of Military Ethics, 15 (4). pp. 299-319. ISSN 1502-7570

https://doi.org/10.1080/15027570.2017.1284463

Justifying Cyber-Intelligence?

Introduction

Edward Forster, in his short story The Machine Stops, describes a world where almost every activity is aided in some way by a vast computerised system known simply as The Machine: 'The Machine feeds us and clothes us and houses us; through it we speak to one another, through it we see one another, in it we have our being; The Machine is omnipotent, eternal; blessed is The Machine' (1909, p.26). Forster's depiction of a world where every activity is influenced, mediated, aided and even controlled by a massive computer system offers a powerful reflection on how intermingled our everyday lives have become with technology. Over the last two decades, the role and pervasiveness of computers and the Internet has exploded in ways unimagined. Communications, data, pictures, music, activities, business, and personal information, are all being increasingly digitised and transferred along information highways. The result has been the birth of the modern information nation, dramatically changing the way people, organisations and states carry out their everyday lives and activities.

This computer revolution, however, comes with its own costs. While it offers ever more efficient and effective means of facilitating every day and long term needs it also offers the same advantages to those who seek to cause others harm. For example, criminals and terrorists are now able to communicate, organise and carry out their aims with greater stealth, reach and efficiency, while states are able to engage in cyber-espionage and attack with increased anonymity and deniability. The Stuxnet computer worm, for example, found in computers at Iran's Natanz nuclear site landed a significant blow on any Iranian nuclear ambitions without anyone lifting a sword (Sanger, 2012; Farwell and Rohozinski, 2011, pp.24-25). Similarly, cyber-attacks on civilian structures, such as the case in Estonia in 2007, which brought down the websites of its banks, governmental agencies and media outlets, demonstrated the vulnerability of such structures as well as their increased importance in the modern world (BBC, 2007; Traynor 2007; Landler and Markoff, 2007; Blomfield, 2007). Equally important is the threat of cyber-espionage. 'Titan Rain', for example, stole data from NASA's Mars Reconnaissance Orbiter and Air Force flight planning software as well as data from US government systems and defence contractors (Posner, 2010; Sommer and Brown, 2011); 'Operation Aurora' consisted of numerous attacks on high-tech, security and defence contractor companies (Cha and Nakashima, 2010); and Operation 'Ghostnet' accessed the

foreign affairs ministries of Iran, Indonesia, Philippines and the embassies of India, South Korea, Indonesia, Thailand, Taiwan as well as computers at NATO headquarters (Information Warfare Monitor , 2009).

The surge in both quantity and variety of cyber-threats has placed significant pressure on the state, and more importantly on its intelligence community, to adapt or leave itself open to attack. This pressure has caused many in both political and intelligence circles to argue for ever greater amounts information in order to catch potential threats before they become real, and in a world dominated by the power of the Internet this means increased access to cyberspace and the vast quantities of information that can be found there (Pace, 2013). By collecting all the digital information people create the intelligence community argues that it is not only able to detail what people have done or are currently doing but can also predict what their next move might be. The aim: to predict and prevent the next large attack. Moreover, this objective is an ethical one. The state and its institutions are tasked with the duty to protect both the individual and political community from harm. For example, Michael Walzer argues that the historical willingness to defend one's state is an outgrowth of the natural attachment to our political community; that our shared experiences and cooperative activity seen in the political community shape our life and is ethically valuable to us as a result. People both need and value the state as their main protector (2000, p.53; Anscombe, 1970, p.43). The intelligence community therefore plays an important role in this task by detecting, locating and preventing potential threats, including threats from international terrorist networks and sub-state actors, domestic crime and social unrest, state aggression, foreign espionage and international instability.

However, the backlash from both the public and politicians that followed Edward Snowden's revelations regarding cyber-intelligence showed that such activities were not without controversy. Reports that the American National Security Agency (NSA) has been collecting and storing some two billion 'record events' per day since 2010 (Lucas, 2014, p.31) were met with significant concern that the intelligence community no longer reflected the ethical or social principles of society (Horwitz and Branigin, 2013; Traynor, 2013). Indeed, for the first time in a decade Americans are concerned that government anti-terrorism policies have gone too far in restricting civil liberties (Greenwald and MacAskill, 2013; Horowitz and Branigin 2013) while in the UK senior politicians have suggested that without greater scrutiny the intelligence services will lose the trust of the British public (Hopkins and Taylor, 2013).

This leaves the debate stuck between the important, ethical role that intelligence can play and the potential for its unrestrained use to cause undue harm. This paper will resolve this by first giving greater detail to cyber-intelligence practices, highlighting the different levels of harm that the various intelligence operations can cause. However, the point of this paper is not that cyber-intelligence should be banned outright, but that it can be justified given the necessary circumstances. Therefore, the paper will develop a specialised set of Just Cyber-Intelligence Principles, built on the just war tradition, to outline if and when such activities are justified.

Cyber-Intelligence: Collection and Analysis

As a process intelligence consists of a 'cycle' whereby information is acquired, converted into its finished product and made available to policy makers. At each stage of this intelligence-cycle, cyberspace has increased in prominence, from using it as a means to collect information by monitoring online habits, to analysing large datasets, to creating predictive models of behaviour, as well as using cyberspace to launch attacks on other computerised systems, such as was the case with Stuxnet.[1] As such, cyber-intelligence is an umbrella term that covers a range of different practices used by intelligence actors through the medium of cyberspace. This paper, however, will focus on collection and analysis, examining how the intelligence community uses cyberspace to collect communication content by accessing emails or voice-calls, as well as the move towards the collection and analysis of meta-data through data-mining and dataveillance.[2] This former cyber-intelligence tactic of data-mining involves collecting an individual's personal information from various data sources – personal identity, financial accounts, medical records, fingerprints or DNA profiles for example – in order to develop a personalised 'digital dossier' (Solove, 2004, p.1). In comparison, 'dataveillance' involves monitoring the 'electronic footprint' inevitably left behind when an individual interacts with a computerised system. Websites, for example, track a customer's web-surfing secretly when he accesses it, including data about the ISP, computer hardware and software, the website he linked in from and exactly what parts of the website he explored and for how long (Solove, 2004, p.23). This data can be collected in a similar way to existing the communication surveillance methods, recording all individuals who visit a particular website, referred to here as a 'server log' for ease as it focuses on the website side of events, or a detailed list of all the websites an individual visits, referred to as 'personal web logs' as this examines activities carried out form the individual's perspective. Moreover, many real world actions also create digital footprints, recording time, place and

action. Money, travel, official documentation, shopping and all forms of communication are but a few examples where even in the real world one is likely to have one's activities logged in some computerised system. This makes avoiding having our activities recorded in our everyday life increasingly difficult in developed societies.

