


The Ethics of Economic Espionage

Ross W. Bellaby 

The ethical value of intelligence comes from its role in protecting people from harm by detecting, locating, and preventing threats. Or more specifically, intelligence protects or provides for the vital interest people have in maintaining their physical and psychological integrity, autonomy, liberty, and privacy. The challenge for intelligence ethics, however, is that in protecting or providing for some people's vital interests, gathering intelligence necessarily involves violating the vital interests of others in order to access secret information or to put a state's policy into effect. The broad debate, therefore, is how to reconcile this tension and be able to know if and when the vital interests of another party can be violated in order to secure one's own interests.¹ Cécile Fabre's recent book *Spying through a Glass Darkly* addresses this concern by arguing for the "ongoing and preemptive imposition of defensive harm," whereby all "individuals have a presumptive right not to be harmed, but they can sometimes become liable to defensive harm: that is to say, it is permissible deliberately to harm them in self-defense or in defense of others without thereby infringing their right."² Intelligence is therefore permissible even though it harms others so long as it is a form of self-defense.

While in the intelligence community, the purpose of defensive harm is often framed as averting direct attacks against critical infrastructure or protecting human life, people can face a range of different threats that come in a variety of forms and from various directions.³ For example, this can mean that at both the individual and societal level there is a need to protect physical infrastructures, economic strength, social well-being, civil order, technological advancement, and diplomatic relations—each of which can then be threatened militarily, politically,

Ross W. Bellaby, University of Sheffield, Sheffield, England (r.bellaby@sheffield.ac.uk)

Ethics & International Affairs, 37, no. 2 (2023), pp. 116–133.

© The Author(s), 2023. Published by Cambridge University Press on behalf of the Carnegie Council for Ethics in International Affairs

doi:10.1017/S0892679423000138

financially, or through social upheaval. This places a wide mandate on intelligence actors, from providing “solid warnings of terrorist plans . . .” to finding out the bottom line “on an impending negotiation about tariffs in trade in cabbages.”⁴

It should come as no surprise, therefore, that protecting the economic welfare of the political community is considered an area of vital importance for intelligence actors and political elites. A strong economy is seen as fundamental both to “traditional concepts of national interest and politico-military security”⁵ and as an important means for people to flourish or, “put in deontic terms, to secure their fundamental moral rights and enable them to fulfil their fundamental moral duties.”⁶ This has meant that in a world where the “economic health of nations and the competitiveness of businesses are determined largely by the ability to develop, commercialize, and capture the economic benefits from scientific and technological innovations,” being able to maintain superiority through accessing secret proprietary information has come to represent an important part of maintaining security and welfare.⁷ The intelligence community is therefore concerned with collecting and analyzing secret economic information in order to “protect and promote national economic security, whether it is information on a new maker for telephone switches in China or reports of impending financial collapse in Mexico.”⁸ Indeed, as former Director of Central Intelligence Stansfield Turner argued, collecting information as a means of securing the economic advantage of the United States is essential, stating that “America would have no compunction about stealing military secrets to help it manufacture better weapons,” and that “if economic strength should now be recognized as a vital component of national security, parallel with military power, why should America be concerned about stealing and employing economic secrets?”⁹

Despite this clear importance and prominent role, economic espionage remains one of the most overlooked areas in intelligence studies, and one of the key contributions of Fabre’s book is to shine a direct light on some ethical debates about its use. Fabre applies the underlying argument of the book to the specifics of economic espionage to argue that while states, businesses, and individuals do have a general right over their information that prevents others from accessing it, such protections can be forfeited or overridden when there is a potential threat to the fundamental rights of third parties, which allows for a state to carry out economic espionage.¹⁰

