# Technology in Espionage and Counterintelligence: Some Cautionary Lessons from Armed Conflict

*Alex Leveringhaus*

In her latest book, *Spying through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence*, Cécile Fabre discusses the ethical issues arising in the realms of espionage and counterintelligence (E-CI).[1] Wide-ranging in its analysis, Fabre's work also deals with the role of technical intelligence (TECHINT)[2] in E-CI. According to Fabre, TECHINT, which falls into several subcategories, should be differentiated from human intelligence (HUMINT).[3] HUMINT refers to intelligence obtained from or by a human asset, while TECHINT denotes that information is obtained via technological means, such as a bug, a spy satellite, or a computer algorithm. As Fabre's examples make clear, however, TECHINT relies on some human input; that is, there still must be a person planting a bug, designing and launching a spy satellite, or writing the code for an algorithm. This is a crucial clarification—indeed I would go even further and offer an important ethical distinction between direct and indirect human involvement in E-CI. For TECHINT, human involvement is, in the field of operations, indirect because relevant spy technologies mediate between intelligence officials and their (human) targets. Yet in the case of HUMINT, relations and interactions between relevant categories of individuals (agents, assets, targets) are direct and largely technologically unmediated. Ultimately, despite the practical

**Alex Leveringhaus**, University of Surrey, Guildford, England (a.c.leveringhaus@surrey.ac.uk)

*Ethics & International Affairs*, 37, no. 2 (2023), pp. 147–160.

doi:10.1017/S0892679423000199

differences I add here, for Fabre there are no *morally* deep salient differences between HUMINT and TECHINT, with the potential exception of cyber intelligence, which she rightly thinks raises separate normative issues.

This essay seeks to critically (yet sympathetically) probe Fabre's main contention that there are no morally deep differences between HUMINT and TECHINT. In particular, the main goal of this essay is to problematize the ethics around TECHINT and show that TECHINT, like many other forms of technology deployed in normatively murky, high-risk domains, is morally ambiguous. On the one hand, the essay argues that compared to HUMINT, TECHINT can, as Fabre's work makes clear, be morally desirable. Indeed, there might be circumstances where reliance on TECHINT, rather than HUMINT, is not just morally permissible but also mandatory. On the other hand, as Fabre's work also shows, the proliferation of technologies that enable TECHINT should make us queasy. This is because TECHINT does not merely act as a like-for-like replacement of HUMINT. Rather, the availability of increasingly sophisticated spy technologies has the capacity to transform practices of E-CI beyond what has hitherto been possible via HUMINT. I argue that this opens the potential for (some) morally relevant differences between TECHINT and HUMINT.

These brief observations on the transformative capability of spy technology raise broader questions about how analytical philosophers (Fabre and myself included) can best theorize the role of technology in politics and society moving forward. This is, in mainstream political theory and philosophy, still a niche topic. To make some headway on this issue in the context of TECHINT, the essay draws on insights from a related area where there has recently been a nascent philosophical discussion of the impact of technology. This is the area of just war theory and armed conflict. More precisely, I argue that the rise of cyber capabilities, remote-controlled-weapons platforms, and "autonomous" weaponry, as well as, more broadly, the centrality of "precision weaponry," in recent military campaigns yields some valuable insights for TECHINT.

Before I explore the analogy between the deployment of TECHINT and the use of certain weapons technologies in armed conflict, it is useful to raise a few general points regarding the relationship between armed conflict and E-CI. Considering whether the ethics of armed conflict can serve as a normative framework for E-CI, Fabre notes that although the two areas are related because of their shared aim to ensure national security, there remain important differences between them.[4] First, armed conflict is a response to a live threat to national security,



https://doi.org/10.1017/S0892679423000199 Published online by Cambridge University Press

such as invading soldiers. By contrast, espionage and counterintelligence can be preventive in orientation, seeking to foil plots to undermine national security. Second, E-CI is not confined to the period of armed conflict but also continues in peacetime. Third, as anyone with a faint acquaintance with just war theory knows, the central ethical question in armed conflict is, naturally, the permissibility of killing and the destruction of property. While it is true that E-CI can also involve the infliction of harms, such harms are usually not as severe as the loss of life, at least not intentionally.