By collecting this type of information from enough people and cross-referencing it into a searchable database it is possible to understand what an individual is both doing and intending to do and determine if this is a threat.

Cyber-Harm

The particular problem that cyber-intelligence raises is that recent developments in both technology and how people use that technology means that there is no roadmap for the intelligence community as to what is expected of them. The semi-public nature of cyberspace along with the difficulty of ascribing provenance once the information leaves the individual means that the very idea of 'privacy' on the Internet is not clear. Changes in social interaction in cyberspace have resulted in an increasingly confused understanding of 'online spaces'. For example, chat rooms, social media forums like Facebook and YouTube, and even web browsing distort established public/private distinctions by representing 'private-social' spheres, acting to publically display and disseminate personal information to be seen by an increasingly large and varied audience. However, it is unclear how much people intend to waive their privacy or control and allow state access to this information. Furthermore, the collection of meta-data detailing online habits can betray personal insights into the individual, including political inclinations, state of health, sexuality, religious sentiments and a huge range of other personal characteristics, preoccupations and individual interests. Importantly, while this information does not necessarily have to be unique and can be pretty superficial – from online chatting, looking at pictures and videos, to searching the minutiae of our everyday lives – but can reveal what the individual might consider his personal life. Indeed, the UK Joint Committee on the Draft Communications Data Bill noted that, 'web logs are a type of communications data from which significant inferences could be drawn about a person's interests and, perhaps, activities' and as a result accessing web logs in this way is likely to be 'at the more intrusive end of the communications data spectrum' (Joint Committee, 2013, §82 p.28). Furthermore, given that a lot of online activity is done within the protection of the home or through a personal computerised system of some form it can feel like a private communication – much like a phone call between yourself and the website – meaning that the individual is likely to carry out his intimate life there.

When examining privacy in cyberspace, therefore, it is important to not think of it as a binary, whole one minute and destroyed the next. Rather, that different situations carry with them different expectations of privacy, established through social understandings or some performance used to denote a specific activity as possessing a particular level of privacy. For example, when an individual withdraws himself from society or actively shuts others out in some way – locking something in a box or being secretive about something – this can indicate a high level of expected privacy. Or, if it can be argued that those actions are widely considered to be personal or intimate (though not necessarily unique) there can be a higher expectation of protected privacy. On the flipside, however, is that an individual can, partially or fully, waive their privacy through their own (in)action. For example, if someone makes it hard for another to not overhear them or acts in such a way as to indicate a lack of care for their privacy then they waive some of the normal protections.

The impact on privacy is not all, however, as the very act of monitoring people in their daily lives can represent a threat to their autonomy. The argument is that an individual will act differently if he thinks he is being watched as compared to when he thinks he is alone, conforming to the standards of what he thinks is expected of him by his watchers. He will imagine the watcher judging him and will alter his behaviour as a result. The fear, therefore, is that cyber-intelligence's ability to transcend space and time limitations brings the asymmetric gaze of the panopticon to non-institutionalised spaces and can detrimentally affect an individual's autonomy as a result. (Foucault, 1979, pp.202-203; McCahill, 1998, pp. 41-65).

Moreover, how this data is used can also cause further problems. There are those that believe that through the use of facts like race, religion, gender and class it is possible to create predictive models. They argue that because of the relatively high correlation between personal attributes and behaviour it is a fairly cheap and easy way of understanding and predicting how an individual or a group will act (Hausman and McPhereson, 1996). By collecting information en masse the hope is one of 'discovering meaningful patterns in the data' (Gandy, 2003, p.28) in order to build profiles of both people and events to create a veritable 'crystal ball' which can be used to understand the individual and predict his intentions (Keefe, 2005, p.99).

Levels of Harm

Importantly, however, it is possible to consider these different cyber-intelligence activities as causing different levels of harm depending on the type of privacy they violate or the degree to

which they affect the individual's autonomy. Both server logs and personal web logs violate an individual's privacy, though it can be argued that they do so to different extents. That is, collecting personal web logs is a greater violation of an individual's privacy than a looking at server logs because they collect more personal information of a greater quantity and quality. Server web logs will only really give a particular snapshot of what a group of individuals were looking at, the one 'dangerous' website visited is examined to see who visited it and so this singular bit of information would only be linked to the individual and nothing more at this stage. What this means is that it is not very revealing in regards to any particular individual, his identity and his personal activity. It is essentially breadth over depth. In comparison a personal web logs give a full detailed web browsing history for an individual making it more likely to reveal his intimate life and what he chooses to do when he thinks he is in private. Depth over breadth. It can be argued that the individual can expect a greater level of control over this information as it is reflecting a more intimate part of his life.

Moreover, both of these types of searches can be done to different extents. Data collection on personal conditions or sexual relations could be considered more private than an individual's address, telephone numbers and email accounts, but that this information is more private than superficial information that the individuals willingly transmits such as gender, age, height, weight and hair colour. Therefore, for data-mining the level of intrusion, and therefore harm, can be tied into the types of databases it accesses. Equally, dataveillance can vary according to whether it collects data on the general website the individual is visiting – before the 'forward slash' (/) in the URL – or has a precise reading on what actual content the individual is looking at – after the 'forward slash' (/).[3] Similarly, when collecting digital data on activities carried out in the real world, identification and location can be considered less intimate than information that details activities carried out.

This means it is possible to delineate different levels of harm caused by cyber-intelligence according to how intrusive the action is. From a superficial identification of an IP address at one end, moving through to a real identification, to superficial data-mining and dataveillance searches, to more intensive data searches, to accessing email and voice-call content at the other end. In response to these different levels, therefore, the justifying principles must be equally nuanced, where there is a correlation between the harm caused and the surrounding circumstances used to justify it. Quite simply, as the level of harm goes up so too should the Just Cyber-Intelligence Principles described below.

Just Cyber-Intelligence?

As an ethical framework the just war tradition was designed to grapple with the notion that there are some acts, such as killing someone, that 'in the normal context are gravely wrong', while understanding that in certain circumstances, war for example, these same acts cannot totally be dismissed, but play an important role in protecting both the political community and its people from a range of threats (Quinlan, 2007, p.2). The state must be able to act to protect those whose duty it is to care for. However, this does not allow unrestrained action and, as such, there is still a need to limit the damage that war can cause. As a result, what evolved over the centuries was a set of principles designed to govern and limit the activity of war and the harm it can cause, while maintaining the broader context of the duty of public authorities to be able to use violence for the protection of one's state or that of international peace and stability (Turner, 1981, p.xxi).

