2 Truth-seeking and the principles of discrimination, necessity, proportionality and reciprocity in national security intelligence activity

Seumas Miller

Introduction

National security intelligence is information or other data collected, analyzed and disseminated by intelligence agencies (in particular) and done so in the service of these agencies' primary institutional purpose (Miller 2010), at least in liberal democracies. Here it is understood that this institutional purpose and these actions are to be understood normatively, that is in terms of what *ought to be* done, as opposed to *what is* in fact being done. Here, the term "normative" has a moral or ethical loading, for example what ought to be done is typically what morally ought to be done all things considered (including consideration of the empirical facts).[1] Moreover, these essentially *epistemic* (from the Greek word, "episteme", meaning knowledge) or evidence-based truth-seeking activities of collection, analysis and dissemination are the main ones performed by national security agencies. That said, many of these agencies also perform *kinetic* tasks, for example the covert operations conducted by the United States CIA (Central Intelligence Agency), and on occasion tasks that might be referred to as *quasi-epistemic*, for example psychological "warfare".

Further, the definition of national security is highly problematic; the concept of national security is ill-defined, indeterminate, shifting, open-ended and contestable (Williams 2003, 511–31, 514; McDonald 2008, 563–87, 567; Buzan, Wæver, and de Wilde 1997, 24). For instance, the US National Intelligence Strategy has as one of its purposes to promote American prosperity.[2] However, let us assume that national security intelligence is, at the very least, intelligence pertaining to serious internal or external threats to the nation-state itself, or to one of its fundamental political, military or criminal justice institutions, and that these threats might emanate from state or non-state actors, for example terrorist groups. So national security intelligence includes not only military intelligence but also some criminal intelligence and economic intelligence, since the latter may have national security implications, for example intelligence on drug cartels destabilizing governments or on fighter aircraft being built by private companies.

It might be claimed that unlike, for instance, much of the intellectual work conducted in universities,[3] intelligence collection, analysis and dissemination is

DOI: 10.4324/9781003164197-4

not an end in itself but rather the means to some further end; that is, the end point of the intelligence process is actionable intelligence, that is intelligence provided to relevant decision makers that is a means to kinetic action. In one sense this claim is true. Intelligence does need to be actionable; intelligence collection and analysis has a purpose beyond acquisition of the truth (so to speak). However, in another sense it is false. For the acquisition of the truth (or, at least, of probable truth) is (or ought to be) an end in itself for intelligence officers, notwithstanding the further requirement that the truths acquired be actionable. Let me explain.

The activities of intelligence collection and analysis are not related to knowledge merely as means to end, but also conceptually. Truth is not an external contingently connected end which some intelligence activities might be directed towards if the intelligence officers happened to have an interest in truth, rather than, say, an interest in falsity or an interest in neither but rather only in "playfulness" (a la postmodernists) or self-interest (a la demagogues, such as former US President, Donald Trump, who have a tendency to say whatever they believe might be useful to them and do so without regard for the truth). Rather truth is internally connected to intelligence activity. Thus aiming at truth is aiming at truth as an end in itself. (This is, of course, consistent with also aiming at truth as a means to some other further end, such as apprehending an offender or winning a war.) In other words, supposed intelligence activity which *only* aimed at truth as a means to some other end would not be genuine intelligence activity or would be defective qua intelligence activity, since for such a pseudo-intelligence officer truth would not be internal to his or her activity. Such pseudo-intelligence officers would abandon truth-aiming if, for example, it turns out that the best means to the officer's end is not after all truth, but rather falsity. Obviously, such pseudo-intelligence officers would be extremely dangerous since their intelligence would be very unreliable. For they are not simply officers who aim at (and more often than not acquire) the truth but who, nevertheless, often present false reports to their political masters (or other "clients") knowing them to be false (or, more likely, to be somewhat misleading because unpalatable truths are omitted or downplayed). Rather these pseudo-intelligence officers do not aim at truth in the first place. That is, having little interest in the truth, they do not seek the truth and, as a result, do not themselves acquire knowledge; therefore, they do not have knowledge to pass on to their political masters. Of course, in the real world such pseudo-intelligence officers are unlikely to exist in a pure form. However, in an intelligence agency lacking in independence and in which intelligence officers' desire to please or, more likely, desire not to antagonize their political masters (e.g. some Soviet intelligence officers who served under Stalin), the commitment to the truth might well weaken, especially when one considers the inherent difficulties in acquiring accurate, significant national security intelligence from adversaries determined to maintain information security. As a consequence, such intelligence officers might initially have the practice of reporting what they know to be false or misleading on some occasions when it is politically or otherwise expedient to do so, but end up over time largely abandoning the practice of evidence-based truth-seeking in favour of selective data collection and skewed analyses in the service of personal,

political or other non-epistemic agendas; that is, end up becoming something akin to pseudo-intelligence officers.

There is an important institutional implication of the earlier discussion. As we have just seen, whereas the primary institutional purpose of national security intelligence agencies is essentially epistemic, the realization of this epistemic purpose serves a larger national security purpose only realizable by the kinetic activity of other institutions, for example the military. Accordingly, there is an institutional division of labour; the intelligence agency provides knowledge (or weaker epistemic goods) to the decision makers, for example politicians and military leaders, who in turn act (or refrain from acting) on that knowledge. In order for this institutional division of labour to function successfully it is critical that the intelligence provided is reliable and, therefore, that the epistemic activity of the intelligence agencies is not unduly influenced or otherwise undermined by the institutions which they serve, for example by their political masters. Accordingly, consistent with an appropriate level of responsiveness to their political masters' national security intelligence demands, it is necessary that intelligence officers' professional commitment to the epistemic purposes of their intelligence agencies overrides any personal loyalty they might have to their political masters; indeed, on occasion, they may need to speak unpalatable truths to power. However, it is also necessary that intelligence officers have an overriding professional commitment to the epistemic purposes of their intelligence agencies rather than seeking to realize the ultimate national security outcomes that might or might not flow from the decisions of the politicians, military leaders and other decision makers who act on their intelligence. It is important that intelligence officers do not engage in institutional overreach.

