National security intelligence activity
a Philosophical analysis

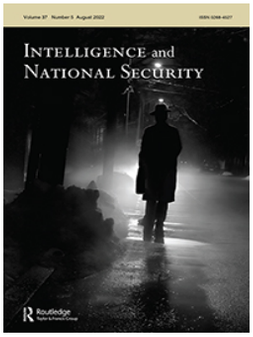
Miller, Seumas

DOI
10.1080/02684527.2022.2076329

Publication date
2022

Document Version
Final published version

Published in
Intelligence and National Security



Intelligence and National Security

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fint20

National security intelligence activity: a Philosophical analysis

Seumas Miller

To cite this article: Seumas Miller (2022): National security intelligence activity: a Philosophical analysis, Intelligence and National Security, DOI: 10.1080/02684527.2022.2076329

To link to this article: https://doi.org/10.1080/02684527.2022.2076329

Published online: 24 May 2022.

INTELLIGENCE AND NATIONAL SECURITY
https://doi.org/10.1080/02684527.2022.2076329

Routledge
Taylor & Francis Group

National security intelligence activity: a Philosophical analysis

Seumas Miller

ABSTRACT

This article provides philosophical analyses of some of the key notions involved in national security intelligence collection, analysis and dissemination. In Section 1, and relying on the intelligence studies literature, the notion of intelligence is characterized by means of an outline its main features or, at least, those features typically ascribed to it. In Section 2, an analysis of the notion, or rather inter-related set of notions, of knowledge (broadly understood) that lies at the heart of intelligence activity is provided. In Section 3, the focus shifts to the activity, or rather inter-related activities, of intelligence collection, analysis and dissemination and, in particular, the notion of joint epistemic action.

Philosophical analysis of fundamental concepts and theories used in national security intelligence activity has been minimal and, where it exists, largely limited to ethical issues, as in the application of the constitutive principles of Just War Theory to secret intelligence. On the other hand, in recent years the definition of intelligence in criminal justice and national security (including the military) has achieved a great deal of attention, albeit not by philosophers.[1] Yet the definition of intelligence remains unresolved. Moreover, a complete and correct one will not be offered here. Rather in this article an initial characterization of national security intelligence is offered (Section 1); that is, in the light of the national security intelligence literature, a list of the main features of national security intelligence are described. Moreover, the concept of intelligence is located in relation to cognate concepts, notably knowledge; in the parlance of philosophers, intelligence is an epistemic concept (from the ancient Greek word, 'episteme' meaning knowledge). It is suggested that ideally intelligence is knowledge, as Sherman Kent argued many year ago in his influential work,[2] albeit we need to keep in mind (as Kent did) the differences between, on the one hand, knowledge of existing conditions and of events that have already taken place and, on the other hand, predictions, and between descriptive knowledge and evaluations, as well as various other distinctions. Further, according to the characterization offered here, intelligence is a teleological concept (i.e., defined in terms of its end or purpose) and (relatedly) institutionally relative, (i.e., relative to some institutions). Accordingly, military intelligence is intelligence that serves the ends or purposes of military institutions; as such, it belongs to a different category than, say, police intelligence. In addition to this initial characterization of national security intelligence this article provides (Section 2) a philosophical analysis of the notion of knowledge or rather notions of knowledge, which it is argued, lie at the heart of national security intelligence activity. Propositional knowledge is distinguished from knowledge how and both from knowledge by acquaintance. These three categories of intelligence are then related to one another and applied to national security intelligence activity, it being clear that knowledge is a state or product that results from such activity (again, as Kent made clear[3]). In Section 3 the notion of joint epistemic action (and some related notions) is introduced and applied to national security collection, analysis and dissemination. National security intelligence activity is cooperative or joint in nature; indeed, it is a form of institutional activity and intelligence agencies

CONTACT Seumas Miller semiller@csu.edu.au

are a species of epistemic institution. Given this, important questions arise as to how intelligence officers could be morally responsible for the intelligence that the institutions that they work for provide to their political masters. Here the notion of collective moral responsibility and chains of institutional responsibility are salient.

Section 1: characterizing intelligence

There are a number of general points, some of which are fairly obvious and oft stated and which can serve to characterize, if not define, intelligence as a phenomenon. Note that we need to keep in mind the threefold distinction between intelligence as the informational, cognitive or epistemic product of intelligence activity, as opposed to the activity itself and the agent (whether an individual or organization[4]) of the activity.

First, the contexts in which such intelligence is collected and analyzed are adversarial. The adversaries are institutions often acting, at least in the modern world, in the service of nation-states. These institutions seek to access the secrets of their adversaries while preventing their adversaries from accessing their own secrets. Moreover, they engage in various forms of deception and disinformation against these adversaries. However, ultimately, they are acting, at least normatively speaking, in the service of the moral rights (specifically, *joint rights*[5]) of their citizens to a collective good,[6] namely, security. As such, intelligence activity is, or ought to be, ultimately directed to the realization of a collective good. That is, it is joint epistemic activity directed to a collective end which is a collective good (of which more in Section 3). Moreover, intelligence activity involves, or at least is implicated in, the exercise, or attempted exercise, of power,[7] influence and the like, albeit in a normative context (by virtue of citizens' joint moral right to the collective good of security which good ought to be the collective end of said activity). Thus, criminal justice intelligence officers are seeking to collect intelligence on criminal organizations in order to see to it that their members are charged, tried and incarcerated. For their part, these criminals are seeking to prevent this intelligence being collected. Again, the military intelligence officers of nation-state A at war with nation-state B, are collecting and analyzing intelligence on the enemy forces of B in order to facilitate their defeat on the battleground. For their part, the intelligence officers of B, firstly, are seeking to prevent this intelligence being collected and, secondly, collecting and analyzing intelligence on the armed forces of A (which intelligence collection activity the intelligence officers of A are seeking to prevent).

Second, given these adversarial contexts, inevitably secrecy is of the utmost important[8]; it is critical that information about police or military operations, methods, tactics, strategies and goals are kept secret if they are successfully to realize their institutional purposes (and, thereby, discharge their moral obligations to the citizenry to ensure their security). For if one side in these adversarial contexts is able to maintain secrecy while the other is not, then the latter will be hugely disadvantaged. This is, of course, not to deny that there is typically much that is common knowledge[9] between adversaries in these contexts. For instance, each side in a war typically knows that the other is trying to win the war, and has some knowledge of the opposing side's resources, and strategic and tactical options. Moreover, each side knows that the other side has access to knowledge that is in the public sphere. Nor is it to deny that the citizens have a right of access, at least in general terms, to information about what their intelligence agencies are doing in their name and in their interest.

But on this last point, what if the information is about the identity of their intelligence agency's own espionage agents, their tradecraft and their databases on foreign agents/activities? If, for instance, MI6 has an informant in the KGB, namely X, why does the British citizenry have a right to know this fact (as opposed to general fact such as MI6 exists and tries to have informants in the KGB)? Regarding the latter kind of information, from the fact that the citizens have a right to security and security agencies are established to provide for this security, it does not follow that the citizens necessarily have a right to *all* the information that the security agencies collect and all the tradecraft that they use in order to discharge their obligations to provide security to the citizens. Rather, citizens have a right to determine (via government) the morally-based constraints on security

agencies and the collective ends (collective goods) security agencies are to serve. Citizens also have a right to know via accountability mechanisms that security agencies are complying with these constraints and serving these ends. However, given, for instance, operational autonomy (see below), these rights of citizens are well short of a right to *all* the information the security agencies collect and all the tradecraft that they use. Note that it may be that no-one has a *moral* right to this information once it is no longer information that has any security implications; neither the citizens nor the members of the security agencies have this moral right. Therefore, it is information that, other things being equal, ought to be publicly available, including (potentially) to non-citizens. In short, it is not clear that information per se should have an owner. Of course, some of this information might have an owner, as in the case of personal information, trade secrets or intellectual property. However, intelligence per se is (largely) information and the only justification for keeping it secret is, ultimately, security; it is a means to an end and perhaps a fleeting means at that. For knowledge that is intelligence may have a relatively short shelf-life in part because it ceases to be of any use in respect of its security purpose and, therefore, no longer has any national security value.