The just war tradition is, therefore, well versed in reconciling the tension that is born from balancing the needs of the political community with the harm this can cause. That is, intelligence can also involve practices that 'unavoidably entail doing some things that are plainly and seriously contrary to the moral rules accepted as governing most human activity' (Quinlan, 2007, p.2) yet can be justified as an important means of protecting both people and the political community. It can be argued, therefore, that the ethical principles that underpin the just war tradition represent the most appropriate starting-point in designing an ethical cyber-intelligence framework. The principles developed here demand both a limitation on the harm that is caused by intelligence collection, while also outlining exactly when that harm is justified.

One importance difference, however, between war and intelligence is that in the former there is a sharp distinction between the justice of going to war, jus ad bellum, and the justice of actions within war, jus in bello. This distinction does not work when we consider cyber-intelligence collection. There is not the same division between evaluating and sanctioning the general act of intelligence collection and the carrying out of the variety of acts under this authorisation that is seen with war. There is no 'time of war / time of peace' distinction for intelligence, but rather operations are running continuously. So, with intelligence, the evaluation must be done continuously, whereby each operation must fulfil all the just cyber-intelligence principles described below, with an operation being sanctioned according to who is being targeted, taking into account whether there is a specific just cause

for the operation, ensuring that there is a right intention, and that the method chosen is proportionate the proposed gains.

Just Cause

The just war principle of 'just cause' is often considered to be one of its most important as it is this that gives the main justification for initiating the war (Orend, 2013, p.49). That is, 'those who are attacked must be attacked because they deserve it on account of some fault' (Aquinas, 2004, p.214). The current accepted manifestation of a just cause is acting in self-defence or the defence of others. This justification is often drawn from either the extrapolation of the 'domestic analogy' - the ontological justification for wars of self-defence whereby ethical frameworks designed for everyday activities are extrapolated 'up' on to the state - or from the argument that the political community represents an ethical good in peoples' lives and so needs protecting. The equivalent just cause for cyber-intelligence is similar in that it relies on a notion of self-defence, whereby the protection of the political community is achieved through the detection and prevention of threats; essentially a pre-emptive, or even preventive, act of self-defence.[4] Importantly, as Walzer points out, we can imagine a spectrum of anticipation, with an imminent but anticipatory pre-emptive act of self-defence at one end and a preventive act designed to forestall a distant danger at the other end (2000, p.75). The significant point is that depending on where the threat falls on this spectrum the level of harm caused that can be justified can change. That is, threats that are larger or more imminent represent a just cause for a greater level of harm than those threats that are distant or are only minimally threatening, though these distant threats might be a just cause for a low-level privacy violation. For cyber-intelligence, by examining the threatening nature of the website itself we can determine if there is just cause to, first, identify, locate or arrest those who made the website, and, second, identify, locate or arrest those who have visited it.

Right Intention

It is thought by just war theorists that it is not enough to have an objective just cause for war, but there must also be a proper subjective right intention. That is, the intention behind an act alters the moral quality of an act and, as such, represents an important part of how an act is judged (Thomson, 1986, p.101-102; Scanlon and Daney, 2000). The reasoning behind this is that it is very possible for 'war to be declared by legitimate authority and have just cause, yet nonetheless be made unlawful through a wicked intention' (Aquinas, 2002, p.214). The aims of the war must be consistent with the just cause invoked to justify the war; acting in self-

defence cannot then be used in order to annihilate or subjugate another. This right intention is then determined by examining the actions deployed: if it is a war of self-defence the tactics employed must not be one of domination. In addition, the principle of right intention plays an important role in the doctrine of double effect, whereby actions with foreseen collateral damage can be permitted when the harm is not directly intended, nor is a means to achieving the good and proportionate end (Mangan, 1949, p.43).

By drawing on this logic it can be argued that in order for intelligence collection to be morally permissible the intelligence collection activity should be used for the stated purpose and not other political, economic, or social objectives. The intention should be to deal with the threat posed directly rather than using the presence of a threat as an excuse for host of other operations. The means used, who is targeted, and how much harm is allowed, should all flow from the intended purpose of dealing with this particular threat.

The principle of right intention, therefore, limits the type of information accessed, how it is stored and how it is shared. Firstly, there must be effort to only collect that information which is directly pertinent to the case at hand, which means using a collection method and picking a target most suited to gaining that intelligence. So in practice, when an application is made, through a warrant for example, the terms should reflect the just cause, and in turn the type of search carried out should reflect the intent behind that just cause.[5] The investigating officer may only search 'places which might reasonably be suspected of containing the specified offending articles' (Stone, 2005, p.171). If the officer was to search places outside the warrant, for example, then he is acting with an ulterior motive to the just cause and is therefore not working with the right intention (Feldman, 1986, p.171). Any information that is incidental to this threat and is not in itself threatening must be stopped and discarded. This is in-line with current law enforcement practices that dictate that when tapping a suspect's phone, the call is marked either as pertinent or non-pertinent within the first 30 seconds and monitored accordingly. However, anything thrown-up incidental to the specified threat but is still inline with search parameters and is threatening in some other way may be seized since, even though the items found were not specified at the beginning, the type of search carried out itself was still in-line with the original intention. Just because the outcome does not match the original intention does not alter the fact that the officer was working with the correct intention in the first place. This would be analogous to finding illegal goods incidentally while performing a legal search. However, what is not permissible is to use a just cause such as tax fraud to justify the collection and retention of DNA, as this

type of information is unrelated and is not reflecting the original just cause, clearly outside what should be the correct intention.

Furthermore, information should only be kept with a direct reason, meaning that without specified reasons retention times should be kept to a minimum.[6] If information is collected, the justification for keeping that information must reflect the intention associated with the threat that supports the just cause. If a case is examined and the suspicion on which the search was based is not made real then the just cause for keeping the information withers. Any further retention of information comes with a different intention, with some broader aim of collecting people's information for the sake of it, regardless of the proposed threat.

Just Intelligence and Last Resort – Temporal Proportionality

In the just war tradition the principle of last resort is an attempt to allow those more benign means of responding to a crisis, such as diplomacy or economic pressure, a chance to resolve the issue before the resort to organised violence is permitted. If possible more harmful acts should therefore be avoided. However, Robert Phillips warns that, 'it is a mistake to suppose that 'last' necessarily designates the final move in a chronological series of actions' (Philips, 1984, p.14). If this were the case then force would never be legitimised as one could always negotiate further. Instead, what it demands is that actors 'carefully evaluate all the different strategies that might bring about the desired end, selecting force as it appears to be the only feasible strategy for securing those ends' (Bellemy, 2006, p.123).

What this means for cyber-intelligence is that any operation should use the least harmful activity first thus giving the opportunity for more harmful activities to be avoided. While there are no rigid steps that must be worked through, it does require that some of the more harmful actions are not resorted to out of ease, expediency or preference.