In relation to national security intelligence and the normative theory thereof, a threefold distinction needs to be kept in mind, namely:

1. **Institutional level** – the core activities, structures, resources and institutional purposes of national security intelligence agencies, for example the raison d'etre for the establishment and continued existence of MI5 in the United Kingdom
2. **Macro-activity level** – the mid- to long-term goals, strategies and campaigns of national security intelligence agencies, for example to win the Cold War, increased reliance on electronic rather than human intelligence
3. **Micro-activity level** – immediate, specific, operations of national security intelligence agencies, for example surveillance of a given terrorist suspect

Note that these three levels interact, for example level 1 drives level 2 which in turn drives level 3 (and the reverse interactive process from level 3 to level 2 to level 1 is also the case).[4] Moreover, the distinction between the three levels is not necessarily clear-cut, for example when does a short-term goal, such as collecting intelligence on the perpetrators of 9/11, become a mid- or even long-term goal, such as collecting intelligence on Al-Qaeda? For our purposes in this chapter, it is important to note the difference between a normative theory of an institution in

an avowed liberal democracy [e.g. of Israel's Mossad or of the United States NSA (National Security Agency)], a normative framework for the conduct of macro-level activity (e.g. of UK secret intelligence activity in the Cold War or of bulk data collection and analysis by the NSA) and a set of ethical guidelines for the conduct of micro-level activity (e.g. ethical guidelines in relation to intelligence collection on a member of a home-grown extremist right-wing subversive group or on "turning" a member of a foreign intelligence agency).

Regarding the normative theory of institutions, we have serviceable normative theories of police organizations [e.g. as the protection by means of police use of coercive force – or the threat thereof – of the legally enshrined, justifiably enforceable, moral rights of citizens from violation by fellow citizens (Miller and Blackler 2016, chap. 1)] and of military organizations [e.g. as the protection by means of military use of lethal force – or the threat thereof – of the legally enshrined, justifiably enforceable, joint moral rights of citizens – e.g. territorial rights – from violation by members of the armed forces of foreign nations or of other political entities (Miller 2016b, chap. 3)]. Accordingly, we can derive serviceable normative theories of intelligence agencies engaged in (respectively) criminal intelligence and military intelligence; the realization of the epistemic purposes definitive of these intelligence agencies ultimately serves in turn the institutional purposes of police and military organizations (respectively). But what of national security intelligence agencies? Their remit is wider in some respects than that of criminal intelligence agencies and that of military intelligence agencies (and also narrower in some respect than each of these types of intelligence agencies, i.e. a great deal of criminal intelligence is not national security intelligence and – arguably – not all military intelligence is of interest to national security agencies, e.g. intelligence at the micro level concerning a small-scale enemy troop movement that is without much strategic significance). Evidently, we do not yet have a serviceable normative theory of national security intelligence agencies (or even an acknowledgement that one is needed). This is a significant gap in normative theory and, given the expanding role of national security intelligence agencies, for example in relation to pandemics and the impact of climate change or as a result of technological developments such as in respect of GEOINT, one with potentially important practical implications. On the other hand, it might be argued that in place of a normative theory, a set of relatively concrete, historically relative, national security purposes could be specified, such as collecting and analyzing intelligence required for counter-terrorism purposes or that will assist the armed forces engaged in combat, and ascertaining the intentions and capabilities of hostile, dangerous, authoritarian states, such as Russia, China, Iran and North Korea. However, ultimately, the selection of these national security purposes would need to be justified, at least in part, by recourse to a normative theory of national security, for example self-defence (an unduly narrow account) or national interest (an unduly wide account).

Importantly, this aforementioned threefold distinction does not parallel the twofold distinction in traditional Just War Theory between the jus ad bellum (the principles justifying waging war) and the jus in bello (the principles under which

the war once embarked upon should be conducted), and even less so the contemporary fivefold distinction between jus ad bellum, jus in bello, jus post bellum (the principles applicable once hostilities have ceased) and jus ad vim (the principles governing the use of force short of war).[5] This so notwithstanding recent attempts to apply Just War Theory to national security intelligence activities via the so-called Just Intelligence theory (Bellaby 2014; Quinlan 2007); evidently the morality of national security intelligence activities does not parallel the morality of kinetic military activities (Miller 2021).