In light of these differences, the essay assumes that the analogy between TECHINT and armed conflict is loose. Crucially, I do not claim that the ethical, political, and conceptual issues arising from military technology are analytically reducible to similar issues in TECHINT or even part of the same normative framework. Still, analogies are useful to get a sense of issues in a relatively underexplored field. In order to develop the analogy between TECHINT and precision weaponry, the essay proceeds as follows. In the first section, I examine Fabre's justification for the use of TECHINT. Indeed, I strengthen it. In the second part of the piece, I offer some general thoughts on the impact of precision weaponry on armed conflict. I then build the analogy between precision weaponry and spy technology. The essay concludes that just as precision weaponry is morally ambiguous, TECHINT also appears to be Janus-faced; namely, morally desirable and undesirable at the same time. Arguably, this raises wider questions about the ethics of technology, especially in high-risk domains.

## Justifying TECHINT via Case Comparisons

Let me begin by outlining the rough contours of Fabre's philosophical treatment of TECHINT. E-CI usually involves (without being limited to) gathering information via observation and surveillance, intercepting communications, and, increasingly, hacking computers and their networks as part of cyber intelligence (CYBINT).[5] It is easy to see why TECHINT is useful here. Spy satellites can be used to observe large areas. Bugs and other listening devices can pick up conversations between targets that would be inaudible to the human ear. And CYBINT, by definition, requires the use of computers and digital infrastructure. As noted above, leaving CYBINT aside for now, Fabre thinks that there are few, if any, morally salient differences between HUMINT and TECHINT. So, at first sight, a switch from HUMINT to TECHINT does not seem undesirable, notwithstanding



https://doi.org/10.1017/S0892679423000199 Published online by Cambridge University Press

potential practical downsides of the latter, such as a lack of technological effectiveness and information overload.[6] For instance, bugs can fail, or they may generate so much information that it is hard to process. Clearly, though, these downsides must be finely balanced against human limitations, such as fatigue or lack of concentration, or the limited range of human eyes and ears. For now, it suffices to note that TECHINT and HUMINT will each have their own practical drawbacks that necessitate trade-offs, some of which are potentially morally relevant. Humans are not perfect; neither is technology.

To assess the ethics of TECHINT, Fabre relies on what I call "case comparisons." Case comparisons are philosophical thought experiments that utilize a fictional base scenario in which a human agent performs, or intends to perform, morally permissible actions in order to accomplish a (morally permissible) task. The base scenario is then contrasted with a second scenario, the contrasting scenario, in which the human agent is replaced by a technological artifact, with all other morally relevant conditions remaining equal. Case comparisons are analytically important because they help us to differentiate between what I have called, in earlier work, "intrinsic and contingent reasons for or against technology."[7] This distinction helps to clarify the nature of our arguments against technologies, such as whether we object to certain technologies because of contingent factors that make human agency preferable (and vice versa), or whether there are deep and intrinsic moral differences between human agency and the use of specific technologies. The conclusion of Fabre's main case comparison is that there are no intrinsic differences between the deployment of human assets and the use of spy technology.

That case involves a base scenario where a state called "Green" is engaged in a conflict with a paramilitary organization called "Blue," loosely modeled (I believe) on the real-world organization calling itself Daesh, the Arabic acronym for the group comprising ISIS, or ISIL.[8] Green uses a human asset ("Asset") to establish a personal relationship with Blue's fighters ("Fighters"), which results in important information about Blue's plans being passed on to Green. There are two variations of this base scenario: in the first, Asset eavesdrops on Fighters in public spaces; in the second, Asset follows Fighters around, recording whom they meet and where they socialize. Needless to say, in the base scenario and its variations, Asset disguises her identity. Fighters do not know that Asset works for Green.