Moreover, by understanding the principle of last resort in this way it resolves an important difference between intelligence and war. Namely, the temporal paradox justifying cyber-intelligence poses. That is, given that it is the duty of intelligence agencies to provide the very information that is then used to establish whether the action is justified, it is difficult to make these initial ethical calculation with no information provided. However, by imagining justification as a spectrum one can consider those actions that cause minimal harm to those targeted as only needing a suspicion of a threat to act as a just cause; whereas more intrusive activities must have a greater level of evidence to justify the action, solid information on a large threat for example. This spectrum is itself nothing new. Various legal

systems mark out levels of evidence, or 'burdens of proof', which are required when assessing whether certain actions are permissible or not. Legal canons mark a distinction between a reasonable suspicion, a probable cause, a balance of probabilities, clear evidence, and beyond any reasonable doubt, whereby depending on the circumstances the level of proof required changes. For example, reasonable suspicion is a low standard of proof often required to determine whether a brief investigative stop or search by a police officer or any government agent is warranted. For anything that is more 'intrusive', to detain someone for example, a higher burden of proof must be provided, for instance a probable cause. These different levels of probability provide, what Polyvious Polyviou calls, the 'best compromise' between two often opposing interests, 'the intrusions upon the individual and the security of the state' (Polyviou, 1982, p.97). This notion is easily compatible with intelligence collection. Intelligence is essentially a calculation of probabilities and possibilities about activities that it is not meant to know about. Intelligence by its very nature is engaged with uncertainties: 'intelligence rarely tells you all you want to know. Often difficult decisions need to be made on the basis of intelligence which is fragmentary and difficult to interpret' (Parkinson and Walker, 2009, p.95). Intelligence operatives must engage with what evidence they have and determine what action is best given the range of possibilities. If the information collected proves fruitful then it can be used as further justification of those activities that are increasingly intrusive.

Proportionality

One can argue that in order for the cyber-intelligence to be just the level of harm that one perceives to be caused by the collection should be outweighed by the perceived gains: 'is the likely impact of the proposed intelligence gathering operation, taking account of the methods to be used, in proportion to the seriousness of the business at hand in terms of the harm it seeks to prevent?' (Omand, 2007, p.162). However, it is only those goods that are related to the just cause that should be counted as a positive, while almost all damages caused should be included as a negative. Thomas Hurka asks us to imagine a situation where 'our nation has a just cause for war but is also in economic recession, and that fighting the war would lift both our and the world economies out of this recession' (Hurka, 2005, p.40). Although the economic benefits here are very real, these cannot be counted towards the proportionality calculation. We cannot justify killing in terms of the economic gains that it might produce. In contrast to this, however, while only certain goods may be counted in favour of acting, all damages or harms, must be counted. Returning to Hurka's example, while the boost to the

economy cannot be counted as a relevant good, the fact that it might hurt the economy could be counted as a negative.

As such, in order to satisfy the principle of proportionality there must be a calculation of the overall damage caused, not just to the individual targeted or from this specific operations, but other, wider social harms caused as well. For example, damage to social cohesion, degradation of trust between social groups, aggregation of minor harms into larger harms and the potential for radicalisation should all be taken into account.

Discrimination

The requirement that an attack must discriminate between legitimate and illegitimate targets is one of the most stridently codified just war rules and is reflected in the international law of war as such (Geneva 1949; 1977, Article 51 §2). Soldiers charged with the deployment of force and violence cannot do so indiscriminately. They have an obligation to exert a particular effort to discriminate between legitimate and illegitimate targets. That is, the target has to have 'something about them' to justify being targeted (Nagel, 1979, p.124). Just as soldiers are legitimate targets because they are a threat or because they have acted in a way so as to waive protective rights, arguably any individual can act in a way so as to forfeit their protective rights. Moreover, revisionist just war theorists make the case that this 'something' does not necessarily have to be based on how directly threatening the individual is, nor should we rely on a simple distinction between combatants and non-combatants. Jeff McMahan argues that instead of defining innocence in terms of guilt, innocence should be the absence of moral responsibility (McMahan, 2009, p.32-34). That, 'civilians can be related to unjust combatants [...]. They can be instigators of unjust wars, or aiders and abettors who share responsibility for unjust acts of war perpetrated by unjust combatants' (McMahan, 2009, p.208). Discrimination conceived in this way rests on the degree of responsibility (and resulting liability) of the individual. Individuals can become morally responsible for a war when they intentionally work to stimulate popular support (publications, public speeches, lobbying, etc.) or support the fighting unintentionally through their employment (McMahan, 2009, p.214-15). Gerhard Øverland makes a similar argument that 'non-threatening people may or may not be morally responsible for the existence of threats and aggressors', arguing that a person can give rise to the materialisation of a threat and so are, through their contribution, a legitimate target (2005, p.349). Importantly, while McMahan argues that 'most unjust civilians are at most responsible to a low degree for their country's unjust war'

and so are 'almost never liable to intentional military attack', this does not preclude other, less harmful actions, such as intelligence (2009, p.231). Strawser, for example, argues that depending on the level of liability the individual represents the response accorded to them can change: 'distinctions could range from 1st, 2nd and 3rd- degree combatants and the like (or more, as needed) and similar degrees for noncombatants' where 'those labeled as simply 'combatants' would instead be considered some lesser-degreed type of combatants with different correlative ROE [Rules of Engagement]. Similarly, the same would be done for those traditionally labeled as simply 'noncombatants'' (2013, p.79-80).

Depending on what level of responsibility or culpability to the threat the individual represents the type of activity to which they are a legitimate target changes. For cyber-intelligence, by holding a particular job, being in possession of important information, being a member of a state's infrastructure, accessing a particular webpage, logistical or contributing support to the threat, are all examples of how individuals contribute to varying degrees to the threat and make themselves legitimate targets to an equal level.

Cases: Targeted Cyber-Intelligence Vs. En Masse Collection

The development of the Internet as one the biggest mediums through which individuals can access and disseminate information means that anyone who has an Internet connection has access to a truly massive (and potentially dangerous) amount of information. The intelligence community is therefore undoubtedly keen to locate both those websites that hold and disseminate dangerous information as well as track those who seek to use that information to cause others harm. 'Targeted cyber-intelligence' involves focusing on a small set of individuals or websites, examining them to determine whether they represent a threat in themselves or if they will instigate, promote or facilitate dangerous activity by those who visit them. Important ethical questions therefore revolve around what website is targeted, who is investigated as a result and how in-depth the investigation becomes. Whereas 'en masse collection' gathers as much information as possible from all data sources, continually collecting and storing the information ready for later exploration and analysis. This introduces important questions regarding the type of information collected, how long it is retained and what role predictive models or profiles should play in the investigation.