There are a number of reasons for this. Firstly, as mentioned the constitutive (proximate) end of intelligence activity is knowledge, that is it is a form of truth-seeking. By contrast, the constitutive end of military activity is non-epistemic, that is it is a form of kinetic activity. Secondly, as a result of intelligence activity being epistemic activity ("knowing things"), it is inherently less harmful than kinetic military action ("killing people and breaking things"). Thirdly, intelligence and military activities stand in (roughly speaking) the relationship of knowledge to action; kinetic action presupposes epistemic action since the decision to perform a kinetic action (or not to do so) presupposes knowledge with respect to the why, how, what, when, where, who etc. of the kinetic action in question (and its alternatives); hence intelligence collection is the first resort and the use of military force the last resort (and, indeed, the principle of last resort is constitutive of Just War Theory but not of intelligence activity). Fourthly, national security intelligence activity is a continuous, ongoing (indeed, cyclical – hence the so-called intelligence cycle) activity in relation to threats and enemies that come and go; unlike war it has no determinate end state, the cessation of hostilities, that is being aimed at (perhaps understood in terms of winning the war).[6]

Notwithstanding that intelligence activity has knowledge as its constitutive end and military activity does not, there do seem to be a number of moral principles that govern both sets of activities, for example the principles of necessity and proportionality. These principles, at least, are in part constitutive of normative theories of intelligence agencies, normative frameworks for ongoing intelligence campaigns and sets of moral guidelines for intelligence operations, and they apply at each of the three levels mentioned earlier. Indeed, *some* of these principles, or analogues of them, are constitutive of quite different types of security agency and their activities, for example military organizations versus police organizations. Consider, for example, Just War Theory[7] and its supposed analogue in intelligence work, Just Intelligence Theory.[8] However, appearances notwithstanding, these principles apply differently in these different institutional settings and within a given institutional setting (e.g. of national security intelligence settings) at each of these three levels. Indeed, each of these principles might actually consist of a set of somewhat diverse principles. For instance, the so-called principle of necessity might in fact denote more than one principle, for example the principle of military necessity typically concerned with avoiding civilian casualties *and* the principle of necessity in policing typically concerned with avoiding death or injury to offenders (Miller and Blackler 2016). Moreover, the principle of necessity might apply at the institutional level (e.g. is it necessary to have a national security

intelligence agency?), at the macro level (e.g. is it necessary to collect secret intelligence on one's allies?) and at the micro level (e.g. is it necessary to intercept the communications of a suspected terrorist with his children?).

The focus of this chapter is with the analysis and application of four moral principles, namely discrimination, necessity, proportionality and reciprocity in national security intelligence activity. However, in doing so we need to keep in mind, firstly, the twofold distinction between these moral principles and the closely associated legal principles; secondly, the twofold distinction between the essentially evidence-based truth seeking *epistemic* activity of national security intelligence agencies and the *kinetic* activities of military and police organizations (and some national security intelligence agencies at times, notably covert action) and thirdly, the threefold distinction between the institutional, and the macro and the micro levels. We begin with the moral principle of discrimination (Green 1993).

Principle of discrimination

The context for the application of the principle of discrimination is typically taken to be a theatre of war in which (especially) the lives of non-combatants are at risk from the combatants waging the war in question. According to this principle it is prohibited for combatants to deliberately target non-combatants. This is consistent with the deaths of non-combatants being an unintended consequence, even a foreseen unintended consequence, of the actions of combatants (although, under an associated precautionary principle combatants are required to take steps to minimize the risks to non-combatants).[9] The principle of discrimination is potentially implicated in national security intelligence activity in so far as it is an expression of a more general moral principle according to which innocent persons ought not to be deliberately harmed or otherwise have their rights deliberately violated. Accordingly, it would be one thing for police to intercept and access the metadata and content of the phone calls and emails of a known terrorist on an ongoing basis for intelligence purposes and quite another for this to be done on an ongoing basis for intelligence purposes to a citizen known to be innocent of any crime, e.g. on the off-chance that some useful intelligence might be picked up. Surveillance of the terrorist would in this instance be *morally justified infringement* of the right to privacy, whereas surveillance of the innocent citizen would evidently be a *violation* of the right to privacy.

However, as just mentioned, the principle of discrimination as it applies in armed conflict assumes a distinction between combatants and non-combatants and prohibits combatants from deliberately targeting non-combatants. By contrast, the analogous (let us assume) principle of discrimination in national security intelligence activities (referred to as the principle of discrimination*) does not consist of a general prohibition on targeting innocent persons and with good reason; innocent persons may be a useful source of national security intelligence. Of course, innocent persons will often willingly provide intelligence if asked (whereas non-combatants are unlikely to consent to being deliberately killed).

Indeed, it is permissible for intelligence officials to collect intelligence from innocent persons even without their consent. For instance, it is permissible for an intelligence official to deliberately obtain information about a terrorist from the terrorist's innocent relative without the latter's consent, for example by accessing their private communication without their permission, or by deception, for example by telling a lie. By contrast, deliberately killing the terrorist's innocent relative is obviously prohibited (with or without their consent).

Intelligence activities ultimately aimed at identifying terrorists and thwarting acts of terrorism now involve the application of machine learning techniques to bulk databases that consist in the main of the communication and other data of innocent civilians – indeed, frequently innocent fellow citizens, that is the data of innocent civilians is deliberately collected and accessed (or, at least, filtered and accessed). It can be argued that while the data of these innocent persons is "read" by a machine it is not seen by human eyes or, at least, it is only the data that results from the application of the machine learning process that is seen by human eyes; however, the argument might continue, such data meets the standard of reasonable suspicion already applicable to intelligence gathering/investigation by law enforcement agencies and does so by virtue of being the result of that very process. Whatever the merits of this argument as a justification for the application of machine learning techniques to bulk databases by way of mitigating the degree and extent of intrusion into the privacy of innocent citizens,[10] nevertheless, this intrusion into the privacy of innocent civilians is deliberately done, albeit as a means to an end. As such, it is not analogous to the principle of discrimination as it applies to the use of lethal force by combatants in war; combatants, to reiterate, are not permitted to *deliberately* kill innocent civilians, even as a means to some further legitimate end. The reason for this difference between the principle of discrimination* applicable in intelligence activities and the principle of discrimination applicable to the use of lethal force by combatants reflects the much greater moral significance that attaches to deliberately taking an innocent person's life than attaches to deliberately invading an innocent person's privacy or deliberately deceiving them. This difference in moral significance in turn reflects, indeed in large part is derived from, the greater moral weight that attaches to life than to privacy or truth-telling. Hence there is an (more or less) absolute legal prohibition on deliberately killing the innocent (even in wartime), but not on deliberately invading their privacy or on telling lies to them (even in peacetime).