Third, intelligence is in the service of kinetic activity, such as making arrests, bombing installations or waging war, and, therefore, needs to be actionable by the relevant decision-makers (police, military commanders or politicians, respectively). Accordingly, intelligence officers need to be responsive to decision-makers but also, if their intelligence is ultimately to be beneficial, somewhat independent of decision-makers so that it is evidence-based and not vitiated by political interference. Intelligence officers may even, at times, need to 'speak the truth to power' rather than tell their superiors what they want to hear. However, many intelligence agencies focussed on the epistemic activity of national security intelligence are also engaged in kinetic activity,[10] such as sabotage (including by way of cyber-attacks, as in the case of the Stuxnet virus), interference in elections, funding dissidents, cross border kidnappings, arming secessionists, assassinations. Moreover, some of their intelligence collection, analysis and communication is in the service of these latter covert operations. Accordingly, not all national security intelligence collected, analysed and communicated by national security intelligence agencies is in the service of kinetic activities to be conducted by other institutions, such as the military or the police. Nor is the distinction between the epistemic and the kinetic always clear-cut. For instance, some of 'intelligence' activities, such as disinformation and propaganda, are seemingly in part epistemic and in part kinetic.

Fourth, some distinction needs to be maintained between intelligence as 'raw data' and intelligence as the epistemic product of some process of analysis and evaluation according to different criteria, including the likelihood that it is true, its importance (assuming it is true), and (relatedly) the reliability of its source. Hence the distinction between collectors and analysts, but also the need for ongoing cooperation between the occupants of these different intelligence roles.

Fifth, in the light of the above-mentioned distinctions between collectors, analysts and decision-makers operating in an adversarial context, it makes sense to introduce *some* notion of an intelligence cycle[11] involving not only a one-way circular process in which intelligence is directed to be collected, analyzed and acted on by decision-makers who in turn direct further intelligence to be collected – doing so in part because of the actions of antagonists (including in response to the actions consequent on the decisions of one's own decision-makers). The process is not simply circular but also (at least ideally) two-way interactive at each of the points in the 'circle', as is the case between intelligence officers and decision-makers.

Sixth, intelligence can be categorized in various ways according to its source, mode of communication, content and potential use. For instance, regarding its potential use, intelligence can be categorized as strategic, tactical or operational. This latter set of distinctions can be seen in the light of the threefold distinction between the institutional, the macro and the micro levels. The institutional level refers to matters such as the purpose, structure, resources and culture of an intelligence agency, and its institutional relationships to, for instance, government or the military forces it serves. There is a further distinction between activities at the macro level (such as the design of a national intelligence strategy, the establishment of bulk databases by security agencies for national security

purposes) and those at the micro level (such as the conduct of a specific operation utilising data from a bulk database). Indeed, this threefold distinction may not be sufficient; perhaps there is a need for a fourfold or fivefold distinction. However, it serves to draw attention to different levels at which intelligence is used, including the political and the strategic at the higher levels, and the tactical and operational at the lower levels.

Intelligence can also be categorized (inter alia, according to its source and mode of existence) as human intelligence (HUMINT), signals intelligence (SIGINT), social media intelligence (SOCMINT), open source intelligence (OSINT), imagery intelligence (IMINT), and geospatial intelligence (GEOINT). In recent times various forms of electronic intelligence have emerged as of great importance, notably metadata (phone or email data other than content, notably the phone number of the caller and the receiver and the time and duration of call) in the context of end-to-end encryption impeding access to content. Moreover, OSINT and SOCMINT are increasingly important intelligence sources. Thus, intelligence agencies have increased their uses of data mining and analytics technologies, notably machine learning techniques and computer vision algorithms.

The content of intelligence is multifarious. Content can include discrete items of information, such as the name of a foreign agent, or larger fragments of epistemic material, such as. a list of associates, the strategic plan of the enemy. The content might be a fact, a formula, a map, an image, an opinion, an ideological claim, an expressed emotion, a video clip or a narrative about a sequence of events. Importantly, intelligence content is holistic. Any particular item of intelligence only has significance in the context of a larger, structure of intelligence content. Thus, the movement of troops within a nation-states own borders might constitute a national security problem for another nation-state or it might not depending on whether the state moving its troops was regarded as belligerent by virtue of its past actions, the troops were well armed, battle-prepared and large in number, and were moved close to the border with the other state.

Seventh, while the raw data collected by intelligence officers (whether human intelligence or electronic intelligence) consists of linguistic (spoken and written) and non-linguistic material such as images, videos, maps, diagrams, etc., once analyzed and disseminated to decision-makers it exists in large part in a form such that it is: (i) expressed or expressible in a language and, therefore, communicable; (ii) epistemic (or knowledge focused) and, as such, capable of being true or false, correct or incorrect, probable or improbable, evidence-based or not; (iii) stored somewhere, such as in an investigator's notebook or in a security organization's data bank, and; (iv) elements or fragments of some larger network or structure in terms of which any given single such item is judged to be at the very least 'of interest' and is, therefore, intelligible or potentially intelligible in terms of an intelligent officer's pre-existing theory, quasi-theory, general understanding or conceptual framework (call it a prior framework of understanding). Intelligence, therefore, can be thought of as in large part consisting of statements (individual or structured), or material expressible as statements, selected and analyzed in accordance with some pre-existing framework of understanding, stored in some information storage system and accessible only to those with the relevant security clearance.[12]

Intelligence that is stored is not necessarily 'in the heads' of intelligence officers or other personnel; indeed, if it is electronic intelligence as in recent times it often is, it may never have been 'in the head' of any member of the intelligence agency in which it is stored. However, such intelligence is, at least in principle, accessible to intelligence officers; if accessed it can be known to them. Such stored intelligence loosely corresponds to what Karl Popper refers to as the third world of objects[13] – the first world consisting of physical objects and the second world of mental objects. That is, the third world consists of abstract objects, albeit abstract objects that are physically embodied but also humanly constructed and invested with semantic properties (and, therefore, logical relations), e.g., the *content or knowledge contained within* a book in a library or an intelligence report in database, or a mathematical formula or an email.

Eighth, information and intelligence are closely related concepts. Both information and intelligence, at least in many of their forms, can be thought of as statements stored in some information system. Moreover, both information and intelligence, as we will use the terms in this article, are

epistemically evaluable, i.e., either true or false (albeit, perhaps unverifiable), correct or incorrect, accurate or inaccurate, or probable or improbable. However, neither information nor intelligence collected is *necessarily* true (or necessarily correct, accurate or probable) This is, of course, true of disinformation masquerading as bona fide intelligence and also of much 'raw' intelligence. But it is also true of intelligence that has been subjected to analysis and is well-evidenced. Finally, neither information nor intelligence necessarily has a good, let alone decisive, justification. Accordingly, neither information nor intelligence is necessarily knowledge. On the other hand, a piece of information or of intelligence might be true and might have a good and decisive justification; *some* information and *some* intelligence is knowledge.

