Intelligence Gathering and Cyberspace

Introduction

Intelligence gathering, understood as the gathering and production of secret information, is routinely undertaken by government security agencies. Such information is deemed necessary by the executive branch of government in order to safeguard national and international security. As the recipient of this information, and ultimate overseer of the activities of the actions taken by security agencies, the executive branch must make ethical decisions regarding how it is obtained and used. This is a difficult task, since the discretion granted to agencies if they are to be effective in protecting national security must be balanced against the possible erosion of the laws and values essential to a democratic society. This difficulty is compounded by the fact that security agencies must by necessity operate with a great decree of secrecy and the consequences of their failing to counter threats effectively are enormous.

Further, the inter-relatedness between what is considered lawful and what is considered ethical is very complex. Some actions which are illegal and normally considered morally reprehensible, say the use of 'enhanced' interrogation methods, might in special circumstances such as the thwarting of an imminent terrorist attack, be considered ethically justified, yet still be illegal. Equally, some actions of intelligence agencies might be legal, yet still unethical, for example the waterboarding of prisoners denied prisoner of war status under the law. Complicating the matter still more is that intelligence agents operating on foreign soil will almost invariably be contravening the laws of the country in which they are working. These types of complexities often lead to situations where members of the executive branch of

government are concerned to preserve plausible deniability regarding their approval of actions taken by their security agencies. The tendency of the executive branch to insist on such deniability, when coupled with the ability of security agencies to operate largely autonomously. makes it important that such agencies take seriously ethical constraints on how they obtain intelligence.

In many areas of ethics, there is a tension between pursuing public goods and protecting the goods of individuals. For example, should an individual's right to ownership of land trump the government from expropriating that land to build a new highway? This tension between public and private good is especially a feature of discussions concerning the ethics of intelligence gathering. Privacy is an important primary individual good, but it cannot automatically trump the public good of national security. Equally, however, the need for public security cannot dismiss that citizens are entitled to have their privacy protected. The balancing of public and private good, and the inevitable tension involved in such balancing, is a fundamental feature of any discussion involving the ethics of intelligence gathering.

Views on the Relation of Ethics and Espionage

We may distinguish between four views concerning the relation between intelligence gathering and ethics. These are: 1) idealism, 2) realism, 3) ethical balance sheet, and 4) proportionality. Traditionally, idealism and realism views dominated discussions of the relation, but recently views based on the ideas of ethical balance sheets and proportionality are receiving increased attention. I think, however, that approaches based on 3) and 4) are best viewed as developments and modifications of the idealism and realism approaches.

Idealism

Idealism is best understood as a deontological approach that emphasizes the intrinsic 'wrongness' of certain actions, irrespective of their consequences. Idealists contend that any kind of effective intelligence gathering necessarily involves unethical behavior. Such behavior, they argue, inevitably undermines the ethical health of a nation leading to it becoming the type of state it wants to protect itself against. Democratic governments on the idealistic view should govern without any reliance on intelligence agencies.

Proportionality

Like idealists, advocates of the proportionality approach insist that certain actions are intrinsically wrong, for example torture, and should never be permitted in the interests of gathering intelligence. They recognize, however, that in many real-world scenarios ethical behavior requires choosing the lesser of two evils. A nation is morally entitled to defend itself against threats to its existence. Intelligence gathering of some form is essential. Unfortunately, intelligence gathering by its very nature involves treating some individuals in ways inimical to their interests. What the proportionality view seeks to do is to differentiate between what must be forbidden, for example torture, and what can be justified, for example, interrogation, always with the goal of ensuring that any harm inflicted is properly proportional to the good achieved.

This is done by adopting a set of principles laid out in just war theory. The cause motivating intelligence gathering must be just, the threat must be such as to justify the harm resulting from the gathering of intelligence, the authority directing the gathering of intelligence must be politically legitimate, there must be a distinction drawn between legitimate and

illegitimate targets, and less harmful means of gathering the required intelligence must be explored before the use of more harmful means.

Realism

Realism is best understood as a utilitarian approach that evaluates actions as ethically correct or not based on their consequences. They appeal to the utilitarian principle that the end justifies the means. Realists contend that what would normally be viewed as immoral actions, for example torture, are nevertheless be justified in the interests of protecting the State. Thus, to protect the great good of democratic government, it is ethically appropriate for a small number of its citizens to engage in acts contrary to democratic ideals and established laws. Otherwise, realists contend, the State would be susceptible to threats from other nations, which would entail an even greater evil than is involved in intelligence gathering.