We have seen that the principle of discrimination assumes a twofold distinction between combatants and non-combatants (even if, at times, there are problems determining whether a person is a combatant or a non-combatant and even if there is a third category of civilians who are engaged in hostilities at particular times but who are not combatants per se). By contrast, police operate with a threefold distinction between innocent persons, suspects and known offenders. Innocent persons ought not to be deliberately harmed whereas known offenders may be, for example police may target known offenders using coercive, incapacitating or even lethal force. But what of suspects? Suspects are the targets of police investigation; that, is an essentially epistemic activity in part constitutive of policing. By

contrast, combatants are not investigators, even if at times they need to determine whether or not a person presenting as an innocent civilian is in fact a combatant. This threefold distinction in policing cuts across the combatant/non-combatant distinction. For instance, combatants are not necessarily suspected of crimes or offenders and neither suspects nor offenders are necessarily combatants. What of national security intelligence officers?

As we have seen, the targets of intelligence officers can be willing or unwilling providers of intelligence (let us take a willing provider to be someone who has consented to provide information). Moreover, those who are willing might be individually contacted or the information they willingly provide (in effect) might already be publicly available. Those who unwillingly provide intelligence might do so without knowing they have done so, for example as a result of a surveillance operation or an undercover operative who deceives them, or they might do so knowingly, for example as a result of a coercive interrogation. Moreover, the "providers" of intelligence might have had the intelligence stolen from them by a field officer, for example a spy. Note that some publicly available information might, nevertheless, not have been willingly provided to intelligence officers, for example some information regarding an adult might be posted on social media by his naïve adolescent daughter who is unaware that it might be accessed by and of interest to intelligence officers.

An additional important point to be made here is that whereas each single item of an integrated body of information might have been willingly provided the aggregate of that information, once analyzed to create the integrated body of information, might not have been willingly or even knowingly provided. For instance, intelligence officers might construct a fairly detailed picture of the characteristics, behaviour and movements of an individual on the basis of multiple, single, incremental items of publicly available information, including information extracted from social media. An analogous, but more alarming, point can be made in relation to intelligence activity at the macro level and, indeed, at the institutional level. What if such detailed pictures can be constructed of most of the members of an entire population? Evidently, the Chinese state is aiming to do just this, notably in Xinjiang, and, thereby, displaying a de facto institutional purpose of its intelligence agencies: social control in the name of national security. It should be noted that this projected surveillance society (Chinese style) is to make use of a wide range of integrated databases of personal and public information much of which is not readily available to intelligence officers (or members of other security agencies) in liberal democracies.

The fundamental point to be made in the light of the earlier discussion is that the principle of discrimination* applicable to intelligence officers is only very loosely analogous to the principle of discrimination applicable to combatants and non-combatants, since the targets of intelligence officers could be virtually anyone (even if not everyone) and the moral constraints on their intelligence activity pertain more to the nature and extent of the intelligence being sought (e.g. is it the confidential or private information of large cohorts of people?) and the particular methods used to collect it, for example coercive interrogation, deception, intrusive surveillance or theft.

A final point regarding the principle of discrimination* (i.e. discrimination as it applies to intelligence activities) does pertain to the targets of intelligence officers. This point arises from differences between internal and external national security threats and it is, therefore, relevant not only to the micro level but also to the macro level. In liberal democracies at least, foreigners who are the targets of national security intelligence activities enjoy few – if any – protections and in this respect they are unlike fellow citizens who are the targets of national security intelligence activities. Yet, the innocent citizens of enemy authoritarian states have moral rights, including privacy rights (whatever their legal rights may be or, more likely, not be). On the other hand, it does seem that given the purpose of the intelligence activities in question is national security, it is perhaps to be expected that the principle of discrimination* and, for that matter, the principles of necessity and proportionality, might justifiably be applied in a more permissive manner to foreigners than to fellow citizens.[11] We return to this issue in the final section.

Principle of necessity

As we saw in the introduction, the principle of necessity applies to both kinetic military and kinetic law enforcement activity and to epistemic intelligence activity, and does so at all three levels, that is the institutional, macro and micro levels. Thus, in respect of epistemic national security intelligence activity, it is necessary to, firstly, have a national security intelligence agency (institutional level), secondly, to spy on hostile enemy powers (macro level) and, thirdly, to intercept the communications of, for instance, Osama bin Laden's trusted courier in order to locate his leader (micro level).

Elsewhere I have provided an analysis of the principle of necessity (or, perhaps, principles of necessity) (Miller 2021) and one that differs from the standard account (Lazar 2012). According to my own analysis, the principle of necessity has at its core a means/end principle and the necessity in question refers to the necessary means to an end (whether it be the end of personal self-defence, or a military, law enforcement or national security intelligence end). Thus if the only available means to achieve an intelligence end is intrusive surveillance of a target then the necessity principle might require that this means be used, notwithstanding that it infringes the target's privacy. If, on the other hand, there was an alternative means, say, collecting the metadata from the target's phone then neither of these two methods would be a necessary means (although it would be necessary to choose one or other of these two methods if the end was to be realized).