In the contrasting scenario, Fabre replaces Asset's attempt to gain information by befriending Fighters with insect-like robots that are, unbeknownst to Fighters,



https://doi.org/10.1017/S0892679423000199 Published online by Cambridge University Press

placed in their residences. Analogically to Asset's trailing of Fighters and eavesdropping on them, Fabre also imagines that spy technology enables Green to intercept email correspondence, as well as telephone conversations, between Fighters.[9] Is Green morally permitted to rely on TECHINT in the contrasting scenario? Fabre thinks so. In fact, she argues that there is a strong reason in favor of using TECHINT. Green, Fabre contends, has duties of care toward Asset; for example, to protect her from potential risks to her life and person that could result from seeking to infiltrate Fighters.[10] If reliance on TECHINT leads to fewer harms and risks being imposed on Asset while yielding the same results, then it is morally preferable to HUMINT.

That said, Fabre does consider a potential difference between the base and contrasting scenarios of her case comparison. When Asset gathers information by befriending Fighters, Fighters have some degree of control over the extent of their interactions with Asset.[11] As a result, their behavior toward Asset has greater potential to frustrate Green's aim to gather intelligence about the group. In the contrasting scenario, they lack such control, since they do not know that they are being monitored via spy technology. Compared to the base scenario, their actions are less likely to frustrate Green's aim. Clearly, from Green's perspective, this explains the attraction of using spy technology. In her discussion of the contrasting scenario, Fabre does not think that Fighters' lack of control poses an ethical problem. This is because, she contends, Fighters are liable to the harms imposed on them by TECHINT due to their illicit activities against Green. From this comparison, Fabre concludes that TECHINT can be morally preferable to HUMINT in certain circumstances.

Overall, I do not take issue with Fabre's base and contrasting scenarios. In fact, I think they can be strengthened, thus underlining the moral desirability of TECHINT. The first way to strengthen Fabre's conclusions involves a return to the issue of agency. Paramilitary and terrorist organizations are usually extremely paranoid about being infiltrated by law enforcement or intelligence services. Surely, as in the base scenario, just as it is up to Fighters to determine how much information they divulge to Asset, it is also, as in the contrasting scenario, up to them to take countermeasures against technological surveillance; for example, by sweeping for bugs, encrypting their messages, or changing between multiple vehicles when traveling to a safe location. They should expect their adversaries to use spy technology against them and act accordingly. Fighters are not unwitting participants in an intelligence operation. If this is correct, the issue of agency does



https://doi.org/10.1017/S0892679423000199 Published online by Cambridge University Press

not pose an ethical obstacle to the deployment of spy technologies against targets such as Fighters.

The second way to strengthen Fabre's case for TECHINT partly draws upon her treatment of the issue of deception.[12] The types of organizations that typically land in the crosshairs of the intelligence services tend to have vetting procedures and loyalty tests that are specifically designed to identify individuals like Asset. These can be brutal: have the opponent murdered or tortured, take drugs, participate in a raid on a weapons cache, or be subjected to violent interrogation. In other words, infiltrating such groups does not merely consist in striking up a conversation with members outside a café. As a result, the strongest argument for TECHINT is twofold: In line with Fabre's point about duties of care, TECHINT (1) protects Asset from potentially severe risks to her own person, and (2) prevents Asset from engaging in wrongdoing against other parties. I would wager that (2) is normatively stronger than (1) due to the stringency of negative duties not to harm nonliable individuals, which Asset may be compelled to violate to prove loyalty.[13]

Taken together, the above shows that Fabre's case in favor of TECHINT is very strong. The use of TECHINT is, in some instances, more justifiable than HUMINT. And yet, the case comparison approach that underpins Fabre's reflections on TECHINT is not unproblematic. In the above analysis, the transition from the base to the contrasting scenario is smooth, for two reasons. First, Fighters are, as per Fabre's argument, liable to being investigated by Green. That is to say, Green is under no moral duty not to take measures against Fighters. The question is *which* measures Green may permissibly take, not *whether* it can permissibly take any measures at all. Second, and directly to the preceding point, the additional normative constraints of necessity, effectiveness, and proportionality remain equal in both scenarios. Compared to HUMINT, the point, as I understand Fabre, is that the use of TECHINT does not subject Fighters, liable as they are, to unnecessary or disproportionate amounts of harm. Nor is there anything intrinsically wrong with using spy technology against Fighters: doing so does not deprive the individuals of their dignity, for example. And, as I argued above, Fighters retain some agency in the contrasting scenario.