Ethical Balance Sheet

The idea of an ethical balance sheet is best understood as an outgrowth of realism. Like realism, it relies on the utilitarian principle that the end justifies the means. It attempts not simply to consider presently existing goods and harms but to anticipate potential goods and harms. The idea then is to balance costs, which is to say harms, against benefits, which is to say goods in such a way that the benefits of intelligence gathering outweighs any harms it causes. A great difficulty that faces both these utilitarian based approaches is that it is often difficult to anticipate what the consequences will be of actions taken to try and obtain intelligence. co It seems that a deontological approach that sets out in advance what activities can be viewed as legitimate in the gathering of intelligence is preferable to a utilitarian approach.

Two Forms of Intelligence Gathering

It is helpful to distinguish between two forms of intelligence gathering. Prior to the second half of the twentieth century intelligence gathering was almost exclusively done by covert agents operating on foreign soil. This form of intelligence gathering involves the type of spying described by novelists such as John Le Carré and Jason Matthews. It is commonly referred to as 'humint' i.e. human intelligence.

The latter half of the twentieth century was marked by large advances in communications technology. This gave rise to a form of intelligence gathering known as 'sigint' i.e. signal intelligence, which focuses on intercepting communications. Arguably, signal intelligence can more easily be justified than human intelligence, since it does not involve immediate physical or mental harm in its gathering. Nevertheless, excepting open source data, i.e. data publicly available in cyberspace, surveillance of the presumably private communications of domestic citizens raises concern about the possible erosion of individual rights.

Human intelligence continues to be important, but there has been a shift in emphasis to signal intelligence. The reason this is so is that the rapid and continuing advancement of communications technology has radically changed the strategic environment in which security agencies function. Sophisticated technologies enable access to vast amounts of data, but this increased access to data is accompanied by increased threats from other nations and non-state organizations who possess the same technological capabilities.

Decision makers in the executive branch of government require real-time immediate information. This is no easy task for intelligence agencies to provide, since although the communication of vast amounts of data can be virtually instantaneous, data if it is to be

transformed into information must be interpreted. This has led in instances to state agencies outsourcing intelligence tasks to private contractors. One need only look to the case of Edward Snowden to see the dangers of such outsourcing. At the very least, if state agencies make use of the private sector, there needs to be improved oversight, clear regulatory policies, and ethical training to ensure that private sector operators have the requisite qualifications needed for intelligence work.

Different Rules, Different Times?

What is considered just and ethical in war is very different than what is considered just and ethical during peace. This, as we have seen in the previous chapter when briefly looking at just war principles, does not mean that 'anything goes' in war, only that certain actions that cannot be sanctioned in peace time can be morally justified in times of war.

Traditionally, this distinction has applied to intelligence gathering. It is not clear, however, that this traditional distinction can be applied in contemporary contexts of intelligence work. This is so for at least two reasons.

First, there has been a rise in what may be termed 'asymmetrical' threats. These are threats that originate not from other nation states, but rather from terrorist organizations both foreign and domestic. Such organizations are increasingly borderless and difficult to track. Indeed, the distinction between foreign and domestic terrorism has become blurred, since the easy communication enabled by cyberspace has allowed a much greater opportunity for terrorist organizations to recruit not only in their own country, but also to recruit 'home-grown' terrorist agents in their target countries.

Second, cyberspace has vastly enabled 'cold wars' between nation states. Although not at the time officially at war with Iran, in 2009-2010 the U.S. and Israel employed the Stuxnet virus to sabotage Iran's nuclear program, setting it back at least two years. Some sources claim this setback motivated Iran to sign the 2015 nuclear deal https://www.jpost.com/Middle-East/Iran-News/How-much-can-intel-agencies-slow-Iranian-nuke-program-by-using-sabotage-580728. More recently, Russia through misinformation and the hacking of the Democratic Congressional Campaign Committee and the Clinton website, attempted to influence the American Presidential Election of 2016 https://time.com/5565991/russia-influence-2016-election/.

Given the global reach of cyberspace and the influence of easily constructed misinformation on public perception, it has become clear that the context in which intelligence gathering takes place necessitates rethinking the peace-time war-time distinction.

The Advantages and Disadvantages of Cooperation

There are obvious advantages to the sharing of intelligence by security agencies. For example, the 9/11 Congressional Report concluded that the Al-Qaida attack on New York's Twin Towers could have been prevented had there been greater cooperation between the CIA, FBI, and NSA. Similarly, there are clear advantages to international intelligence sharing.