Ninth, notwithstanding that information and intelligence are closely related concepts, they are not the same thing; specifically, intelligence is information, but information is not necessarily intelligence. For instance, the information from the surgeon that my ankle is broken is not necessarily intelligence, given the irrelevance, let us assume, of my medical condition to the activities of intelligence agencies. On the other hand, this information might be intelligence if, for instance, I am a fugitive whose whereabouts is being sought by an intelligence agency. In the context of criminal investigations,[14] intelligence is information that is utilized, actually or potentially: (i) to facilitate the outcome of specific criminal investigations, (for instance, to identify and apprehend the Yorkshire Ripper); (ii) in the day-to-day tasking and deployment of an organization's sub-units, (for instance, in a local police station or local area command unit) in response to crimes of particular types in particular locations, (for instance, violence at closing time outside certain late night venues on weekends) (tactical intelligence), or; (iii) in the long term planning of the organization's deployment of resources and its strategic response to crime trends (for instance, to home-grown terrorism) (strategic intelligence).

Tenth, notice that intelligence, whether it be criminal intelligence, market intelligence, or military intelligence is defined relative to some institutional purpose or function.[15] Police seek information for purposes of investigation, arrest, prosecution of criminals. That the information is sought in order to realize these kinds of purposes is what makes the information in question criminal intelligence. Likewise, members of military intelligence agencies seek information for the purposes of winning wars and battles and deterring military aggressors inter alia, and that the information is sought for these purposes makes it military intelligence. Again, corporations seek information on other corporations for purposes of gaining commercial advantage in a context market-based competition, and that the information is sought for these purposes makes it market intelligence.

Accordingly, we should accept a teleological (purpose-based) or functional account of intelligence; intelligence is, by definition, information or data (expressible as a statement or, more likely, structured set of statements) that is acquired for various institutional purposes. Moreover, intelligence is institutionally relative in that it is relative to the purposes of some institution. So military intelligence is a different category of intelligence from criminal intelligence because military institutions have a somewhat different institutional purpose than police organizations. That said, one and the same item of knowledge might be both an item of military intelligence and an item of criminal intelligence. Consider, for example the intelligence that Abū Bakr al-Baghdadi is engaged in war crimes. The fact that military intelligence and criminal intelligence are different categories of intelligence does not mean that a given piece of information might not belong to both categories.

If the primary purpose or function of an institution is knowledge (understood broadly in the sense of evidence-based understanding) then the institution is an *epistemic* institution. Thus universities, news organizations and, arguably, intelligence agencies are epistemic institutions.

What of national security intelligence; the collection, analysis and dissemination of which is, let us assume, the primary purpose of many intelligence agencies?[16] National security intelligence is sometimes collected and analysed by military organisations, sometimes by police organisations, but paradigmatically by intelligence agencies the institutional purpose of which is internal and/or external national security, e.g., the CIA, NSA, GCHQ, MI5, MI6, Mossad, RAW, ASIO etc. Accordingly, what makes information or other data collected by these agencies national security intelligence is that these

agencies collect and analyse this information in the service of national security – national security being their primary institutional purpose. This immediately raises the vexed question as to what national security is; after all, the content of the term 'national security' is notoriously ill-defined, indeterminate, shifting, open-ended and contestable. For instance, the US National Intelligence Strategy has as one of its purposes to promote liberal democracy, and the UK's has as one of its combating crime. Importantly, national security should not simply be understood as national interest, since the latter notion is very permissive and could license all manner of individual and collective rights violations. For instance, it might be in the national interest of a nation-state to increase its territory by invading a neighbouring nation-state. Perhaps Germany's invasion Poland was thought to be in Germany's national interest; perhaps the possible future Russian invasion of Ukraine might be thought to be in Russia's national interest. Again, it might be thought to be in the national interest of some nation-state to enslave a population, or to otherwise engage in widespread, serious rights' violations, to increase its own wealth. Historically, the slave trade was thought to be an economic imperative and, therefore, in the interest of, for instance, the United States during the 18th century. The Chinese incarceration of hundreds of thousands of Uighurs in oil and resources rich Xinjiang might be thought by members of the Chinese communist party to be in the national interest. However, let us assume that national security intelligence is intelligence pertaining to serious internal or external (direct or indirect) threats to the nation-state itself, or to one of its fundamental political, military, criminal justice or economic institutions, and that these threats might emanate from state or non-state actors, such as terrorist groups. So national security intelligence includes military intelligence, but also some criminal intelligence and economic intelligence, since the latter may have national security implications. Consider, for instance, intelligence on drug cartels destabilizing governments or on fighter aircraft being built by private companies. Note also that while national security threats (as opposed to safety threats) are necessarily posed by state or non-state (and, therefore, human) actors, the conditions under which these security threats emerge might have arisen as a result of other, including non-human, sources, such as pandemics, famines or water shortages consequent on climate change.

Section 2: knowledge and the aims of intelligence collection and analysis

Intelligence is, as we have seen, an epistemic notion and, ideally it consists of knowledge; that is, it is true or correct or accurate or probably true, or some such. Accordingly, intelligence officers aim at, or ought to aim at, knowledge (of which more below) and have associated traits of objectivity, a capacity for judgment in relation to what is important and what is not and relevant expertise, such as of a specific language, but also we able to work to a deadline.[17] Moreover, we have suggested that ultimately intelligence needs to be rendered (in large part) into a linguistic form. As such, ideally it will consist of so-called propositional knowledge.

Here we need to invoke the following traditional distinctions in relation to knowledge. There is knowledge in the sense of *knowledge-by-acquaintance*.[18] That is, knowing someone or something. For example, if two strangers have a face-to-face conversation then there is direct (physical and psychological) experience of one another; there is, therefore, knowledge-by-acquaintance. Such knowledge-by-acquaintance can have greater or lesser depth. Thus a man has knowledge-by-acquaintance of his wife of many years, and this knowledge has considerable depth as a consequence of the detailed background knowledge (based in large part on past encounters) which the man brings to bear on any particular face-to-face encounter with her. In a brief face-to-face conversation with her he will notice much that would be missed by a stranger. On the other hand, if the stranger is a well-trained, intelligence officer then he might notice things about her which her husband would miss. So, the intelligence officer's knowledge-by-acquaintance might also have depth, albeit of a less personal, more impersonal kind.

In addition to knowledge-by-acquaintance there is so-called *knowing-how*.[19] To know how to do something, such as to know how to ride a bike or to know how to interrogate a detainee, is in essence to possess a skill. Naturally, knowledge-how typically goes hand-in-glove with

knowledge by acquaintance. Knowing how to ride a bike, for example, presupposes direct experience of bikes (knowledge-by-acquaintance), knowing how to interrogate a detainee presupposes direct experience of detainees (knowledge-by-acquaintance), and so on. Moreover, knowledge-how facilitates knowledge-by-acquaintance. Thus an experienced and competent interrogator (someone with a high degree of knowledge-how to interrogate) may well quickly come to know a detainee (knowledge-by-acquaintance) at a level of depth which a novice interrogator would struggle to attain because, for example, the novice is unable to make the detainee feel at ease.

Finally, there is so-called *propositional knowledge*. This is knowledge that that some state of affairs obtains. Propositional knowledge is expressed in language by sentences with a subject and a predicate. For example, suppose an intelligence officer knows that his informant is reliable and the informant tells him that a man, X, is a courier for a terrorist group and regularly travels to a certain location, L. The officer infers that the leader of the terrorist group, Y, is probably residing at that location and, indeed Y is at L. The intelligence officer has *propositional* knowledge of the state of affairs that Y is at L, if the officer knows it and has expressed this knowledge in a sentence(s) of a language.