Nevertheless, and without getting into a general debate about the advantages and disadvantages of case comparisons, the moral lens granted by Fabre's case comparison has blind spots for the following reason: spy technology (just like any other form of technology) rarely acts as a like-for-like replacement for direct



https://doi.org/10.1017/S0892679423000199 Published online by Cambridge University Press

and technologically unmediated human involvement. Nor does it (in the case of emerging spy technologies) necessarily act as a like-for-like replacement for older spy technologies. Fabre herself seems to recognize this when she states that the deployment of spy technology instead of human assets must be judged on a case-by-case basis.[14] So, although Fabre concludes, in my terminology, that there are no intrinsic objections to TECHINT as such, the justification of any particular technology is contingent on specific circumstances. This has two potential repercussions. First, compared to HUMINT, some spy technologies may cause disproportionate and unnecessary harm. As a result, and following Fabre, a justification of any given technology and its deployment can only be done on a case-by-case basis. That is, individual case comparisons do not necessarily yield a satisfying answer to the moral permissibility of TECHINT since it depends on the system under consideration and not upon a general justification of TECHINT. Second, the shift from HUMINT to TECHINT could lead to wider transformations of E-CI practices that are difficult to capture via case comparisons.

## The Moral Desirability of Spy Technology: A Cautionary Tale

In this section, I explore how the shift from HUMINT to TECHINT potentially transforms E-CI practices, thereby challenging the use of case comparisons in this context. As indicated in my introductory remarks, the current debate on military technology, I believe, serves as a useful illustration of the shortcomings of case comparisons, with some of its insights speaking directly to the transformative capacity inherent in TECHINT.

### *Precision Weaponry and Its Moral (Un)desirability*

Armed conflict and technology exist in a close relationship. As Hegel once famously put it, gunpowder was the result of human thought and promoted human thinking. Gunpowder and similar inventions ensured that the (physically) strongest no longer prevailed. Humans could rely on their intelligence instead. Gunpowder was necessary; hence humans invented it.[15] In recent years, claims about the alleged ethical desirability of certain forms of weaponry have become prominent in (largely Western) political, military, legal, and philosophical discourses. The development of so-called precision weaponry stands out, representing an attempt to render warfare more humane by limiting its destructiveness.



https://doi.org/10.1017/S0892679423000199 Published online by Cambridge University Press

Precision weaponry, so the argument goes, enables better compliance with the legal and normative frameworks governing the use of force in armed conflict.[16] In particular, it becomes easier for belligerents to comply with the legal and ethical requirement to distinguish between legitimate and illegitimate targets in war.

Arguably, the impact of precision weaponry is exemplified by two phenomena. First, since the 1990s especially, the concept of humanitarian military intervention has sought to render the use of military force compatible with the protection of human rights, drawing heavily on the existence of precision weapons for the conduct of such operations.[17] In many respects, without advances in the delivery of airpower, GPS navigation, and computer-assisted targeting, it would have been fanciful to even entertain the seemingly paradoxical idea of "humanitarian war." Whether, with such advances, it withstands critical scrutiny is another question (see below). Second, remote-controlled unmanned aerial vehicles—or "drones"—have been lauded as having great potential for ensuring compliance with in bello norms.[18] This is partly due to their complex sensor suite and their resulting surveillance capacity. This provides drone pilots with unprecedented situational understanding. Moreover, being remote controlled, the pilots on drones are physically removed from theaters, thus lowering the prospects of rash—and deadly—decisions being made by soldiers under acute combat stress.

It is easy to develop case comparisons to justify the above claims. Suppose "Red" is pursuing a morally justified war of self-defense against aggressor "Yellow." Should Red, other things being equal, use long-range artillery with unguided munitions or GPS-guided cruise missiles to destroy Yellow's military installations? Should Red deploy nineteen-year-old soldiers to pursue one of Yellow's generals or should Red, other things being equal, use a drone to target the general's convoy? I would argue that there is hardly a moral contest here. It borders on the obvious to say that cruise missiles are morally preferable to unguided munitions, or that a targeted killing in an international armed conflict, even if carried out from the asymmetric position afforded by drone technology, is preferable to a highly volatile confrontation between young and inexperienced soldiers.