There are, however, ethical concerns that arise, especially in the area of sharing intelligence at the international level. Not all foreign security agencies share similar rules and values regarding the protection of human rights. This raises concerns regarding both the receiving and giving of intelligence internationally. These ethical concerns are further warranted because most cooperative arrangements between intelligence agencies of different

countries are not covered by treaty law. This allows security agencies to subcontract intelligence gathering to allied foreign agencies, thus formally following the legal and ethical obligations of their own country, nevertheless knowing that the agency to which they subcontracted pays little attention to such obligations. For example, between 2001-2005 the U.S. carried out extraordinary rendition operations which involved the kidnapping, secret detention, and interrogation of suspected terrorists at CIA black sites. These sites were hosted by foreign countries, only some of which are democracies, thus enabling techniques of interrogation that were not legal on U.S. soil https://www.washingtonpost.com/news/monkey-cage/wp/2017/03/14/the-u-s-carried-out-extraordinary-rendition-flights-from-2001-2005-here-are-15-more-countries-that-helped/?noredirect=on&utm_term=.99246c0b8aa4.

Government Data Mining and Privacy

Increasingly, predictive data mining, i.e. the extraction of potentially significant data from enormous bodies of data is being used by intelligence agencies attempting to prevent terrorist attacks. As previously mentioned, data must be interpreted before it can be understood as information. Concerns exist, therefore, not simply regarding the collection of data, much of which may be in the public sphere, but its interpretation.

Apart from worries regarding accuracy of data and the legitimacy of the interpretative inferences by which it becomes information, there are concerns about the use of the resulting information. The potential misuse of information by employees who have authorized access to that information is a real risk, as is the risk of 'mission creep' i.e. the tendency of security agencies to use data it possesses for new purposes not originally authorized by government.

Going Forward

Cyberspace has irrevocably changed intelligence gathering. Something which has not changed, however, is the ethical tension between protecting the security of the State and protecting the security of its individual citizens. Both are legitimate concerns necessitating a careful balancing. This balancing is best accomplishing by rejecting the myth that intelligence gathering is inherently unethical. Intelligence agencies need to be staffed with individuals who take their ethical responsibilities seriously, rejecting claims that the ends invariably justify the means. These agencies need to be guided by clear regulatory frameworks overseen by the executive arm of government, such that citizens can have justified confidence that their rights to privacy and autonomy, even in not absolute, are protected.

Canadian Civil Liberties Association versus Canada, 2016 Ontario Superior Court of Justice

Citation: Canadian Civil Liberties Association v Canada, 2016 ONSC 4172 (CanLII), <**http://canlii.ca/t/gs8w1**>

This case was brought by the Canadian Civil Liberties Association (CCLA) concerning its right to challenge those sections of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) that permit a private sector business organization to collect personal information without a person's knowledge and consent, and then disclose it to a government institution without the person's knowledge and consent. The question before the Court was whether the CCLA in fact had the right to challenge.

As stated in its preamble, the purpose of PIPEDA is to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain

circumstances, by providing for the use of electronic means to communicate or record information or transactions.

The CCLA maintains that Section 7 of PIPEDA breaches ss. 7 and 8 of the *Canadian Charter of Rights and Freedoms*. The organizations that most concern the CCLA are Internet service providers (ISPs) and government institutions whom the CCLA says collect large amounts of personal information in violation of the Charter. The CCLA claims that the scope of permissible disclosure of personal information included in s. 7(3)(c.1) of PIPRDA is arbitrary, overbroad and grossly disproportionate and that the barriers to obtaining information about whether disclosure has been made further the violation of s. 7 and s. 8 of the Charter.

The CCLA claims that law enforcement and security intelligence agencies collect massive amounts of personal information and that the majority of these disclosures are made without prior judicial authorization on the basis of s. 7(3)(c.1) of PIPEDA. Generally, ISPs do not inform individuals if a government agency has requested personal information about them and some ISPs refuse to disclose the number of requests made by government agencies for personal information. The information collected can be used for both criminal proceedings and intelligence purposes and may also be shared with foreign law enforcement and intelligence agencies. Both the Canadian Security Intelligence Service and the Communications Security Established refused to disclose the frequency of their requests, claiming that disclosure would harm national security, their ability to collect intelligence, and their ability to advise the government. At the time of the case, the RCMP was not able to provide information about the frequency of its requests because it did not maintain a central data repository. The judge ruled that the CCLA did have the right to challenge those sections of PIPEDA that permit an ISP to collect personal information without a person's knowledge or consent and then disclose it to a government institution without the person's knowledge or consent.