Note that whereas propositional knowledge is expressed in language, it is not necessarily expressed in a form accessible to others. Thus, the intelligence officer might know that Y is at L and express this thought to himself in a sentence, but the officer does not necessarily utter this sentence for others to hear it. He does not necessarily assert or *make a statement* (in the ordinary common-sense meaning of that term, as opposed to its more specialised meaning in a criminal justice context, such as to take the statement of a witness) expressing his propositional knowledge. A statement in the common sense meaning of that term (and, for that matter in the formal criminal justice sense) is something that is outwardly expressed; it is said out loud or put in writing, and does not merely remain in the realm of inner thought.

Propositional knowledge goes hand-in-glove with both knowledge-by-acquaintance and knowledge-how. Much knowledge-by-acquaintance is translated into explicit thought and, as such, is expressed in language (to oneself and, very often, also to others). Moreover, propositional knowledge, such as that acquired by the intelligence officer just mentioned, presuppose knowledge-how, as in the case of knowledge how to track down a terrorist.

On the other hand, propositional knowledge can facilitate, and give direction to, knowledge-by-acquaintance. Suppose on the basis of the above-mentioned officer's intelligence report, together with satellite images of Y walking around at location L, a special forces team is despatched to kill or capture Y. At the point where they confront Y face-to-face they will have knowledge by acquaintance.

Clearly intelligence officers need to have all three sorts of knowledge. They need to verify certain claims by direct observation (knowledge-by-acquaintance). They need to know how to do various things, including how to collect and analyse intelligence, such as how to interrogate a detainee (knowing-how). They also have to have, and to be able to obtain, propositional knowledge. Indeed, most of what they end up putting into print, for instance an intelligence report, is propositional knowledge (expressed in statements).

Consistent with the above made claim that national security intelligence activity is ultimately undertaken in the service of kinetic action undertaken by other agencies, I suggest, nevertheless, that the fundamental (proximate) *point* of intelligence collection and analysis is knowledge[20] and, more specifically, propositional knowledge expressed in statements – since such knowledge needs to be disseminated to others, notably decision-makers, and not 'left in the head' of the intelligence officer (let alone in the database of the intelligence agency). In short, intelligence officers *ought* to have the acquisition of knowledge as their principal aim or end. Accordingly, a necessary condition for being a good intelligence officer is that one aims at knowledge. So an otherwise highly skilled intelligence officer who did not have knowledge as his *overriding* aim, but rather a desire to, for instance, please her political masters, would not be a good intelligence officer. For example, the

highly skilled officer who, nevertheless, ignores counter-evidence when forced to choose between getting to the truth of the matter (and, thereby, coming to have knowledge) and providing confirmation of a view of her political masters is not a good intelligence officer.

We saw above that intelligence collection, analysis and dissemination is the means to a further end, namely kinetic action. Nevertheless, the acquisition of knowledge is *also* an end-in-itself for intelligence officers, notwithstanding the further requirement that the truths acquired be actionable. For 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. Rather truth is internally connected to intelligence activity. Thus, aiming at truth is aiming at truth as an end-in-itself. This is consistent with also aiming at truth as a means to some other further end, such as 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 a 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 antagonise their political masters (as in the case of many 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 above discussion. As we have just seen, whereas the primary institutional purpose of national security intelligence agencies is essentially epistemic, the realisation of this epistemic purpose serves a larger national security purpose only realizable by the kinetic activity of other institutions, such as the military. Accordingly, there is an institutional division of labour; the intelligence agency provides knowledge (or weaker epistemic goods) to the decision-makers, such as politicians or military or police 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 unduly influenced or otherwise undermined by the institutions which they serve, notably 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 override 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 to not engage in institutional overreach.

Thus far we have been using an unanalysed notion of knowledge and a somewhat loose one. In what follows we need to keep in mind a threefold distinction between intelligence, knowledge and certainty. Here we need to distinguish between knowledge and so-called intelligence, on the one hand, and knowledge and certainty on the other.

Knowledge is to be distinguished from intelligence in the sense of unanalysed 'information' – including unsubstantiated reports, hearsay and the like – that is collected by intelligence officers. Intelligence in this sense is more likely to be true than, for instance, blatant lies or ideology. However, intelligence is often unconfirmed; some intelligence is at best *prima facie* true. Intelligence may have some evidential backing, but even if so this backing might not be sufficiently strong to warrant it being believed.

It is also important to distinguish between knowledge and certainty. If someone has certainty then s/he cannot be mistaken. But of course there is very little that intelligence officers could not be mistaken about. This raises the issue of the degree of certainty; is the' intelligence' mere suspicion, probably true, true beyond reasonable doubt (a legal epistemic standard)? Here the notion of certainty in play is rational, as opposed to merely psychological, certainty. A psychotic who holds the entirely irrational belief that a harmless person is trying to kill him, nevertheless, might be psychologically certain of this falsehood. Rational certainty, by contrast, is the possession of reasons that provide grounds for believing that there is a very high probability that, for instance, the person walking around in a compound is Osama bin Laden. Psychological certainty (one's de facto psychological state of certainty) should, but often does not, mirror rational certainty (the psychological state of certainty one rationally *ought* to be in, given the evidence).

Roughly speaking, rational certainty exists on a continuum and the degree of psychological certainty one has ought to mirror this continuum and, in particular, reflect the degree of evidence for the belief in question. At one end of the spectrum there is no certainty or even belief. Thus an intelligence officer might have a suspicion based on knowledge of a person's motive; however, motive is far from sufficient to justify the belief that the person is lying. The officer's knowledge that the claim being made is not corroborated would increase the likelihood that the person is lying but not necessarily demonstrate that he is.

Let us now return to the matter of defining the notion of knowledge.[21] By definition, knowledge is at least true belief and, given that, as we saw above, the knowledge in question is propositional and expressed in a language, then knowledge is true, *stated* belief. If knowledge is at least true belief then an existing state of affairs, e.g., a dead body, is not a matter of knowledge until it, so to speak, 'enters the head' of someone and becomes the content of a belief. However, in order for a belief to be knowledge it must be a *true* belief; falsehoods are not knowledge. If someone believes that the world is flat or that $2 + 2 = 5$ then that person has a false belief and, therefore, does not have knowledge. So knowledge is at least true belief.

Truth is attained by the intelligence officer when she has a true belief that, for instance, Kim Philby is spying for the Soviets. However, truth in the sense of true belief is not sufficient. The intelligence officers need to be able to justify their true belief by recourse to evidence. Moreover this justification must consist in reasons, namely, good and (hopefully) decisive reasons; a bad reason is an unacceptable justification and a good reason is not necessarily sufficient to warrant true belief (there might be, for example, a countervailing good reason not to hold that belief). Hopefully, there will be a set of good reasons which cumulatively should constitute a decisive reason for the investigator's true belief. However, if this is not the case then decisions will need to be make on the basis of probabilities or (in the case of unacceptable outcomes) even possibilities.

Accordingly, the intelligence officers have as a goal *justified* true belief. But justified true belief is knowledge. So knowledge is the goal of the officer; specifically, propositional knowledge expressed in statements.

But why does the intelligence officer need a rational justification? Why is not the truth (true belief or, at least sincerely held true statement) sufficient? Firstly, speaking generally, beliefs need to be grounded in reasons if they are to be rationally held beliefs, as opposed to irrational or non-rational ones. Here reasons are the means by which we reliably determine which beliefs are true and which are false. An irrational person might accidentally possess true beliefs. But as Plato famously argued centuries ago in the *Theaetetus* and elsewhere, accidental true beliefs do not constitute knowledge. For example, taking a hallucinogenic drug might cause you to believe that Y is a terrorist, and Y might in fact be a terrorist. But your true belief that Y is a terrorist would not thereby constitute knowledge. This is because hallucinogenic drugs are not a reliable method (we are assuming) for arriving at the truth.