While this position generally works for many intelligence activities, I will argue that economic espionage is distinct compared to many other forms of intelligence

activity, and less permissible than Fabre outlines in the book, because it is more likely to cause a wider set of costs across society that will produce harm for those who have not acted in a way as to be justified targets. This is analogous to Joy Gordon's argument against economic sanctions in which she suggests that those that are the least involved and potentially the most vulnerable can be harmed, and thus the practice fails the principle of discrimination.¹¹ I will argue that economic espionage aims to provide one country's own economy a competitive advantage, but that this economic benefit for one party will necessarily come at the economic cost of another party that has not necessarily done anything to warrant it. Such a competitive advantage is achieved by gathering information from competitors so that one country's own companies or institutions can produce its goods or services at a greater rate, at a higher quality, and/or for a lower cost with the aim of increasing its market share at the expense of competitors.¹² So, when the intelligence community intervenes to achieve success for economic actors within its home state, it is necessarily inflicting harm on other economic actors. Moreover, I will argue that given the complex way in which the economy interlinks with people's lives and society, the harms caused by economic intelligence will be spread widely across society, more readily than other forms of intelligence activity, and will result in broad harm to those that have done nothing to warrant it. Significant harms or costs to one economic actor will have repercussions on those secondary economic entities dependent on that entity, such as workers, buyers, and investors, which, in turn, can cause further harms to tertiary economic actors dependent on those groups, and, from there, their own workers. This produces damages that can ripple outward across society and cause further harm to others that may not have acted in a way to be justifiably harmed.¹³ To account for this, additional care needs to be given to questions of proportionality and discrimination. I will also argue that while scenarios that focus on high-end state negotiations and critical infrastructure cases are important, much of economic espionage is targeted against private companies where the gains are less easily framed as providing vital assistance to a state and its political community. Economic espionage, I conclude, is not as justifiable as might be initially thought.

JUSTIFYING ECONOMIC ESPIONAGE

At the center of the tension in intelligence ethics is the fact that there are aspects of the intelligence business that seem "notably disreputable,"¹⁴ leading to the

argument that without secret intelligence states cannot “understand sufficiently the nature of some important threats.”¹⁵ Over the last century, intelligence has become one of the most vital tools that a political community has in providing timely information designed to serve and protect people from harm and, as such, has become central to the ethical good represented by protecting the political community. However, it can also be argued that the damage that intelligence can cause means that there should be limits on its use. Indeed, Michael Quinlan, David Omand, and Michael Herman, all of whom have highly distinguished careers in intelligence, defense, and government, have each noted the “ethical baggage” intelligence activity carries with it.¹⁶

This ethical baggage can be best understood as the harm caused when many of the actions and consequences of intelligence activity, such as surveillance, manipulation, coercion, and deception, come into conflict with people’s core vital interests. These vital interests are those aspects of the human condition that are so fundamental that without them people are not able to carry out their own version of the good life. As Joel Feinberg argues, individuals have a set of interests that form the prerequisites or preconditions that must exist if they are to fulfill their more ultimate life goals and flourish as human beings. That is, regardless of what conception of the good life the individual holds or what his or her life plans might be in detail, these preconditions must be satisfied first in order to achieve them.¹⁷ This includes the interest that people have in maintaining and protecting their vital interest in their physical and mental wellbeing, autonomy, liberty, and privacy. If the quality of these interests were to fall below a threshold level, the individual would cease to be considered to be living as “truly human, that is, *worthy* of a human being” and would thus be harmed.¹⁸

The ethical justification for intelligence, therefore, recognizes the need to both limit and license its activity by reconciling the harm caused by the intelligence activity when it violates these vital interests with the objective of protecting the vital interests of the members of the political community.¹⁹ Fabre addresses this concern by arguing that the “main rationale for the existence of the state . . . lies in its ability and willingness . . . to provide for individuals’ security, and more widely, their prospects for a flourishing life.”²⁰ People have a fundamental right to defend themselves from harm, and part of the state’s ethical mandate is derived from its ability to provide this defense. And so, one can justify the harm intelligence may cause when it is done to protect people’s vital interests

from a greater harm as a manifestation of the right to self-defense or the defense of others.²¹

Economic espionage, broadly understood, involves the secret collection of economic information from both other states and private economic actors as a tool of statecraft, often framed as a form of (economic) national security.²² This can include accessing and collecting secret information about a target's operations, strategy, and resources.²³ The information taken can include intellectual property, which consists of ideas, concepts, and inventions; industry-prevalent recipes or formulas; operational information, such as detailed production and marketing data and strategy-orientated competitive intelligence; and personal information from or about particular individuals. As such, economic espionage similarly starts with the general recognition that actors—whether individuals, private economic actors, or state institutions—have rights that protect their own information from outside interference. For some, this right can be framed in terms of the interest such entities have in their privacy, creating boundaries and protections over information pertaining to or created by an actor.²⁴ Or such rights can be based on Lockean conceptions of property, where information can be created, sold, bought, or distributed only at the will of the author or owner.²⁵