Case 1: Dangerous Websites, Dangerous People

In the first case the type of websites targeted are those that are engaging in violent, harmful or destructive activities themselves. This might include, for example, websites being used to

organize, plan or carry out an act of terrorism or to recruit and train potential terrorists. It has become increasingly apparent that on the operational side of terrorism the Internet can play a pivotal role in communicating information to those concerned, either directly through web chats and emails or indirectly through hiding information in otherwise seemingly harmless stenography. Or equally powerful, as a tool to 'develop relationships with, and solicit support… as a means of clandestine recruitment' (Gerwehr and Daly, 2006, p.83; Denning, 2010). What this means is that the website itself represents a threat as a key facilitator of the end goal and can be used to link those individuals who make up that threat. So, as long as there is enough evidence to demonstrate that the website or web account is being used to plan and organise terrorist acts, there is a just cause to explore both those who created it and visit the site.

For proportionality, searches that have a targeted individual or website in mind, the harm caused is mostly localised to those few directly involved and given that there is often a clear benefit – including preventing a terrorist operation, fraud or sexual abuse – it is easy to determine if the harm is offset by the information gained.

Equally, with targeted searches there is the occasion to highlight, evaluate and determine whether those examined are legitimate targets. It is not too difficult to discern those individuals who manufacture, maintain or use the website to facilitate the threat. However, in order for the visitors to be linked to the conspiracy they must be connected through one overt act to show complicity in the threat.[7] Complicity might include a relationship that provides either intellectual or direct logistical support, often demonstrated by the transference of money and/or goods, mutual communication on a member's only password-protected site, or other actions that reflect the intent to cause others harm. This would also include knowing about the threat and not acting to prevent it. Luckily, determining contributors for these types of websites can be relatively easy. Their closed nature means that participation can be demonstrated through signing up and using passwords to gain access, contributing to the organisation of the threat, or sanctioning or encouraging an operation through dialogue. Each of these requires an exerted effort by the visitor, marking their contributing to part of the threat.

A recent case from France, Public Prosecutor v. Hicheur, illustrated how different forms of online technology can be used to facilitate the preparation of acts of terrorism by disseminating information and plans through password-protected websites.[8] Adlène Hicheur, a nuclear physicists, had translated, encrypted, compressed and password-protected pro-jihadist materials, including documents and videos, which he then uploaded and circulated

via the Internet; distributed the encryption software 'Mujahedeen Secrets' to facilitate covert Internet communications; conspired with an AQIM member to organize and coordinate pro-jihadist activities, including, but not limited to, providing financial support to the jihadist cause, disseminating pro-jihadist information and supporting the creation of an operational unit in Europe, and in particular in France, to potentially prepare terrorist attacks; acted as moderator on the pro-jihadist Ribaat website; and took concrete steps to provide financial support to AQIM, including through the attempted use of PayPal and other virtual payment systems (United Nations Office on Drugs and Crime, 2012, p.9). These actions mark all those involved in the digital interaction as clear conspirators in the larger plan, complicit in the threat and so there is a just cause to use intrusive cyber-intelligence activities to locate and detain those involved.

For the intelligence operative this means they are justified in carrying out in-depth data-mining and dataveillance operations, accessing both server web logs and personal web logs to locate those involved digitally as well as in the real world. This can also include using some of the more intrusive forms of information collection such as accessing their email and voice-call content and accessing personal databases – medical, financial and tracking them through their real world electronic footprint. What is clear is that if these actions were performed in the real world – engagement, knowledge, logistical or contributory support, training or planning of a terrorist operation for example – these individuals would represent a legitimate target.

Case 2: Promoting and Listening to Violent Speech

A different case might be where the website is seen to be dangerous or threating, but does not necessarily mean that those who visit it are participating in the threat itself. For instance, websites that advocate, foster or encourage the use of violence. In the case of terrorism this means messages designed to incite violent activity (United Nations Office on Drugs and Crime, 2012, p.6). However, in order to protect the important freedom of expression while still defending the wider political community, a distinction must be made between propaganda and materials intended to incite acts of terrorism, where the latter has the intent to directly promote violence through the development and realisation of some terrorist plot (International Covenant on Civil and Political Rights, General Assembly Resolution, 1979). For example, three Islamist extremists who were jailed for engaging in a 'cyber-jihad' where they 'promoted martyrdom and holy war through online forums and websites, including discussions about a plot by 45 doctors to explode a car bomb at an American naval base' with

the aim of inciting terrorism through the Internet (Woolcock, 2007). They were supporting and conveying a message of violence in order to encourage others to join and so the video itself represents a just cause to locate those who are behind it and its efforts. In this case, those who created the website have acted to contribute to the threat through their promoting, encouraging and sanctioning, and even possible recruitment, of the threat itself. This level of threat and involvement offers a just cause to locate the creators in the real world as well as some detailed cyber-investigation, including accessing emails, a search of other online activities and a search of personal data databases.

The difference between this and last case is that those who visit the website are not necessarily engaging in the threatening act. This means that there is only a just cause for identification of the individual, keeping a record and flagging the individual as possibly dangerous for a determined amount of time, cross-referencing their details with other security databases, and a superficial check on their web activity. This superficial check means limiting the data collected to the overall title of the website, so anything before the first forward-slash (/). Without any further evidence they cannot have their detailed weblogs seized or their lives interfered with, as this causes wider harms for which there is no just cause. For example, those visiting the cyber-jihad YouTube sites cannot be detained and questioned in the real world. This is because while it can be argued that visiting threatening websites represents the possibility of them becoming threatening, their presence is not in itself enough to contribute to the threat sufficiently, and is also only a suspicion rather than being an actual threat. If, from the other online searches, it turns out they have being promoting violence themselves or contributing to a threat elsewhere, then they can be detained; if not then they must be left alone.

Case 3: Dangerous Information and Curiosity

A third case, similar to the previous but with important differences, is a site that has information which itself is not problematic, though has the potential to being used in a dangerous way. For example, a webpage detailing the mechanics behind making a bomb. In itself the webpage is not advocating harm though when read and used by someone with ill intent has the potential to be very dangerous. In this situation the webpage itself does not represent a direct threat. This means that those who maintain the website can be identified, but if it appears that they are unthreatening and there is an understandable reason for having the information (a chemistry teacher for example) the record should be deleted. They cannot be tracked down in real life, detained or have their personal information stores examined

without further evidence that they wish to use this information for harm or are encouraging others to use this information to cause others harm. The website itself can be monitored and non-identifying information (IP addresses for example) can be stored for a short time and cross-referenced to determine if they are visiting any other web pages or distributing the information, which might indicate an increased level of threat. If no further evidence comes to light then the data must be deleted.

However, those who visit the website should not be directly identified nor are they legitimate targets for intrusive actions. Curiosity in information is not a sufficient just cause. A notable example is the Masters student researching terrorist tactics who was arrested and detained for six days after Nottingham University informed police about the al-Qaida-related material he downloaded (Curtis and Hodgson, 2013). The data itself was not harmful nor was it likely to be harmful when visited by those with benign intent. There was also a reasonable explanation for the information collection. There should have been no identification of the individual made, nor should the student have been detained. Therefore, unless there is some communication that contains information specifying that the material is shared for the furtherance of a terrorist purpose, websites such as these that are simply informative.