Indeed, not only should your true belief be based on the use of a reliable method, you should be competent in the use of that method on pain of it being mere luck that you arrived at the truth using that method.[22] Consider a novice intelligence officer who uses a method that is reliable if used by those competent in the use of the method, but who is himself incompetent in the use of the method, such as might be so in an instance of the use of a complex code to decipher the enemy's communications. Because the novice officer in question is incompetent under normal circumstances, he would not succeed in correctly deciphering the messages; rather his efforts would simply generate a meaningless string of letters. However, as a result of pure luck, on a particular occasion his incompetent use of the code delivers the same result as a competent use of the code would have delivered. Accordingly, while his misuse of the method delivered the correct result on this one occasion by sheer luck, arguably he does not know that this result is correct. Thus if his misuse of the method was discovered by the senior analyst, his result would not be believed.

The second reason a rational justification is required is because, institutionally speaking, the intelligence official needs to be able to justify his or her beliefs, his or her statements, to others and do so by means of the provision of good and decisive reasons. To the extent that intelligence officers know how to use reliable methods, in fact use these methods and, thereby, come to acquire true beliefs, then intelligence agencies embody a general principle of epistemic rationality.

Thus far we have largely been concerned with intelligence activity as, at least implicitly, the epistemic activity of individuals, as indeed much of it is. However, it is also a collective epistemic undertaking; it is joint epistemic action.

Section 3: joint epistemic action

National security intelligence activity is cooperative or joint in nature; indeed, it is a form of institutionalized epistemic activity. As such, it is a species of joint *epistemic* action. The activities of other security agencies are also forms of cooperative, institutional activity and, therefore, they are also species of joint action; however, they are predominantly species of joint *kinetic* activity. Accordingly, we can distinguish epistemic institutions, such as universities and national security intelligence agencies, from non-epistemic (especially kinetic) institutions, such as police and military institutions.

As suggested above, and argued in detail elsewhere,[23] security agencies are, or ought to be, established to realise collective ends which are collective goods, namely security (to which the relevant citizens have joint rights), and inevitably do so via joint action or, at least, multi-layered structures of joint action[24] and joint institutional mechanisms[25] (as will become clear below). Intelligence agencies are no exception. However, as already stated, the joint action which they perform is distinctive in that it is essentially joint *epistemic* action[26] (at least, in so far as the intelligence agencies in question do not engage in so-called covert action, such as sabotage, targeted killing and other kinetic activity). Importantly, joint epistemic action, as is the case with epistemic action more generally, while it is a necessary condition for kinetic action is not a sufficient condition. Rather, roughly speaking, it stands to kinetic action as beliefs stand to action (other than to mental actions, such as judgements), more generally. That is, it is mediated by affective and,

especially, conative (as opposed to cognitive) states, such as intentions, ends and the like. Hence, an intelligence report that Saddam Hussein is building WMDs does not in and of itself cause a kinetic response, such as war; rather the kinetic response depends on a decision to act (or not) based in part on the intelligence report but also and in part on some goal or end, such as to prevent Hussein from possessing an arsenal of WMDs. In short, knowledge does not in and of itself generate kinetic action.

This indirect relationship between knowledge and action and, therefore, between epistemic, including joint epistemic, action and kinetic action (and in turn the outcome of kinetic action) has important implications for our understanding of responsibility and, specifically, moral responsibility, as we shall see. Roughly speaking, intelligence officers have *some degree* of moral responsibility for the actions of their political masters, given that the latter make morally significant decisions based in part on intelligence reports. However, their political masters are, nevertheless, morally responsible for their own actions (and the reasonably foreseeable outcomes of their actions), notwithstanding their reliance on intelligence reports. Thus, President Bush and Prime Minister Blair were morally responsible for waging war against Saddam Hussein and, therefore, for the disastrous outcomes of that conflict. However, in so far as intelligence officers provided them with incorrect intelligence, they must also bear some responsibility. On the other hand, the latter responsibility of intelligence officers is diminished to the extent that the intelligence they provided, namely that there was insufficient evidence that Hussein was developing WMDs, was ignored.

The notion of joint action is a familiar one in the philosophical literature.[27] An example of a joint action is two people lifting a table. Moreover, we can distinguish between epistemic actions and non-epistemic, notably kinetic actions. Roughly speaking, epistemic actions are actions directed to an epistemic end, such as knowledge. An example of an epistemic action is an intelligence officer deciphering a coded message. Elsewhere I have argued that these two notions can be brought together to yield the notion of joint epistemic action and I have provided a relational individualist analysis of joint epistemic actions.[28] An example of a joint epistemic action is a team of intelligence officers jointly breaking a code.

Joint epistemic actions involve two or more persons jointly pursuing a common or collective goal or end.[29] Consider, for example, members of a counter-terrorist national security task force identifying, surveilling and, potentially, arresting suspected terrorists. Each participant involved in a particular operation intentionally does his or her epistemic part. For instance, an intelligence analyst identifies person X as a potential terrorist and a surveillance team conducts surveillance on X. On the basis of the information gained, the commander decides to use an undercover officer to establish a relationship with X. Finally, on the basis of evidence gained by the undercover officer, X is arrested by uniformed police officers (since, let us assume, the members of the national security task force in question do not have the legal power to effect arrests). Moreover, there is interdependence among the epistemic actions of each participant; each believes (or at least hopes) that the others will do their parts and, indeed, relies on at least some of the others to do their part if the shared epistemic end is to be realised. Moreover, there is interdependence between the epistemic end (to determine whether or not X is a terrorist) and the kinetic end (to arrest X, if he proves to be a terrorist). Further, there is typically interdependence with respect to the possession of the epistemic end. Since no single participant could realise the ultimate end on their own (or could only do so with difficulty) each only has the end if the others do. Finally, it is a matter of mutual true belief among participants that each has the (interdependent) end and beliefs in question. So each has these true beliefs, believes the others have them and that they believe he or she has them, and so on.[30]

There are a couple of points to notice about joint epistemic action on this account. First, while each participant has beliefs with respect to the actions of other participants, no participant *necessarily* has any intentions with respect to the actions of others. Rather each only necessarily has intentions with respect to their own actions. That said, such intentions with respect to the actions of others *might* be present in some cases, such as those involving authority relations between participants. A superior might issue a direct order to a subordinate to do their part in some joint epistemic action and in issuing the order also intend that the subordinate perform the act in

question. Second, joint epistemic action typically involves mental acts[31] such as judgments, and behavioural actions, such as communicating and physical evidence gathering. I am assuming that what makes an action an epistemic action is that its goal or end is epistemic and that this point applies both to individual and joint epistemic actions.

Elsewhere I have introduced and analysed three notions that are derived from the core notion of a joint epistemic actions. There three derived notions can be used to analyse more complex forms of joint epistemic activity, including at the macro or organisational level, engaged in by institutional actors in epistemic institutions, including by intelligence officers in intelligence agencies. In short, these notions are in part constitutive of the core activity of epistemic institutions, such as intelligence agencies. The notions in question are joint institutional mechanism (epistemic), multi-layered structure of joint epistemic actions, and chain of institutional responsibility. Let me now elaborate on each of these.

Joint institutional mechanisms (epistemic)

Joint institutional mechanisms[32] consist of: (a) a complex of differentiated but interlocking actions (the input to the mechanism); (b) the result of the performance of those actions (the output of the mechanism), and; (c) the mechanism itself. Thus, a given agent might vote for a candidate. He will do so only if others also vote. But further to this, there is the action of the candidates, namely, that they present themselves as candidates. That they present themselves as candidates is (in part) constitutive of the input to the voting mechanism. Voters vote *for candidates*. So, there is interlocking and differentiated action (the input). Further there is some result (as opposed to consequence) of the joint action; the joint action consisting of the actions of putting oneself forward as a candidate and of the actions of voting. The result is that some candidate, say, Jones is voted in (the output). That there is a result is (in part) constitutive of the mechanism. That to receive the greatest number of votes is to be voted in, is (in part) constitutive of the voting mechanism. Moreover, that Jones is voted in is not a collective end of all the voters. (Although it is a collective end of those who voted for Jones.) However, that the one who gets the most votes – whoever that happens to be – is voted in, is a collective end of all the voters.