In discussing economic espionage, Fabre argues that accessing such information and violating the vital interest in privacy can, however, be justified when it is done to protect people from more significant harms; for example, when it “targets a business whose activities threaten a state's national security,” including “not just its military security or the security of its critical infrastructure . . . but also the basic well-being of its population.”²⁶ The argument is that the right to self-defense acts as a means of justifying accessing another's protected information.²⁷

However, the right to self-defense is not without its limits, as the harm caused should also be proportional, and should discriminate between legitimate and illegitimate targets. While these additional criteria of proportionality and discrimination are mentioned in Fabre's chapter on economic espionage, they are not fully explored, and there are some key concerns for the practice of economic espionage.²⁸ Indeed, in addition to the privacy violations, the consequences of economic espionage also represent an important threat to people's other vital interests, such as their physical and mental well-being and autonomy. This can exist in terms of the role that stable economic actors play in providing people with the material assets and structures they need to survive and, in turn, flourish; assets such as food, water, shelter, education, and other materials—whether this is

through individuals working to directly secure required resources or by society developing structures and opportunities for subsequent access to such resources. Or it can relate to the important role the economy plays people having the opportunity to fulfill their autonomy and mental well-being through making an economic contribution. Indeed, there is value in people having a right to work as a means of expressing their own vital interest in their autonomy, which includes their creative and social capabilities and feeling as though they are contributing to their political community.²⁹ Therefore, even if self-defense provides a sound justification for economic espionage to violate a target's privacy, there are additional harms likely to be inflicted on a wide range of agents, including people who have not acted in a way to waive their normal protections. This makes both the discrimination and proportionality criteria harder to satisfy.

Indeed, the requirement that an attack must discriminate between legitimate and illegitimate targets is one of the most important ethical criteria across a number of different disciplines, from retributive justice to the codified international laws of war.³⁰ Traditionally, the distinction comes from the moral prohibition on harming those who have done nothing to warrant being harmed, in contrast to those who have acted in some way or have "something about them" that justifies targeting them.³¹ One becomes a legitimate target—that is, has acted in such a way that their normal protections have been waived—by, for example, voluntarily suspending their rights when they join a particular profession or group.³² Or they can forfeit their rights by acting in such a way as to represent a threat to a third party.³³ Failing this, the target's rights can be overridden "when the ends pursued by intelligence officers are sufficiently weighty to provide them with a justification for so treating those individuals even though the latter are not liable to such treatment."³⁴

However, in order to make this overriding argument, Fabre notes that the justified ends need to be "sufficiently weighty" so as to allow harm to be produced toward those that are ultimately innocent.³⁵ In unpacking this, it can be argued that the ends can be considered weighty enough to justify harm to the innocent when the course of action protects interests that are more important than the interests of the innocent, such as violating someone's privacy to protect another's life; or when it involves interests that are of equal importance but protect a significant number of people compared to those harmed. This means that proportionality is also an important part of this discrimination calculation, because it must be determined whether there is a greater need in terms of the

number of vital interests that will be protected by the harm brought about through the intelligence action.

In order to understand what this means for economic espionage, some distinctions should be made. First, a distinction should be made between economic espionage collected to inform or reassure political elites and espionage collected to get information that is then used by the political elites for some policy or activity. While Fabre focuses on the former in her chapter by discussing operations to understand whether an energy provider is acting according to an agreement,³⁶ the latter is more reflective of how economic espionage is used. Many of the publicly known examples of economic espionage detail how the information gained is used to provide an economic advantage, whether for a private actor or in state trade negotiations. This latter form is also more problematic. Since its aim is to gain information and to provide home actors a competitive advantage, it necessarily relies on another actor losing out.