However, there is a further factor in play. For it will be claimed that the means that ought to be relied on is metadata collection since it is *not necessary* to engage in intrusive surveillance. However, from the mere fact that one of two available means is not necessary to realize some end it does not follow that it ought not to be chosen. After all, ex hypothesi neither of the two available means is a necessary means to achieve the end in question and it would be irrational not to choose any of the available means to one's ends. Clearly, the idea is that the less harmful means morally ought to be chosen. Metadata collection ought to be preferred to

intrusive surveillance since it is the less harmful means. Evidently, there is another end in play here; an end in addition to the end of acquiring intelligence. The end in question is the moral end to minimize harm, from which can be derived the moral principle to minimize harm to others. So the necessity principle is to be analyzed in terms of a core means/end principle and an implied harm minimization principle. Notice that the necessity principle in play in intelligence activity (the principle of necessity*) is different from the principle of military necessity (and from the principle of necessity applicable in law enforcement) by virtue of the different constitutive ends of the two principles: an epistemic end and a kinetic end (respectively). Since both of these constitutive ends are morally significant the principle of necessity and the principle of necessity* are moral principles twice over (given they are also moral principles by virtue of their implied harm minimization principle).

While epistemic actions, including intelligence activity, have knowledge as their constitutive end, kinetic actions, including military activity, do not; rather military activity has the end of winning battles (and, ultimately, wars). However, as we also saw, intelligence activities and kinetic military activities (and, also intelligence activities and kinetic law enforcement activities, respectively) stand in the relationship of knowledge to action; the decision to perform a kinetic action presupposes knowledge with respect to the why, how, what, when, where, who etc. of the kinetic action in question. Hence, intelligence collection is temporally and logically prior to the use of military force; intelligence collection is, for these reasons, the first resort. Moreover, the use of military force, unlike intelligence collection and analysis, is inherently extremely harmful; it involves killing people rather than merely coming to know things. Hence, the use of military force is a last resort – this time for moral reasons.

While obviously the principle of necessity* thus analyzed (as an amalgam of a core means/epistemic end principle and an implied harm minimization principle) is applicable to national security intelligence activities in some circumstances, a question arises as to the extent of this applicability; perhaps its applicability is actually quite limited, unlike the analogous principle of military necessity, for instance. Thus intelligence activities, including collection, might not be necessary to a strategic or operational end but might, nevertheless, be justified on some weaker basis, such as being potentially useful. A related point is that the intelligence value of some collected intelligence is not known prior to analysis of it; that is, at the point of collection the intelligence might only be believed to be potentially useful (and possibly true), but certainly not believed to be necessary. Again, under a policy of redundancy a number of informers might be deliberately cultivated in relation to some national security task only one, or at most two, of whom might be necessary, that is any one (or at most two) of the informers would be sufficient for the task. However, multiple informers might increase the likelihood that the intelligence collected was reliable. By contrast, it would be hard to justify shooting dead all the members of a large cohort of enemy combatants (let alone embarking on a war against another nation-state), on the grounds that while unnecessary it was potentially useful. So the applicability of the principle of

military necessity to military action is wide and strict whereas the applicability of the corresponding principle of necessity* to national security intelligence activities is much more limited and much less strict.

The width and strictness of the applicability of the principle of necessity to military action reflect the obvious fact, as mentioned earlier, that the means to achieve military ends, that is use of lethal force, are inherently extremely harmful, whereas the means to achieve epistemic ends, including epistemic national security intelligence ends, typically are not, or need not be. Of course, the realization of epistemic national security intelligence ends is the means to kinetic ends that can be inherently extremely harmful, for example war. However, in and of itself the proximate end state of successful epistemic national security intelligence activity is not harmful, even if the means to that end state are, for instance, violations of privacy, since this end state simply consists in intelligence officers (and those who receive their intelligence) being in a state of knowledge. Whether harm results from this knowledge depends on the decision makers who receive this knowledge from the intelligence officers, for example if these decision makers decide to go to war on the basis of the intelligence they have received. Accordingly, it is the decision makers, such as military leaders and politicians, who are directly morally responsible for the harm resulting from their decisions. On the other hand, the intelligence officers who provide them with the intelligence which informs their decisions bear a degree of indirect moral responsibility for the harms (as well as benefits) that result from these decisions. Indeed, in the case of avoidable great harm resulting from bad intelligence the relevant intelligence officers may well have a high degree of moral culpability [albeit in the context of being morally responsible jointly with the decision makers, i.e. there is collective responsibility (Miller 2016b)].

Notwithstanding the contrast with lethal force in theatres of war, the means used to achieve epistemic national security intelligence ends may well be somewhat, even very, harmful, for example coercive interrogation, and frequently involve infringement of privacy, confidentiality or informational property rights. Accordingly, it is important to consider the threshold at which the use of harmful methods and, in particular, methods involving privacy/confidentiality infringements/violations or information theft might justifiably be used to collect national security intelligence. The threshold at which discrete national security intelligence operations *at the micro level* can justifiably be conducted if, for example, they infringe some individual's privacy, confidentiality or property rights is somewhat unclear. It might be thought that the notion of reasonable suspicion could be invoked in relation to domestically focused national security intelligence operations, as it is invoked in relation to criminal investigations (a related essentially epistemic activity). However, intelligence collection cannot be expected to wait for reasonable suspicion; after all, it is often intelligence collection that generates reasonable suspicion. Accordingly, reasonable suspicion seems too high a threshold standard for intelligence collection to have to meet. Of course, intelligence collection which is restricted to information already in the public domain (or otherwise uncontroversially, justifiably accessible to security agencies, e.g. in the case files

of past investigations) can generate reasonable suspicion. However, this suggestion runs into the problem mentioned earlier of privacy/autonomy violations arising from the creation of detailed profiles of individuals based solely on publicly available information (in conjunction with other information uncontroversially, justifiably available to security agencies).