And yet, despite these technological advances, all is not well in the world of precision warfare. Most notably, over the last twenty-five years, civilian death tolls and the destruction of civilian infrastructure have remained very high, notwithstanding the deployment of precision weaponry. Some critics of the "Western way of war," for example, speak of "risk-transfer war." Rather than minimizing



https://doi.org/10.1017/S0892679423000199 Published online by Cambridge University Press

civilian losses, reliance on precision weaponry has transferred risks from combatants to civilians.[19] Others contend that the availability of precision weaponry has led to a form of military hubris. This hubris is the result of the belief that these weapons are superior to older, less precise weaponry. This has led to their deployment in theaters where it is inappropriate, perhaps even reckless, to use military force in the first place.[20] The (not-unreasonable) belief, in other words, that the use of precision weaponry leads to low civilian casualties has led, in actual conflicts, to high(er) casualties.

In addition, the availability of drones has made feasible the application of military force to individuals merely suspected of engagement in terrorist activity. This is because no "boots on the ground" are needed to track such individuals and kill them. In this context, military force has increasingly gained a preventive, rather than reactive, component. This has led to fundamental questions about the status of targeted killings under the laws of war, as well as just war theory.[21] Moreover, there is a more practical question of whether targeted killing via drones has crowded out alternative approaches to counterterrorism, especially the arrest and trial of suspected terrorists. Lastly, drones have enabled an unprecedented nexus between military and intelligence agencies. The very platform that makes possible long-term surveillance and the building of complex intelligence pictures is also capable of applying military force to a target.

In short, weapons technology is often—forgive the pun—a double-edged sword. From the perspective of case comparisons, few would dispute that any of the aforementioned weapons are morally undesirable. At the same time, the availability of morally desirable weaponry can have morally questionable long-term consequences. Contrary to the underlying structure of case comparisons, weapons never exclusively act as like-for-like replacements for either direct and unmediated human agency or older types of weaponry. Weapons also have the capacity to transform, over time, the practices and understandings associated with the use of military force—perhaps even transforming the character of war itself. On the one hand, they may enable better compliance with existing regulatory frameworks. On the other hand, they can undermine such frameworks by giving rise to new practices that are hard to regulate. In a worst-case scenario, they may enable abuse.[22] They may also lead to a form of technological hubris. This leads to the somewhat paradoxical position that certain weapons can be morally desirable and undesirable (or at least problematic) at the same time.

### *Implications for TECHINT and Spy Technology*

The above observations, I believe, are directly relevant to the kinds of spy technologies that make TECHINT possible. True, in her case comparison, Fabre is correct that, compared to HUMINT, the deployment of insect-like robots against Fighters does not pose special moral problems. Certainly, it is also possible to formulate other case comparisons where the replacement of HUMINT with TECHINT is morally desirable, perhaps even mandatory. That said, the availability of insect-sized machines should worry us. Like drones, for example, they might enable an ever-tighter connection between surveillance and assassination, with low levels of attributability. More broadly, the emergence of new spy technologies could transform our very understanding of the scope of E-CI and its associated practices, thereby challenging our ethical justifications of this domain.[23] Below, I offer four general thoughts on how experiences with precision weaponry can illuminate the long-term challenges raised by spy technology.