Some joint institutional mechanisms are essentially epistemic in character since the output is an epistemic state, namely knowledge.[33] Moreover, this knowledge output can be stored in a database and rendered accessible to relevant members of the epistemic institution in question; indeed, this knowledge output probably itself have relied in part on pre-existing knowledge stored in a database. Consider an intelligence officer using a profiling technique to identify security personnel in the police and armed forces who might be sympathetic to extremist right wing groups and, as a consequence, compromising operations targeting these groups. He first constructs a profile of such a person; for instance, someone who expresses relevant extremist views, associates with known members of these groups, and has had complaints from members of relevant vulnerable populations. At this stage the officer uses a search engine to search the data base for personnel that fit this profile. Eventually, a number of personnel are identified as fitting the profile (say, John Smith, Peter Jones and Harry Brown) and these become targets of further scrutiny. This profiling process is the operation of a joint institutional mechanism. First, it relies on the differentiated, but interlocking, actions of a number of intelligence officers, including those who initially stored the old information from which the new information is derived, and the officer who inserted the profile into the search engine. Moreover, as is the case with most joint institutional mechanisms, this profiling process is repeatable and repeated; different profiles can be and are searched for. Second, the new information, namely, that Smith, Jones and Brown fit the profile, is the resultant action; it is derived by means of the profiling mechanism from the inputs of the profile in conjunction with the stored data. However, that Smith, Jones and Brown fit a certain profile is not in itself part of the profiling mechanism per se. Third, there is the profiling mechanism itself.

The resultant action of the use of the profiling mechanism is akin to the resultant action of the use of a voting system. As with the voting case, at one level of description identifying Smith, Jones and Brown. was an intentional action; it was intended that the persons who fits this profile be identified. (This is akin to the manner in which it was intended that the person with the most votes win the election in the voting scenario.) At another level of description, it was not intended; it was not intended or known that Smith, Jones and Brown, in particular, would fit the profile. (This is akin to the manner in which it was not intended by all the voters that Jones win the election in the voting scenario.)

The joint institutional mechanisms (epistemic) used in intelligence activity are embedded in intelligence organisations whose members conduct individual and joint epistemic action. How are we to understand this organisational action?

Multi-layered structures of joint epistemic action

Organizational action typically consists in large part of, what elsewhere I have termed, a *multi-layered structure of joint actions*.[34] One illustration of the notion of a multi-layered structure of joint actions in a kinetic institution is an armed force fighting a battle. Suppose at an organizational level a number of joint actions ('actions') are severally necessary and jointly sufficient to achieve some collective end. Consider an army fighting a battle. Here the 'action' of the mortar squad destroying enemy gun emplacements, the 'action' of the flight of military planes providing air cover, and the 'action' of the infantry platoon taking and holding the ground might be severally necessary and jointly sufficient to achieve the collective end of defeating the enemy; as such, these 'actions' taken together constitute a joint action. Call each of these 'actions' level-two 'actions', and the joint action that they constitute a level-two joint action. From the perspective of the collective end of defeating the enemy, each of these level-two 'actions' is an individual action that is a component of a (level-two) joint action: the joint action directed to the collective end of defeating the enemy.

However, each of these level-two 'actions' is already in itself a joint action with component individual actions; and these component individual actions are severally necessary and jointly sufficient for the performance of some collective end. Thus, the individual members of the mortar squad jointly operate the mortar to realize the collective end of destroying enemy gun emplacements. Each pilot, jointly with the other pilots, strafes enemy soldiers to realize the collective end of providing air cover for their advancing foot soldiers. Further, the set of foot soldiers jointly advance to take and hold the ground vacated by the members of the retreating enemy force.

At level one there are individual actions directed to three distinct collective ends: the collective ends of (respectively) destroying gun emplacements, providing air cover, and taking and holding ground. So, at level one there are three joint actions, namely, the members of the mortar squad destroying gun emplacements, the members of the flight of planes providing air cover, and the members of the infantry taking and holding ground. However, taken together these three joint actions constitute a single level-two joint action. The collective end of this level-two joint action is to defeat the enemy; and from the perspective of this level-two joint action, and its collective end, these constitutive actions are (level-two) individual actions.

Importantly for our purposes here there are multi-layered structures of joint *epistemic* action and these are characteristic of epistemic institutions such as intelligence agencies. Consider a number of intelligence agencies focused on a terrorist group, T, in a foreign country as their target. The intelligence to be collected includes the identities, locations and movements of the senior leadership of T and of their IED (improvised explosive devices) engineers. The goal is to degrade the capacity of T to engage in a terrorist campaign reliant in large part on IEDs. Assume the initial direction has come from the military high command and there is a military command and control group overseeing the entire operation. In relation to the intelligence dimension, there is a military intelligence agency involved which is utilising some of its HUMINT collectors, (who are relying on informants within T and overt sources, e.g., refugees), intelligence analysts, and a team of interrogators of already detained

members of T. Moreover, there is a separate SIGINT agency involved. In addition, special forces are part of the operation since they are the ones to conduct kinetic action on the basis on the intelligence gained, such as to capture or kill the identified and located members of T.

At level one, so to speak, there is the military intelligence agency (comprised of collectors, analysts and interrogators) engaged in joint epistemic actions (given the necessary division between interrogators, on the one hand, and the intelligence collectors and analysts, on the other). In addition, there is the joint epistemic action performed by members of the SIGINT agency. So, there are three main joint epistemic actions corresponding to the three teams: HUMINT collectors/analysts; interrogators; SIGINT collectors/analysts. The collective end of each of these joint epistemic actions is *some fragment* of the required knowledge of the identities, locations and movements of the key members of T in question. The intelligence reports provided by each of these three intelligence groups (as a result of their respective level one joint epistemic actions) is evaluated and integrated by a fourth team of intelligence officers and rendered into an intelligence report for dissemination to the command and control group. This report specifies the names, descriptions, locations, movements and so on of the members of T to be killed by the special forces group. The epistemic work of integration and evaluation by the fourth group of intelligence officers of the various fragments of knowledge provided by the other three groups is a fourth (level one) joint epistemic task; its collective end is knowledge of the identities, locations and movements of the key members of T in question. However, this integrative epistemic work and the derived report is reliant on the initial epistemic work of the other three intelligence groups. Therefore, the *four* joint epistemic actions *taken together* are constitutive of a single *level two* joint epistemic action, namely, the level two joint epistemic action directed towards the collective end of knowledge of the identities, locations and movements of the key members of T in question. It follows that when each of the four level one joint epistemic actions is successfully performed then the level two joint epistemic action is successfully performed. That is, a complete and correct report is prepared and able to be disseminated to the command and control group who direct the special forces accordingly.