In the absence of a principle-based solution to this first threshold problem it is unclear where the line is to be drawn in relation to (at least) domestically focused national security intelligence collection. Moreover, it has implications for our question concerning the extent of the applicability of the principle of necessity* to national security intelligence activities. For a solution to the threshold problem would, in effect, place a prior constraint on national security intelligence collection such that even if the collection in question was reasonably judged to be necessary it might, nevertheless, not be morally (or legally, if the relevant law tracked morality) permissible. In this respect, the prior constraint would interact with the principle of necessity* in a way analogous to the way the principle of discrimination interacts with the principle of military necessity, that is combatants cannot deliberately kill innocent civilians, even if it is reasonably judged to be militarily necessary to do so.

There is a second related threshold problem, namely one with respect to the threshold at which national security-based bulk data collection and/or use *at the macro level* can justifiably be undertaken, given the potential for such collection/use to increase to the point where it compromises liberal democracy.[12] Consider in this connection the establishment of biometric databases and their integration with existing criminal justice, financial, health and so on databases (Miller and Smith 2021). Perhaps it can be justified in relation to bulk data pertaining to specific foreign powers who have by their hostile and other actions already met the threshold standard of reasonable suspicion. However, the creation of, or access to, such bulk data collections might be made difficult, if not impossible, by the foreign power in question. It is, presumably, far easier to create bulk data collections pertaining to one's own citizenry. However, doing so may lead to a power imbalance between the state and the citizenry that compromises liberal democracy. Accordingly, in the absence of a solution to this second threshold problem it is unclear where the line is to be drawn in relation to national security intelligence collection. On the other hand, a solution to this second threshold problem would, in effect, place a prior constraint on national security intelligence collection such that even if the collection in question was reasonably judged to be necessary (and not merely potentially useful) for national security ends, it might, nevertheless, not be morally (or legally, if the relevant law tracked morality) permissible.

Principle of proportionality

In national security intelligence activities, as in personal self-defence, law enforcement and waging war, the application of the principle of necessity* implies the application of the principle of proportionality (in the weighing of means against ends) or, at least, a principle of proportionality (principle of proportionality*);

and the application of the principle of proportionality* presupposes the application of the principle of discrimination*. Moreover, the implied principle of harm minimization is also in play.

On the one hand, harm in terms of privacy infringements, deception and theft of information (as opposed to, say, coercive interrogation) is easy or, at least, easier to justify in the case of suspects – and certainly known offenders, for example known terrorists – than in the case of innocent citizens. Hence the application of the principle of proportionality* presupposes the principle of discrimination* in play; it might be disproportionate to collect intelligence by means of an intrusive method from a person believed to be innocent of any serious crime but not disproportionate if the target were a known terrorist. On the other hand, the principle of proportionality* presupposes the provision of some moral weight to be accorded to national security (the ultimate end, we are assuming, of the activity) or, at least, to be accorded to the likely national security outcome that might result from the use of the intelligence to be collected, analyzed and disseminated. Hence the application of the principle of proportionality* presupposes the principle of necessity*. Here we should also note that inherent differences between epistemic action and kinetic action mentioned earlier infect the application of the principle of proportionality* as they did the application of the principle of necessity*. We saw earlier that the intelligence value of some collected intelligence is not known prior to analysis of it; that is, at the point of collection the intelligence might only be believed to be potentially useful (and possibly true), but certainly not believed to be necessary. Accordingly, it will be difficult at the point of collection to determine whether or not a harmful method, for example deception of an innocent person, necessary to collect the intelligence is disproportionately harmful.

As argued before, national security intelligence activity exists at both micro and macro levels. This has implications for the application of the principle of proportionality* (as we saw it had for the application of the principle of necessity*). Consider in this connection national security intelligence bulk data collection. At the micro level, the application of the principle of proportionality* (and of the principle of necessity* and of discrimination*) is on specific intelligence operations directed at particular targets, for example collecting information concerning the associates of a suspected terrorist. Thus, a question to be addressed might be: is intrusive surveillance proportionate? What of the macro level? Key ethical issues at the macro level pertain to proportionality of the establishment and general uses of the bulk databases themselves (Anderson 2016).

The principle of proportionality needs to take into account not only the somewhat vague character of the end of national security (definitive, as we saw earlier, of the principle of necessity) and the obstacles faced by intelligence officers, for example high-level encryption, but also potential future harms arising from national security intelligence activities and, in particular, from the utilization of bulk data. Concerns in this area are somewhat allayed by the fact that the bulk data collected and analyzed is typically in an anonymized form (e.g. by means of machine learning techniques), and, therefore, only the privacy rights of genuine suspects are infringed (i.e. the individuals identified upon completion of the

analysis). However, these harms, such as the aforementioned power imbalance between citizens and the state arising from extensive privacy infringements by intelligence agencies, and a diminution in public trust as a consequence of the secret nature of national security intelligence activities, may be incremental in character and difficult to quantify.