First, just as drones have lowered the cost of carrying out targeted killings, spy technology has lowered the cost and complexity of E-CI operations. As a result, E-CI can relatively easily be extended to individuals and contexts where it previously would not have been appropriate. To illustrate the point, Fabre mentions the case of former German chancellor Angela Merkel, whose mobile phone was infamously hacked by the CIA (and the British Government Communications Headquarters, or GCHQ) in 2009 ahead of the G-20 summit in London, souring diplomatic relations between Germany and the United States. Arguably, this constituted improper use of spy technology.[24] But now, compare this instance of TECHINT with an equally infamous case of HUMINT; namely, the so-called Guillaume Affair. During the existence of separate East and West German states between 1949 and 1990, the feared East German Ministerium für Staatssicherheit (STASI), or Ministry for State Security, managed to install one of its agents, Günter Guillaume, as a personal secretary to West Germany's legendary social-democratic chancellor Willy Brandt. When this was revealed, Brandt fell. True, the complexity of the Guillaume operation did not deter the STASI (few things did). But it must have taken months, perhaps years, to create an identity for Guillaume and position him close to Brandt. Guillaume's success in gaining access was not guaranteed, either. The STASI gambled. There was some risk that the resources invested into Guillaume could have been wasted. By contrast, in 2009, the CIA's listening station was placed on the roof of the American embassy, right next to the Brandenburg Gate and a stone's throw away from the chancellery.



https://doi.org/10.1017/S0892679423000199 Published online by Cambridge University Press

All it took was for the CIA to identify Merkel's mobile phone and decrypt its signal—something a tech whiz could accomplish in a couple of hours or days. In short, simplicity may encourage improper use, not least because, when conducting TECHINT, the risk of wasting precious resources is low and the chances of success are higher than in HUMINT. That said, due to the secretive nature of E-CI operations, it is hard to ascertain the extent to which states spy on each other's leaders. The Guillaume Affair and the hacking of Merkel's phone are prominent examples of espionage precisely because they are among the few cases that we know about. Still, given the vulnerability of digital information infrastructure, I do not think that it is far-fetched to hypothesize that intelligence agencies have broadened and intensified their targeting of leading politicians, with higher levels of success than was possible at the time of the Guillaume Affair.[25]

Second, as noted above, overreliance on drones might foreclose other, less lethal approaches to counterterrorism. Overreliance on, and overconfidence in, spy technology and TECHINT could have similar repercussions. To speculate, I do not think it is far-fetched to assume that (some) governments may have used TECHINT to gain information about other governments' bidding and negotiating strategies for the procurement of vaccines against COVID-19.[26] After all, as Fabre's work reminds us, economic espionage is nothing new.[27] That said, in the case of vaccine procurement the availability of TECHINT may have potentially crowded out a more cooperative and coordinated approach between governments (for example, joint bidding) that could have led to lower costs for taxpayers and more stringent legal obligations for vaccine manufacturers, albeit at the expense of a faster vaccine rollout.

Third, the main moral justification for precision weaponry is that it reduces the suffering of the innocent during armed conflict. As we saw above, in practice, there are serious questions about this claim. In some ways, one could argue, precision weaponry has transferred risks toward civilians. The same dynamic, I think, is at play in the context of spy technology. As the example of CYBINT shows, technology enables the extension of E-CI practices beyond what one would deem legitimate targets of E-CI (senior politicians, some state officials, and some figures of industry). Increasingly, the data of, and information about, innocent individuals can be accessed and used by intelligence agencies. And this is not just a matter of CYBINT. In Fabre's case comparison, the insect-like robots installed in Fighters' homes presumably also pick up private conversations between Fighters and their family members. The use of AI to process and learn

from vast quantities of data aggravates this problem. Suppose that the insect-like robots in Fighters' homes have an underlying AI-based speech-analysis program that can offer an intelligence officer an assessment of whether Fighters are lying or speaking in code.[28] Somehow such an AI needs to have been trained beforehand. One wonders where the data necessary for this training comes from and to what extent recorded conversations between civilians need to be used to generate the necessary quantity of material. Needless to say, this has a deep impact on how we think about civil liberties and other relevant rights.