Case 4: En Masse Data Collection

In comparison to the above cases that target small groups of people or a selection of websites, using en masse collection methods to access and search large databases such as those held by Google or ISPs and using pattern-based analysis to locate potential threats does not and could not have a just cause. Due to its en masse and ubiquitous nature, the searches are carried out regardless of any particular threat present. Randomly searching information stores with the hope of finding a threat, means that for the majority of the time no specific threat exists. Even if the intelligence agency only searched particular ‘dangerous’ terms, the threatening nature of the terms is too ephemeral, indistinct and open to mistake to act as a sufficient just cause for the harm it causes. What this shows is that, importantly, the general threat of terrorism, the so-called War on Terror for example, is too indistinct to offer any specific just cause for an operation; there must be a known threat of some form to justify the use of such cyber practices.

Similarly, proportionality becomes of increased importance when examining en masse collection as it is at this stage that wider or cumulative harms are included in the ethical calculation. It can be argued that simply having one’s information on a database is not necessarily harmful. No specific individual is actually, directly examined. The information

exists in some database far away. Moreover, when the information is examined it is by some computerised system, rather than a human.

However, this position is problematic. It was argued earlier that accessing personal web logs is more harmful than accessing server logs because the former gave a more detailed in-depth look into an individual's personal life, while the latter is a shallow look but for more individuals. This argument, however, was in regards to targeted operations that only included a select number of targets. However the limits of the position are shown here in that even if the monitoring is superficial, when carried out over a large group of individuals – whether across all of society or in regards to a particular sub-set of society – the large scale can cause wider harms.

It is first disproportionate because of the aggregation problem. The interest the individual has in their privacy has an intrinsic value and damaging it can cause harm regardless of the repercussions.[9] That is, even if, on balance, the individual does not experience the harm in a 'tangible and material' way, he is still harmed since his vital interests have been violated or wronged (Feinberg, 1984, p.35). So, while the individual might not necessarily 'feel' the direct impact of the violation, he indeed still harmed, even though it could be argued minimally. However, when such harms aggregate over large groups of people it can be argued that the level of harm is greater than the vague and unquantified gains of potentially finding a threat at some point.

In addition to violating our privacy these en masse collection methods can also represent a threat to our autonomy. Regardless of whether people are actually directly targeted, when dealing with such activities it is the perception that becomes important. En masse collection creates the implicit understanding that the Internet is being watched for security purposes and even though individuals are not likely to be singled out, the perception that they are being watched is still present and so acts as a force on their decision-making processes.

Importantly, this effect can be more readily felt by those sections of society that are highlighted as risk groups, suspect communities or consider themselves to be particularly marginalised. For example, while there was an official rhetoric by the Bush Administration during the 1990s and up to 9/11 terrorist attacks that profiling towards African-Americans and Hispanics was damaging and should be eliminated as a police practice, David Harris notes that after 9/11 attitudes in America have shifted in favour of ethic profiling in the context of searches against Arabs, Muslims and other Middle Easterners, showing how political and social trends can manifest so that certain groups are marked as 'at risk' and how

this superficial data still plays a role in the surveillance of individuals (2002, pp.36-37). These groups are more likely to feel the adverse affects of en masse surveillance, perceiving their social group as being separate them from the rest of society, marking them as deviant in some way. This can cause wider problems, as profiled individuals are 'necessarily labelled and henceforth seen as a member of a group the peculiar features of which are assumed to constitute personal characteristics' (Simitis, 1987, p.719). Individuals are treated according to the perception of the group rather than their actions, closing options to the individual or causing self-fulfilling prophecies as individuals act according to these expectations. (Merton, 1968, p.477). This only serves to erode the important bonds of trust within a society between the individual and the state, that social group and the state and even between different social groups. (Misztal, 1996, p.12; also see Hardin, 2002, p.3; Hertzberg, 1988, p.307-322). In sum, the fear is that these activities create feelings of marginalisation, exclusion and the potential for radicalisation (See Gandy, 2003; Kennedy, 1997; Lever, 2005; and Robinson, 2000).

In practice, the databases created end up over-representing particular social groups, heightening social fear of that group as well as reinforcing distorted criminal statistics. For example, a report by the Equalities and Human Right Commission (EHRC) notes that 'by our own calculation... in excess of 30% of all black males are on the National DNA Database (NDNAD), compared with only 10% white males and 10% Asian males' (Bennetto , 2009, p.5). The taint of suspicion lingers and can then lead to either inappropriate treatment later in life or can even spread like a stain across their associated, and overrepresented, group. The EHRC commented, 'We are concerned that the high proportion of black males recorded on the database is creating an impression that a single racial group represents an 'alien wedge' of criminality' (Bennetto , 2009, p.39-40). Such overrepresentation of a particular group can come with a loss of trust and confidence in the state apparatus that can lead to a decrease in the willingness of people in communities perceived as victimised to cooperate.

Such implicit and explicit forms of social control where the state strictly outlines what it thinks to be dangerous, unwanted or even deviant behaviour raises concerns regarding the state using its power to set social norms, meaning that those who fall outside those norms either alter their behaviour or face become increasingly marginalised. Arguably, broader harms means such as these activities become disproportional given the lack of direct or solid gains.

Importantly, however, the principle of intention plays an important part in the discussion on these wider harms at this stage. It can be argued that these wider harms are not

actually intended, and unfair comparisons to the Stasi – who used en masse collection methods in order to maintain control – overshadow that there is not the same intention to exert social control with NSA's cyber-intelligence collection methods. This argument is essentially one of double effect: that while the additional harms are foreseen they are not intended nor are they actually required for the good ends. However, again proportionality forms an important part of this discussion, in that while it might not be the direct intention to exert social control over the populous, it is foreseeably disproportionate.

Finally, with these en masse or pattern-based investigations they are essentially, by their very nature, unable to discriminate between legitimate and illegitimate targets and so are prohibited. They target everyone in the hope of finding a threat from within the masses, meaning that much of the time they are targeting individuals who have not done anything to mark themselves as a threat or acted in a way to make them a legitimate target.