Chains of institutional responsibility

In institutional arrangements such as the one in question, there is a segregation of sequentially performed roles (and associated responsibilities), (e.g., between members of the intelligence agencies, members of the command and control group who receive this intelligence (the decision makers) and members of the special forces group who directed by the command and control group to act on this intelligence). While each of these three groups performs a joint action (and in the case of the members of the various intelligence groups, a multi-layered structure of joint epistemic actions), nevertheless, there is a common end (collective end), (e.g., degrading of T) to which each of these prior joint actions are directed, at least under some description (e.g., kill *or* capture key members); there is what I have referred to elsewhere as a 'chain of institutional responsibility'.[35] In chains of institutional responsibility: (i) each participant (or group of participants) aims at the collective end constitutive of their particular institutional role, e.g., that of member of the HUMINT intelligence team; (ii) the occupants of any given constitutive role (the links in the chain) perform their role-based actions sequentially and interdependently with the actions of the occupants of the other roles, e.g., the actions of the intelligence team are performed prior to actions of the special forces group, and; (iii) in doing so, at least potentially, all or most of the participants aim (or should be aiming) at the ultimate collective end under some description (e.g., degrading T) that is an end further to that which might be definitive of their particular role. Moreover, all the participants (at least, in principle) share in the *collective responsibility*[36] for the realization of this end (or the failure to realize this end, as the case may be).

Notice also that chains of institutional responsibility might involve multi-layered structures of joint epistemic action and joint institutional mechanisms, as is the case in our example. The example obviously involves a multi-layered structure of joint epistemic action; it is the very same example as

the one used to illustrate this in the earlier sub-section. However, less obviously, it also involves a joint institutional mechanism. For while the outcome of the operation was known in advance under the description (let us assume) kill members of T, it was not known who these individuals in fact were. And, indeed, conceivably the members of the intelligence teams might not have been told that the persons who they identify as being members of T are to be shot dead (as opposed to, for example, captured and interrogated). For their part, the members of the special forces team might know that they are to shoot dead a number of persons who are members of T but they do not know who these individuals are in advance of the work of the members of the intelligence team. Indeed, when they shoot these individuals dead, they are largely taking it on trust that they are in fact members of T and, in any case, they are doing so under direct orders from the command and control group. Notice further that the killing of the members of T is, therefore, an exercise of a joint ability[37] of the members of the intelligence team, the members of the command and control group and the members of the special forces group since this outcome could not be achieved by the members of any one of these three group acting without the cooperation of the members of the other two groups; rather the joint action of the members of each of the three groups is a necessary condition for this outcome.

The significance of these analyses of national security intelligence activity in terms of the notions of joint epistemic action, multi-layered structures of joint epistemic action, joint institutional mechanism (epistemic) and chains of institutional responsibility is threefold. Firstly, if correct, these analyses provide conceptual illumination of various salient, indeed dominant, structural forms of national security intelligence activity. Moreover, since these institutional structural forms are epistemic in character (being species of joint epistemic action), they display the inherently cooperative, epistemic nature of national security intelligence agencies; that is, they reveal national security intelligence agencies to be epistemic institutions. Secondly, these analyses display how individual and collective responsibility (including, in the case of morally significant activity, collective moral responsibility) for intelligence activity might be ascribed. That is, each member of a team is individually responsible for his or her individual epistemic contribution while the members of the team can, at least in principle, be held jointly responsible for the final intelligence product and, in the case of joint institutional mechanisms, this can be joint responsible notwithstanding that the content of this epistemic product was not predictable and might not even be known by many of those contributing to it. That said, the often very indirect and minimal epistemic contribution of a single intelligence officer to a final intelligence product also reveals very significant limitations on the ascription of individual responsibility for such products. For it is likely that no single individual is fully responsible for the intelligence product, even if all share some responsibility for it, albeit some made a greater epistemic contribution than others. Again, some individual may have severely diminished institutional (and to that extent, therefore, moral) responsibility relative to others. For instance, other things being equal lower echelon officers might have less institutionally-based responsibility than their superiors, notwithstanding the possibly greater epistemic contribution of these lower echelon officers.[38] Thirdly, it displays how collective moral responsibility for joint epistemic action might be implicated in the responsibility for kinetic actions and the outcomes of kinetic actions. Let us assume that the individual members of a HUMINT intelligence team were collectively (i.e., jointly) morally responsible for wrongly identifying someone as a member of T and the person in question, although innocent, was shot dead by the special forces group. Presumably, the members of the intelligence team would have some degree of collective moral responsibility for the death of the innocent person, notwithstanding that it was the members of the special forces group who shot him dead.[39]

Section 4: conclusion

In this article philosophical analyses of some of the key notions involved in national security intelligence collection, analysis and dissemination have been provided. In Section 1, and relying on the intelligence studies literature, the notion of intelligence has been characterized by means of an outline its main features or, at least, those features typically ascribed to it. In Section 2, intelligence activity has been characterized by recourse to, firstly, a well-known analysis of the

notion of propositional knowledge in terms of true belief based on the competent use of a reliable method and, secondly, the familiar distinctions between propositional knowledge, knowledge by acquaintance and knowledge how. In Section 3, the notion of joint epistemic action, and related notions of multi-layered structures of joint epistemic action, joint institutional mechanism (epistemic) and chains of institutional responsibility have been used to characterize various institutional structural forms of intelligence activity and their relationship to kinetic action. These notions have inter alia displayed the inherently cooperative epistemic nature of national security intelligence agencies; that is, they reveal these agencies to be epistemic institutions. They have also revealed how individual and collective moral responsibility can, at least in principle, be ascribed to intelligence officers engaged in intelligence activity (but also the limitations of such ascriptions).

Notes

1. Breakspear, "A New Definition of Intelligence," Marrin, "Evaluating Intelligence Theories," Gill, "The Way Ahead in Explaining Intelligence Organization and Process"; Stout and Warner, "Intelligence Is as Intelligence Does"; Barnea, "Strategic Intelligence."
2. Kent, *Strategic Intelligence for American World Policy*, Ch. 1.
3. Ibid. Ch. 9.
4. Ibid. Ch. 5.
5. Miller, *The Moral Foundations of Social Institutions: A Philosophical Study*, 66-76; Miller, *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force*, Ch. 3.
6. Miller, *The Moral Foundations of Social Institutions: A Philosophical Study*, 66-76.
7. Miller, *Institutional Corruption: A Study in Applied Philosophy*, Ch. 2; Phythian, *Understanding the Intelligence Cycle*.
8. Bok, *Secrets: On the Ethics of Concealment and Revelation*.
9. Smith, *Mutual Knowledge*.
10. Stout and Warner, "Intelligence Is as Intelligence Does."
11. Treverton, *Reshaping National Intelligence for an Age of Information*; Phythian, *Understanding the Intelligence Cycle*.
12. Miller and Gordon, *Investigative Ethics: Ethics for Police Detectives and Criminal Investigators*.
13. Popper, *Objective Knowledge*, Ch. 4.
14. Ibid.
15. Miller, "Rethinking the Just Intelligence of National Security Intelligence Collection and Analysis."
16. Ibid.
17. Kent, *Strategic Intelligence for American World Policy*, 74.
18. Russell, *On Denoting*.
19. Ryle, *Concept of Mind*; Cath, "Knowing How"; Miller, "Joint Abilities, Joint Know-How and Collective Knowledge."
20. Miller and Gordon, *Investigative Ethics: Ethics for Police Detectives and Criminal Investigators*; Pili, "Intelligence and Social Epistemology," Miller, "Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis."
21. Moser, *Knowledge and Evidence*.
22. Sosa, *judgment and Agency*.
23. See above 5. 3.
24. Miller, *Social Action: A Teleological Account*, 173-179; Miller, *The Moral Foundations of Social Institutions: A Philosophical Study*, 47-52.
25. Ibid.
26. Miller, "Joint Epistemic Action: Some Applications"; Pili, "Intelligence and Social Epistemology."
27. Miller, "Joint Action"; Miller, *Social Action: A Teleological Account*, Ch. 2; Bratman, "Shared Intention."
28. Miller, "Joint Epistemic Action and Collective Moral Responsibility"; Miller, "Joint Epistemic Action: Some Applications."
29. Fallis, "Collective Epistemic Goals," Miller, "Collective Responsibility and Information and Communication Technology," Miller, "Joint Epistemic Action and Collective Moral Responsibility," Miller, "Joint Epistemic Action: Some Applications," Pili, "Intelligence and Social Epistemology."
30. See above 9.
31. Geach, *Mental Acts*.
32. Miller, "Joint Action," Miller, *Social Action: A Teleological Account*, 174-179; Miller, *The Moral Foundations of Social Institutions: A Philosophical Study*, 50-52.
33. Miller, "Joint Epistemic Action: Some Applications."