Accordingly, an aspect of the aforementioned threshold problem comes into view. For it can be difficult to know exactly where to draw the line between proportionate and disproportionate intelligence activities when it comes to the utilization of bulk data for national security purposes. Consider in this connection the aforementioned potential utilization of integrated biometric and non-biometric databases. One prominent concern about the inadequacy of privacy protections is the potential for "function creep", where the use of information taken for a particular purpose is used for other purposes for which consent was not obtained. The underlying concern in relation to "function creep" is, in effect, the power imbalance already mentioned. More specifically, there is a threat to individual autonomy posed by comprehensive, integrated biometric and non-biometric databases utilized by governments and their security agencies in the service of ill-defined notions of necessity and national security and, at least potentially, without appropriate regulatory constraints and democratic accountability.

Espionage and the principle of reciprocity

Thus far I have provided an analysis of the principles of necessity* and proportionality*, and of their relationship to one another and to the principle of discrimination* in their application to national security intelligence activity. I have done so in the context of knowledge derived from evidence-based truth-seeking being the constitutive (proximate) normative end of national security intelligence activity and the fundamental normative institutional purpose of national security intelligence agencies. I now want to argue that there is an additional normative principle governing external national security intelligence activities (call it espionage), in particular; this is a principle of reciprocity. Since I have discussed this in detail elsewhere I will be brief.[13]

Intelligence gathering, surveillance and so on of citizens by domestic law enforcement agencies might be thought to be reasonably well defined and regulated; hence the *apparent* feasibility of simply extending the law enforcement model to national security intelligence collection within domestic jurisdictions. However, this domestic law enforcement model is clearly too restrictive, and not practicable, in relation to external national security intelligence gathering from, for example, hostile foreign states during peacetime, let alone wartime. So the question arises as to whether some different moral principle(s) needs to be invoked in relation to espionage, in particular. I argue that two principles of reciprocity need to be invoked: a retrospective and a prospective principle.[14]

The retrospective principle of reciprocity would justify nation-state, A, engaging in espionage against nation-state (or non-state actor), B, in circumstances in which B had engaged, or was engaging, in unjustifiable espionage on A, but only

if A's espionage was in the service of A's morally justifiable political purposes, namely, national security.

The prospective principle of reciprocity is a tit-for-tat principle in the service of bringing about a morally desirable future state of affairs. The state of affairs in question is an equilibrium state among nation-states; more specifically, a morally justifiable equilibrium under the rule of international law. So this principle does not justify harmful actions in the manner of its sister retrospective principle; rather it has as its purpose to eliminate, or at least greatly reduce, harmful actions and, in this case, espionage and, thereby, move relevant nation-states into some form of a social contract.

On the one hand, the United States and its allies cannot be expected to defend their legitimate national interests with their hands tied behind their backs. So their recourse to espionage seems justified and the retrospective principle of reciprocity provides a specific moral justification for this. On the other hand, understood as a prospective tit-for-tat procedure in the service of bringing about a social contract, the principle of reciprocity requires the moral renovation of espionage, including cyber espionage, as it is currently conducted. Second, I make a couple of suggestions: (i) the clustering of nation-states and (ii) a demarcation between government and security personnel on the one hand and ordinary citizens on the other.

Under existing arrangements the United States, the United Kingdom, Canada, Australia and New Zealand – the so-called Five Eyes – share information gathered from other states. These nation-states are, so to speak, allies in espionage, notably cyber espionage; for example, they share intelligence. They are the members of my first cluster. There are, of course, other liberal democratic states outside the Five Eyes, such as various EU countries, which have "shared core liberal democratic values" with one another and with the Five Eyes and, specifically, a commitment to privacy rights. This is a second cluster.

The members of these two clusters ought to make good on their claims to respect privacy rights by developing privacy-respecting protocols governing their intelligence gathering activities in relation to one another. Of course, determining the precise content of such protocols is no easy matter given, for example, that there are often competing national interests in play, even between liberal democracies with shared values and many common political interests. But there does not appear to be any in-principle reason why such protocols could not be developed and the fact that this might be difficult is no objection to attempting to do so. Moreover, since adherence to the protocols in question would consist, in so far as it is practicable, in ensuring compliance with some of the standard moral principles protecting privacy and confidentiality rights, such as probable cause/reasonable suspicion and use of judicial warrants, these two clusters would essentially consist of an extension of the law enforcement model to espionage conducted within and between these countries.

Further, such a process of clustering of liberal democratic states would be in accordance with the prospective principle of reciprocity; each of these nation-states would need to agree to, and actually comply with, the privacy respecting

protocols in question but each might be deterred from not doing so by the tit-for-tat procedure of the prospective principle.

What of authoritarian states known to be supporting international terrorism and/or engaging in hostile covert political operations, including espionage and cyber-espionage, for example China and North Korea?

In respect of authoritarian states of this kind, the retrospective principle of reciprocity reigns. Accordingly, there are few, if any constraints on intelligence-gathering and analysis, including cyber-espionage, if it is done in the service of a legitimate political interest such as national security.[15] Nevertheless, it is important to demarcate within such an authoritarian state between the government and its security agencies, on the one hand, and private citizens, on the other. Notwithstanding the applicability of the retrospective reciprocity principle, the need to respect the privacy rights of private citizens in authoritarian states remains; perhaps all the more so given these rights (and, for that matter, human rights in general) are routinely violated by their own governments.

So a stringent principle of discrimination* ought to govern espionage, including cyber-espionage, directed at authoritarian states. At the very least, the citizens of these states ought to be able to differentiate between morally justified infringements of the privacy and confidentiality rights of members of their government and its security agencies, on the one hand, and violations of their own privacy and confidentiality rights, on the other, and be justified in believing that whereas the former might be routine the latter are few and far between.