Conclusion

The computer revolution is seemingly a sword with many edges. The benefit it offers people in terms of making everyday lives more efficient and enjoyable comes with the cost of the help it offers those who would seek to cause harm. More importantly, however, is that this paper has argued that it can be the very fight to stop these threats by the intelligence community that in turn can cause harm to the very people it is designed to protect. Moreover, this paper has also claimed that there is an ethical argument to be made that this harm can be justified in reference to the ethical good found within the political community. Privacy and autonomy represent vital interests in everyone's lives and so any interference should be robustly justified. The problem is that the Internet is constantly evolving, and with it so evolves the way that people use it to interact with each other. There are no real clear rules for what should be expected from the intelligence community because there are no clear understandings regarding what sort of space or even activity it represents. The aim of this paper was to establish that intelligence collection does indeed cause harm which needs limiting, but that sometimes this harm is necessary in order to protect those for whom a political community carries responsibility. It is only by understanding this dual quality found within cyber-intelligence and balancing the concerns in relation to each other that we can then develop an appropriate set of guidelines in order to prevent undue harm to both the individual and the rest of society.

Bibliography

Anscombe, Elizabeth (1970) 'War and Murder', in Richard A. Wasserstrom (ed.), War and Morality (Belmont, Calif.:Wadsworth).

Aquinas, Thomas (2002) 'From Summa Theologiae', in Chris Brown, Terry Nardin, and Nicholas Rengger, (eds.) International Relations in Political Thought. (Cambridge: Cambridge University Press) pp.213-220.

BBC News, (2007) 'Estonia hit by 'Moscow cyber war', BBC News, Available from: http://news.bbc.co.uk/1/hi/world/europe/6665145.stm [Accessed on 12 July 2012].

Bellamy, Alex (2006) Just Wars: From Cicero to Iraq (Cambridge; Malden, MA: Polity Press)

Bennetto, Jason (2009) Police and Racism: What Has Been Achieved 10 Years After the Stephen Lawrence Inquiry Report? (London: Equality and Human Rights Commission)

Cha, Eunjung and Nakashima, Ellen (2010) 'Google China Cyberattack Part of Vast Espionage Campaign, Experts Say', The Washington Post, 14th January, Available at: http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html [Accessed on 6th September 2012].

Curtis, Polly and Hodgson, Martin (2008) 'Student Researching al-Qaida Tactics Held for Six Days', The Guardian, 24th May, Available at http://www.theguardian.com/education/2008/may/24/highereducation.uk?guni=Article:in%20body%20 [Accessed 13th November 2013].

Denning, Dorothy (2010) 'Terror's Web: How the Internet is Transforming Terrorism' in Yvonne Jewkes and Majid Yar (eds.) Handbook of Internet Crime (Cullompton, Willan Publishing) pp.194-213.

Dipert, Randall (2013) 'Other-Than-Internet (OTI) Cyberwarefare: Challenges for Ethics, Law and Policy' Journal of Military Ethics 12(1), pp.34-53.

Eberle, Christopher (2013) 'Just War and Cyberwar' Journal of Military Ethics 12(1), pp.54-67.

Farwell, James and Rohozinski, Rafal (2011) 'Stuxnet and the Future of Cyber War' Survival: Global Politics and Strategy 53(1), pp.23-40.

Feinberg, Joel (1984) Moral Limits of the Criminal Law: Vol.1 Harm to Others (Oxford: Oxford University Press)

Feldman, David (1986) The Law Relating to Entry, Search and Seizure (London: Butterworths).

Forster, Edward (1909) The Machine Stops (DodoPress).

Foucault, Michel (1979) Discipline and Punish: The Birth of the Prison (Harmondsworth: Penguin).

Gandy, Oscar. (2003) 'Data Mining and Surveillance in the Post 9/11 Environment' in Kirstie Bell and Frank Webster (eds.) The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age (London; Sterling, VA:Pluto Press), pp.26-41.

Gerwehr, Scott and Daly, Sara (2006) 'Al-Qaida: Terrorist Selection and Recruitment' in David Kamien (ed.) The McGraw-Hill Homeland Security Handbook (New York, McGraw-Hill) pp.73-90

Greenwald, Glen and MacAskill, Ewen (2013) 'NSA Prism Program Taps in to user data of Apple, Google and Others', The Guardian, 7th June, Available at http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data [Accessed 8 June 2013].

Hardin, Russell (2002) Trust and Trustworthiness (New York: Russell Sage Foundation).

Harris, David (2002) 'Racial Profiling Revisited: 'Just Common Sense' in the Fight Against Terror?' Criminal Justice 17, pp.36-59.

Hausman, Daniel and McPhereson, Michael (1996) Economic Analysis and Moral Philosophy (Cambridge: Cambridge University Press).

Hertzberg, Lars (1988) 'On the Attitude of Trust' Inquiry 31(3), pp.307-322.

Hopkins, Nick and Taylor, Matthew (2013) 'David Blunkett Calls for Urgent Review of Laws Governing Security Services' The Guardian, 4th November, Available at http://www.theguardian.com/world/2013/nov/04/david-blunkett-review-laws-security-services [Accessed 13th February 2014].

Horwitz, Sari and Branigin, William (2013) 'Lawmakers of both parties voice doubts about NSA surveillance programs', The Washington Post, 17th July, Available at

http://www.washingtonpost.com/world/national-security/house-committee-holds-hearing-on-nsa-surveillance-programs/2013/07/17/ffc3056c-eee3-11e2-9008-61e94a7ea20d_story.html. [Accessed 17th July 2013].

Hurka, Thomas (2005) 'Proportionality in the Morality of War' Philosophy and Public Affairs 33(1), pp.34-66.

Information Warfare Monitor, (2009) Tracking Ghostnet: Investigating a Cyber Espionage Network, 5 Available from http://www.nartv.org/mirror/ghostnet.pdf [Accessed on 6 September 2012].

Jenkins, Ryan (2013) 'Is Stuxnet Physical? Does it Matter?' Journal of Military Ethics 12(1), pp.68-79.

Joint Committee (2013) 'Draft Communications Bill', Session 2012-13, Available at http://www.parliament.uk/draft-communications-bill/ [Accessed 9th Setember 2013]

Keefe, Patrick (2005) Chatter: Dispatches From The Secret World Of Global Eavesdropping (New York: Random House).

Kennedy, Randall (1997) Race Crime and the Law (New York: Patheon)

Landler, Mark and Markoff, John (2007) 'Digital Fears Emerge After Data Siege in Estonia' The New York Times, 29th May, Available at http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all [Accessed 13 November 2013]

Lever, Annabelle (2005) 'Why Racial Profiling is Hard to Justify: A Response to Risse and Zeckhauser' Philosophy and Public Affairs 33(1), pp.94-110.

Lucas, George (2014) 'NSA Management Directive # 424: Secrecy and Privacy in the Aftermath of Snowden' Ethics and International Affairs 28(1), pp.29-38.

Mangan, Joseph (1949) 'An Historical Analysis of the Principle of Double Effect,' Theological Studies 10, pp.41–61.