Fourth, I have already noted that the availability of drones has resulted in an increasing breakdown of boundaries between E-CI and military operations, even outside of an armed conflict. Among just war theorists, the possibility of using targeted and small-scale military force for situations falling short of a full-blown armed conflict has led to some soul searching.[29] Likewise, the potential breakdown of boundaries between preventive intelligence work and more reactive uses of military force might necessitate a rethinking of the ethics of E-CI and its relationship with just war theory. Like drones, other emerging technologies may combine dual E-CI and military functions, which raises questions over their regulation. For instance, does an intelligence-led targeted killing operation that utilizes drones constitute an act of war or not? Or does it constitute an intelligence operation and a military operation at the same time? If so, which regulatory framework applies at what stage of the targeted killing? To complicate matters, what if technological innovations in the private sector (for example, in social media and big data), rather than state-led research and development processes, begin to drive TECHINT, as well as weapons development?[30] This would give rise to "triple-use functions": civilian, intelligence, and military. Without going into detail, it is easy to see how it becomes difficult to apply discrete regulatory frameworks that were developed for specific domains to (some) emerging technologies.

Admittedly, none of these four points inspires confidence. Indeed, just as in a globalized world some attempts to theorize international order only generate "rules for a vanished Westphalian world," the normative and legal frameworks for E-CI are in danger of being increasingly outpaced by the development of spy technology and resulting TECHINT practices.[31] Further, from a philosophical perspective, the analogy between precision weaponry and spy technology illustrates the difficulty of balancing the moral desirability of technologies against their potentially undesirable long-term effects. How this can be done remains to be seen.



https://doi.org/10.1017/S0892679423000199 Published online by Cambridge University Press

## Conclusion

The moral justification for using technology, rather than human assets, to conduct espionage and counterintelligence operations is a thought-provoking theme in Cécile Fabre's stellar *Spying through a Glass Darkly*. It is hard to disagree with Fabre's finding that the use of spy technology is sometimes morally desirable, not least if it protects (nonliable) individuals from severe harms. Yet, by drawing an analogy between spy technology and military weapons, this essay shows that spy technology has the capacity to change established practices in, and understandings of, espionage and counterintelligence. It needs to be clarified how to best harness the morally desirable impact of spy technology while reining in its morally undesirable effects. More controversially, it needs to be clarified whether states should sometimes forgo the development of certain spy technologies if their long-term effects would be extraordinarily detrimental. All in all, Fabre's arguments in *Spying through a Glass Darkly* act as an important starting point for a wider, and much needed, ethical debate on the role of spy technology in espionage and counterintelligence, as well as its broader societal impact in the years ahead.

### Notes

[1] Some of the material on precision weaponry that appears in the third part of this essay was developed during a Leverhulme early career fellowship (ECF-2016-643). The support of the trust is gratefully acknowledged. I would like to thank Cécile Fabre for her comments on early drafts of this essay, as well as all the participants in the virtual book symposium, "Spying Through a Glass Darkly: The Ethics of Espionage and Counterintelligence," on Fabre's *Spying through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence* (New York: Oxford University Press, 2022), held on May 23, 2022, via Zoom.

[2] Fabre, *Spying through a Glass Darkly*, ch. 8.

[3] HUMINT and TECHINT are standard acronyms in the world of E-CI. See ibid., pp. 174–75.

[4] Ibid., pp. 24–25.

[5] Ibid., pp. 175–77.

[6] Ibid., p. 179.

[7] Alex Leveringhaus, "What's So Bad about Killer Robots?," *Journal of Applied Philosophy* 35, no. 2 (May 2018), pp. 341–58, at p. 343.

[8] Fabre, *Spying through a Glass Darkly*, p. 178.

[9] Ibid.

[10] Ibid., p. 178.

[11] Ibid., p. 179.

[12] Ibid., see esp. pp. 110–11.

[13] On this theme, see F. M. Kamm, "Nonconsequentialism," ch. 1 in *Intricate Ethics: Rights, Responsibilities, and Permissible Harm* (Oxford: Oxford University Press, 2007), pp. 11–46.

[14] Fabre, *Spying through a Glass Darkly*, p. 181.

[15] Edward Black, "Hegel on War," *Monist* 57, no. 4 (October 1973), pp. 570–83.

[16] For an attempt to disambiguate the concept of precision, see Alex Leveringhaus, "Autonomous Weapons and the Future of Armed Conflict," in Jai Galliott, Duncan MacIntosh, and Jens David Ohlin (eds.), *Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare* (New York: Oxford University Press, 2021), pp. 175–88.