Conclusion

In this chapter I have framed intelligence activity as evidence-based truth-seeking epistemic activity (by contrast with, for instance, military activity or covert action), offered analyses of the key principles of discrimination, necessity and proportionality, and shown in general terms how they apply, or ought to apply, to national security intelligence activity. I have also introduced and analyzed a principle of reciprocity and argued that it needs to be introduced to govern espionage, in particular.

Notes

1 I use these terms more or less interchangeably in this chapter, although distinctions are sometimes made (Alexandra and Miller 2009).
2 See *National Security Strategy of the United States of America*, 2017, p. 4 "Second, we will *promote American prosperity*. We will rejuvenate the American economy for the benefit of American workers and companies", available at www.hsdl.org/?view&did=806478.
3 Or at least I assume that many, if not most, academics believe this. More specifically, I assume that most academics believe that intellectual work in universities is an end-in-itself *and* that it is in the service of further ends, for example. community well-being.
4 This point relates to the so-called intelligence cycle. See, for instance, Hulnick (2006).
5 See, for instance Walzer (2015).

6 See Mark Phythian in Omand and Phythian (2018, 85) for this kind of point and David Omand in same (91–2) for a response to it.
7 See, for instance, Walzer (2015).
8 See, for instance, Bellaby (2014), Quinlan (2007) and Omand and Phythian (2018, chap. 3).
9 There are various different versions and interpretations of the legal and moral principle of discrimination and, for that matter, of the legal and moral principles of precaution, necessity and proportionality. My concern is with these principles understood as *contested* moral principles. Accordingly, I take myself to have a significant degree of licence in formulating these principles.
10 See, for instance, Sorell (2018).
11 See, for instance, Miller (2009).
12 See Macnish (2017, Chap. 5) for an account of the ethical issues in this area.
13 An earlier version of this section appeared in Miller (2016a).
14 Reciprocity-based principles are related to, but distinct from, consent-based principles. In relation to the latter applied to espionage, see Pfaff and Tiel (2004).
15 There are important questions here concerning what counts as a legitimate purpose, particularly in the context of the blurring of the distinction between a political interest and an economic interest, for example China's cyber-theft operations. For reasons of space I cannot pursue these here.

References

Alexandra, Andrew, and Seumus Miller. 2009. *Ethics in Practice: Moral Theory and the Profession*. 1st edition. Sydney: University of New South Wales Press.

Anderson, David. 2016. *Report of the Bulk Powers Review*. London: HMSO. https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

Bellaby, Ross W. 2014. *The Ethics of Intelligence: A New Framework*. 1st edition. London; New York: Routledge.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1997. *Security: A New Framework for Analysis*. 1st edition. Boulder, CO: Lynne Rienner Publishers.

Green, Leslie C. 1993. *The Contemporary Law of Armed Conflict*. Manchester; Canada: Manchester University Press.

Hulnick, Arthur S. 2006. "What's Wrong with the Intelligence Cycle". *Intelligence and National Security* 21 (6): 959–79. https://doi.org/10.1080/02684520601046291.

Lazar, Seth. 2012. "Necessity in Self-Defense and War". *Philosophy & Public Affairs* 40 (1): 3–44. https://doi.org/10.1111/j.1088-4963.2012.01214.x.

Macnish, Kevin. 2017. *The Ethics of Surveillance: An Introduction*. 1st edition. London: New York: Routledge.

McDonald, Matt. 2008. "Securitization and the Construction of Security". *European Journal of International Relations* 14 (4): 563–87. https://doi.org/10.1177/1354066108097553.

Miller, Seumas. 2009. *Terrorism and Counter-Terrorism: Ethics and Liberal Democracy*. Blackwell. https://doi.org/10.1002/9781444302837.ch4.

———. 2010. *The Moral Foundations of Social Institutions: A Philosophical Study*. Cambridge; New York: Cambridge University Press.

———. 2016a. "Cyberattacks and 'Dirty Hands': Cyberwar, Cybercrime, or Covert Political Action?" In *Binary Bullets: The Ethics of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke, and Bradley J. Strawser, 228–50. New York: Oxford University Press.

www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190221072.001.0001/acprof-9780190221072.

———. 2016b. *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force*. New York: Oxford University Press.

———. 2021. "Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis". *Social Epistemology* 35.

Miller, Seumas, and John Blackler. 2016. *Ethical Issues in Policing*. 1st edition. London: Routledge.

Miller, Seumas, and Marcus Smith. 2021. *Biometrics, Ethics and Law*. Dordrecht: Springer.

Omand, David, and Mark Phythian. 2018. *Principled Spying: The Ethics of Secret Intelligence*. Washington, DC: Georgetown University Press.

Pfaff, Tony, and Jeffrey R. Tiel. 2004. "The Ethics of Espionage". *Journal of Military Ethics* 3 (1): 1–15. https://doi.org/10.1080/15027570310004447.

Quinlan, Michael. 2007. "Just Intelligence: Prolegomena to an Ethical Theory". *Intelligence and National Security* 22 (1): 1–13. https://doi.org/10.1080/02684520701200715.

Sorell, Tom. 2018. "Bulk Collection, Intrusion and Domination". In *Philosophy and Public Policy*, edited by Andrew I. Cohen, 39–60. London; New York: Rowman & Littlefield Publishers.

Walzer, Michael. 2015. *Just and Unjust Wars*. 5th edition. New York: Basic Books.

Williams, Michael C. 2003. "Words, Images, Enemies: Securitization and International Politics". *International Studies Quarterly* 47 (4): 511–31.