34. Miller, "Joint Action," Miller, *Social Action: A Teleological Account*, 173-174; Miller, *The Moral Foundations of Social Institutions: A Philosophical Study*, 47-50.
35. Miller, "Police Detectives, Criminal Investigations and Collective Moral Responsibility," Miller, *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force*, Ch. 5.
36. Miller, "Collective Moral Responsibility: An Individualist Account," Miller, "Joint Epistemic Action and Collective Moral Responsibility."
37. Miller, "Joint Abilities, Joint Know-How and Collective Knowledge."
38. See above 36.
39. Miller, *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force*, Ch. 5.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

European Research Council Advanced Grant (GTCMR) on counter-terrorism ethics - Principal Investigator Seumas Miller; Australian Research Council Discovery Grant on national security intelligence ethics –1st Chief Investigator Seumas Miller

Notes on contributor

Seumas Miller holds academic appointments at Charles Sturt University, the University of Oxford and TU Delft. He was Foundation Director of the ARC Special Research Centre in Applied Philosophy and Public Ethics and the Principal Investigator on an ERC Advanced Grant on counter-terrorism ethics. He is the author of over 250 academic articles and 22 books, including Shooting to Kill: The Ethics of Military and Police Use of Lethal Force (Oxford University Press, 2016 – open access) and Institutional Corruption (Cambridge University Press, 2017). He is co-editor (with Mitt Regan and Patrick Walsh of National Security Intelligence and Ethics (Routledge, 2021 – open access).

ORCID

Seumas Miller http://orcid.org/0000-0002-4851-3177

Bibliography

Barnea, A. "Strategic Intelligence: A Concentrated and Diffused Intelligence Model." *Intelligence and National Security* 35, no. 5 (2020): 701–716. doi:10.1080/02684527.2020.1747004.
Bellaby, D. *Ethics of Intelligence*. London: Routledge, 2014.
Bok, S. *Secrets: On the Ethics of Concealment and Revelation*. New York: Pantheon Books, 1982.
Bratman, M. E. "Shared Intention." *Ethics* 104, no. 1 (1993): 97–113. doi:10.1086/293577.
Breakspear, A. "A New Definition of Intelligence." *Intelligence and National Security* 28, no. 5 (2013): 678–693. doi:10.1080/02684527.2012.699285.
Cath, Y. "Knowing How." *Analysis* 79, no. 3 (2019): 487–503. doi:10.1093/analys/anz027.
Fabre, C. *Spying through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence*. Oxford: Oxford University Press, 2022.
Fallis, D. "Collective Epistemic Goals." *Social Epistemology* 21, no. 3 (2007): 267–280. doi:10.1080/02691720701674106.
Geach, P. *Mental Acts*. London: Routledge and Kegan Paul, 1957.
Gill, P. "The Way Ahead in Explaining Intelligence Organization and Process." *Intelligence and National Security* 33, no. 4 (2018): 574–586. doi:10.1080/02684527.2018.1452566.
Henschke, A., S. Miller, P. Walsh, and R. Bradbury. *Just Intelligence Institutions*. London: Routledge, 2022.
Kent, S. *Strategic Intelligence for American World Policy*. Princeton, N.J: Princeton University Press, 2015.
Marrin, S. "Evaluating Intelligence Theories: Current State of Play." *Intelligence and National Security* 33, no. 4 (2018): 479–490. doi:10.1080/02684527.2018.1452567.
Miller, S. "Joint Action." *Philosophical Papers* 21, no. 3 (1992): 275–297. doi:10.1080/05568649209506386.
Miller, S. *Social Action: A Teleological Account*. New York: Cambridge University Press, 2001.
Miller, S. "Collective Moral Responsibility: An Individualist Account." *Midwest Studies in Philosophy* 30, no. 1 (2006): 176–193. doi:10.1111/j.1475-4975.2006.00134.x.

Miller, S. "Collective Responsibility and Information and Communication Technology." In *Information Technology and Moral Philosophy, by Jeroen van Den. Hoven and John Weckert*, pp. 226-250. Cambridge: Cambridge University Press, 2008.
Miller, S. *The Moral Foundations of Social Institutions: A Philosophical Study*. New York: Cambridge University Press, 2010.
Miller, S., and I. Gordon. *Investigative Ethics: Ethics for Police Detectives and Criminal Investigators*. London: Wiley-Blackwell, 2014.
Miller, S. "Police Detectives, Criminal Investigations and Collective Moral Responsibility." *Criminal Justice Ethics* 33, no. 1 (2014): 21–39. doi:10.1080/0731129x.2014.906094.
Miller, S. "Joint Epistemic Action and Collective Moral Responsibility." *Social Epistemology* 29, no. 3 (2015): 280–302. doi:10.1080/02691728.2014.971908.
Miller, S. *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force*. New York: Oxford University Press, 2016.
Miller, S. *Institutional Corruption: A Study in Applied Philosophy*. New York: Cambridge University Press, 2017.
Miller, S. "Joint Epistemic Action: Some Applications." *Journal of Applied Philosophy* 35, no. 2 (2018): 300–318. doi:10.1111/japp.12197.
Miller, S. "Joint Abilities, Joint Know-how and Collective Knowledge." *Social Epistemology* 34, no. 3 (2019): 197–212. doi:10.1080/02691728.2019.1677799.
Miller, S., R. Mitt, and P. Walsh, eds. *National Security Intelligence and Ethics*. London: Routledge, 2021.
Miller, S. "Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis: The Principles of Discrimination, Necessity, Proportionality and Reciprocity." *Social Epistemology* 35, no. 3 (2021a): 211–231. doi:10.1080/02691728.2020.1855484.
Moser, P. K. *Knowledge and Evidence*. Cambridge: Cambridge University Press, 1989.
Omand, D., and M. Phythian. *Principled Spying*. Oxford: Oxford University Press, 2018.
Perry, D. *Partly Cloudy: Ethics in War, Espionage, Covert Action and Interrogation*. 2nd ed. Lanham, MD.: Rowman and Littlefield, 2016.
Phythian, M., ed. *Understanding the Intelligence Cycle*. Abingdon: Routledge, 2013.
Pili, G. "Intelligence and Social Epistemology - toward a Social Epistemological Theory of Intelligence." *Social Epistemology* 33, no. 6 (2019): 574–592. doi:10.1080/02691728.2019.1658823.
Popper, K. *Objective Knowledge*. Oxford: Clarendon Press, 1972.
Russell, B. *On Denoting*. Oxford: Blackwell, 1905.
Ryle, G. *The Concept of Mind*. London: Hutchinson & Co, 1949.
Smith, N. V. *Mutual Knowledge*. London: Academic Press, 1982.
Sosa, E. *Judgment and Agency*. Oxford: Oxford University Press, 2015.
Stout, M., and M. Warner. "Intelligence Is as Intelligence Does." *Intelligence and National Security* 33, no. 4 (2018): 517–526. doi:10.1080/02684527.2018.1452593.
Treverton, G. F. *Reshaping National Intelligence for an Age of Information*. Cambridge: Cambridge University Press, 2001.