McCahill, Michael (1998) 'Beyond Foucault: Towards a Contemporary Theory of Surveillance' in Clive Norris, Moran, Jade and Armstrong, Gary (eds.) Surveillance, Closed-Circuit Television and Social Control (Aldershot: Ashgate) pp.41-65.

McMahan, Jeff (2009) Killing in War (Oxford: Oxford University Press)

Merton, Robert (1968) Social Theory and Social Structure. (New York: Free Press).

Misztal, Barbara (1996) Trust in Modern Societies: The Search for the Bases of Social Order (Cambridge: Blackwell Publishers, Inc.).

Nagel, Thomas (1979) Mortal Questions (Cambridge: Cambridge University Press).

Omand, David (2007) 'The Dilemmas of Using Secret Intelligence for Public Security' in Peter Hennessy (ed.) New Protective State: Government, Intelligence and Terrorism (London: Continuum) pp.142–69.

Orend, Brian (2013) Morality of War, Second Edition (Peterborough: Broadview Press).

Øverland, Gerhard (2005) 'Killing Civilians' European Journal of Philosophy 13(3) pp.345-363

Pace, Julie (2013) 'Obama Defends NSA Surveillance Programs Anew', ABC News, 4th September. Available from http://abcnews.go.com/International/wireStory/sweden-obama-showcase-common-global-goals-20150013 [Accessed 4 September 2013].

Parkinson, John and Walker, Clive (2009) *Blackstone's Counter*-Terrorism Handbook (Oxford: Oxford University Press)

Phillips, Robert (1984) War and Justice (Norman: University of Oklahoma Press).

Polyviou, Polyvois (1982) Search and Seizure: Constitutional and Common Law (London: Duckworth)

Posner, Gerald (2010) 'China's Secret Cyberterrorism', The Daily Beast, 1st December, Available from http://www.thedailybeast.com/articles/2010/01/13/chinas-secret-cyber-terrorism.html [Accessed 9 September 2012]

Quinlan, Michael (2007) 'Just Intelligence: Prolegomena to an Ethical Theory' Intelligence and National Security 22(1) pp.1-13.

Rawls, John (1971) Theory of Justice (Cambridge: Harvard University Press)

Robinson, Matthew (2000) 'The Construction and Reinforcement of the Myth of Race Crime' Journal of Contemporary Criminal Justice 16, pp.133-156.

Sanger, David (2012) 'Obama Order Sped Up Wave of Cyberattacks Against Iran', The New York Times, 1st June, A1, Available from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [Accessed 8th June 2013].

Scanlon, Thomas (2000) 'Intention and Permissibility' Supplement to the Proceedings of the Aristotelian Society Vol.74 No.1 pp.301-317

Simitis, S. (1987) 'Reviewing Privacy in an Information Age', University of Pennsylvania Law Review, 135(3) pp.707-46.

Solove, Daniel (2004) The Digital Person: Technology and Privacy in the Information Age (New York: New York University Press)

Sommer, Peter and Brown, Ian (2011) 'Reducing Systemic Cybersecurity Risk', Organisation for Economic Cooperation and Development [online] 57. Available from: http://ssrn.com/abstract=1743384 [Accessed 6 September 2012].

Stone, Richard (2005) The Law of Entry, Search and Seizure (Oxford: Oxford University Press)

Strawser, Bradley (2013) 'Revisionist Just War Theory and the Real World: A Cautiously Optimistic Proposal' in Fritz Allhoff, Nicholas Evans and Adam Henschke (eds.) Routledge Handbook of Ethics and War: Just war in the 21st Century (London and New York: Routledge) pp.76-90

Thomson, Judith (1986) Rights, Restitution and Risk: Essays in Moral Theory (Cambridge: Harvard University Press)

Traynor, Ian (2007) 'Russia Accused of Unleashing Cyberwar to Disable Estonia', The Guardian 17th May Available at http://www.guardian.co.uk/world/2007/may/17/topstories3.russia [Accessed 12 July 2012].

Turner, James T. (1981) Just War Tradition and the Restraint of War: A Moral and Historical Inquiry (Princeton: Princeton University Press)

United Nations Office on Drugs and Crime, (2012) 'The Use of the Internet for Terrorist Purposes' [online] p.9, Available from http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [Accessed 13 November 2013].

Walzer, Michael (2000) Just and Unjust Wars: A Moral Argument with Historical Illustrations (New York: BasicBooks).

Woolcock, Nicola (2007) 'Three Students Jailed for Inciting Terrorism on 'holy war' websites' The Times, 6th July, Available at http://www.thetimes.co.uk/tto/news/uk/crime/article1872875.ece [Accessed 13 November 2013].

[1] Jenkins (2013) explores the boundaries between cyberspace and the physical realm, and argues that even though these might include software they are very much the same as any physical attack. This means not that they should be held to the same legal restrictions as any physical attack. Similarly, even though intelligence covert operations or counterintelligence attacks can be carried out in cyberspace, their impact is very much in the physical realm as so should be examined under equal terms.

[2] Dipert (2013) examines the different cyber domains arguing that it is not restricted simply to the Internet and includes other factors, referred to as Other-Than-Internet or OTI attacks. Dipert discusses on other technologies such as GPS and thumb drives, with the latter being a key part of the Stuxnet attack, using networks but do not necessarily use the Internet.

[3] This type of terminology was reflected in the UK government's Draft Communication Data Bill (2013, §77 p.26): 'So the fact that a person visited www.nhs.uk is communications data and could form part of a web log, but it would not be permissible to record the fact that a person visited www.nhs.uk/conditions/depression'.

[4] This conception of just cause moves away from its traditional war based understanding in order to update it for intelligence. However, Eberle (2013) discusses 'just cause' in relation to the emergence of cyber 'attacks', framing it more inline with military responses.

[5] 'A search under a warrant may only be a search to the extent required for the purpose for which the warrant was issued' UK Police and Criminal Evidence Act 1984 § 16(8).

[6] The maximum length of time to which information collected can be kept collection under this type of example is set by the European Court council through the Parliamentary Assembly of the Council of Europe Data Retention Directive of the European Parliament and of the Council (2006/24/EC March 15, 2006).

[7] Section 5(3) Criminal Law Act 1977 preserved the common law offence of conspiracy tending to corrupt public morals or outrages public decency.

[8] Judgement of 4 May 2012 Case No.0926639036 of the Tribunal de Grande Instance de Paris (14th Chamber/2), Paris.

[9] Feinberg (1984, p.37) calls these requirements 'welfare interests' and John Rawls (1971, p.62) calls them 'primary goods', but essentially they both amount to the same thing, that is, regardless of what conception of the good life the individual holds or what his life plans might be in detail, these preconditions must be satisfied first in order to achieve them. If these vital interests fall below a threshold level, the ability to realise the more ultimate needs, goals or activities can become dramatically hindered. In this way, these interests are the most important interests a person has, and thus cry out for protection.