[17] For a recent philosophically sophisticated debate on humanitarian intervention, see Fernando R. Tesón and Bas van der Vossen, *Debating Humanitarian Intervention: Should We Try to Save Strangers?* (Oxford: Oxford University Press, 2018).
[18] See Bradley J. Strawser, "Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles," *Journal of Military Ethics* 9, no. 4 (2010), pp. 342–68.
[19] See Martin Shaw, *The New Western Way of War: Risk-Transfer War and Its Crisis in Iraq* (Cambridge, U.K.: Polity, 2005).
[20] See Bruce Cronin, *Bugsplat: The Politics of Collateral Damage in Western Armed Conflicts* (New York: Oxford University Press, 2018).
[21] See Clare Finkelstein, Jens David Ohlin, and Andrew Altman, eds., *Targeted Killings: Law and Morality in an Asymmetrical World* (Oxford: Oxford University Press, 2012).
[22] Of course, any weapon may be abused. I could use a gun to shoot an aggressing soldier or a civilian. However, one should not dismiss the prospect that some weapons lend themselves to abuse more than others, or with more catastrophic consequences. Or that some weapons give rise to practices that are hard to regulate through existing frameworks.
[23] One could argue that CYBINT proves the point. The advent of complex IT infrastructures since the late 1980s (the Internet) has generated new challenges that would have been inconceivable in the 1950s. Due to its complexity, I leave CYBINT aside in this essay. See Fabre, *Spying through a Glass Darkly*, p. 186.
[24] Ibid., pp. 176, 181.
[25] My own recollection of the press coverage in Germany at the time of the phone-hacking scandal is that the German government itself faced questions about its attempts to gain intelligence about the leaders of other countries, including friendly nations. Some politicians and state officials seemed keen to move on quickly.
[26] Jon Sharman, "Hackers Targeted University of Oxford's Covid Vaccine Research, Cyber Spies Reveal," *Independent*, November 17, 2021, www.independent.co.uk/news/uk/home-news/covid-vaccine-hack-cyber-oxford-b1959147.html.
[27] Fabre, *Spying through a Glass Darkly*, ch. 4.
[28] In China, for instance, such speech-analysis programs are used by call centers in the banking sector in order to determine whether a customer who tries to obtain a loan over the phone is genuine. The programs usually monitor the conversation between the client and the call center worker, often without the knowledge of the former. I thank Bonnie Buchanan for drawing my attention to this.
[29] See Daniel R. Brunstetter, *Just and Unjust Uses of Limited Force: A Moral Argument with Contemporary Illustrations* (Oxford: Oxford University Press, 2021).
[30] I thank Mikolaj Firlej for this point.
[31] Allen Buchanan, "Rawls's Law of Peoples: Rules for a Vanished Westphalian World," *Ethics* 110, no. 4 (July 2000), pp. 697–721.

---

Abstract: This essay contends that the ethics around the use of spy technology to gather intelligence (TECHINT) during espionage and counterintelligence operations is ambiguous. To build this argument, the essay critically scrutinizes Cécile Fabre's recent and excellent book *Spying through a Glass Darkly,* which argues that there are no ethical differences between the use of human intelligence (HUMINT) obtained from or by human assets and TECHINT in these operations. As the essay explains, Fabre arrives at this position by treating TECHINT as a like-for-like replacement for HUMINT. The essay argues instead that TECHINT is unlikely to act as a like-for-like replacement for HUMINT. As such, TECHINT might transform existing practices of espionage and counterintelligence, giving rise to new ethical challenges not captured in Fabre's analysis. To illustrate the point, the essay builds an analogy between TECHINT and recent armed conflicts in which precision weapons have been deployed. Although precision weapons seem ethically desirable, their availability has created new practices of waging war that are ethically problematic. By analogy, TECHINT, though not intrinsically undesirable, has the capacity to generate new practices of intelligence gathering that are ethically problematic—potentially more than HUMINT. Ultimately, recent negative experiences with the use of precision weaponry should caution against an overly positive assessment of TECHINT's ethical desirability.

Keywords: ethics of espionage, ethics of intelligence, ethics of technology, weapons technology, Western way of war, just war theory, armed conflict