Second, in some forms of intelligence activity, those targeted and any subsequent collateral damage can be confined to a select set of targets, which allows for more accurately determining whether they are justified targets or not. For example, wiretapping specific targets and violating their privacy and autonomy with the aim of being more informed about a possible threat, such as terrorist activity or an aggressive state, can be judged on the role or threat that those being tapped represent and/or the level of attack anticipated. In comparison, there are those operations that inherently impact a wider range of people with potentially uncontrollable or unknowable implications. This can include instances where the intelligence operation is itself unable to discriminate in its practice, for example, with mass surveillance, or where the implications of utilizing the intelligence is likely to cause widespread and indiscriminate harm. Economic espionage used to inform policy or practice can fall into this latter indiscriminate camp, as the harms inflicted on the target are not confined to those directly engaged but are also spread to other actors who are dependent on these initial economic targets that are forced to suffer the impact of any resulting economic losses. This, in turn, can violate the vital interests of these dependent actors as they lose access to the resources or opportunities necessary to fulfill their continued existence or their ability to fully realize their autonomy. Any failing promoted in these secondary economic actors can then be further passed onto their dependents, and so on. The harm inflicted does not necessarily diminish as it ripples outward, and can even be exacerbated.

This means that even if the target of the economic espionage who loses out is an ethically justified target, those who are reliant on that entity are not necessarily justified targets as well. More problematically, given the complex relationship between a society and its economy, these repercussions are likely to be wide reaching, difficult to control or predict, and to fall on those who were not part of the original operation and so would not be justified targets. Indeed, economic influence permeates so many different aspects of people's lives, at both the local and societal level, that any impact on an economic actor can also create additional impacts on those who are dependent on them. For example, as Fabre herself acknowledges, those "who are neither shareholders, employees, managers, nor consumers of a particular business" may yet have an interest in a company's "robustness," such as large employers or economic actors who are "interwoven in our daily lives."³⁷

There is also a compound effect here: When many people are impacted, the overall harm done is far greater than the simple sum of each of the individual harms. This is especially true for those in particular cultural, racial, or geographic groups, for whom the harm negatively affects social cohesion, well-being, and stability, which can then, in turn, cause further harms and loss of opportunities. For example, economic compound harms can include an increase in crime, loss of education and progression opportunities, escalation of poor physical and mental health, and growth of extremist political views, all of which can be unequally distributed along political, racial, religious, or economic fissures in society. In this way, it is possible to think of how a society or specific sections of a society can be harmed.³⁸ The challenge for economic espionage is that these repercussions on other actors are more readily distributed across society while also being disaggregated and hard to pin down. With many other intelligence operations, the targets and impact can be confined to those intended targets who represent a threat: gangs, insurgents, terrorists, or national security institutions, for example. Arguably, when targeted, the impact is more confined to these groups and those directly associated with them when compared to economic actors who are more widely interconnected with other individuals and across society. Economic systems are so interconnected with society, both globally and locally, and in numerous complex ways, that negative impacts on one economic actor can reverberate out along the various economic interconnections, including employees, shareholders, trade partners, supply chains, and other businesses. Though while such secondary or tertiary implications can be hard to track, this

does not mean these ripples are unimportant or unforeseeable and thus not worthy of consideration.

Finally, and crucially, the problem is not only that there are a greater number of individual harms that can be inflicted on a wider set of people but also that those harmed have done nothing to warrant this harm. If the argument is that people can justifiably have their rights overridden when there is a greater threat present, this becomes increasingly difficult to maintain when the harms inflicted by economic espionage are widely, and potentially uncontrollably, distributed across a society, impacting a wider number of people's vital interests. As the harm is inflicted on an increasing number of illegitimate targets, it becomes harder to proffer an economic benefit. It would therefore require a gain to be of significant value to be part of the justification.

ECONOMIC ESPIONAGE

The challenge for the ethical calculation comes into sharper focus when we look at economic espionage in both the hypotheticals referenced in Fabre's book and the few publicly available known cases of these scenarios. In both instances, they can be categorized in terms of those operations regarding critical infrastructures or state institutions; or cases against private economic actors, covering a range of important economic industries, and can include both large, established, economically significant actors and emerging startups. A trend that becomes evident rather quickly is that of those known cases of economic espionage, many have been carried out against noncritical actors for noncritical returns.³⁹ This challenges some of the assumptions used to justify economic espionage where the violation is done to protect critical infrastructures in extreme circumstances.

Critical Infrastructures

Justifications for economic espionage often focus on examples that stress the importance of protecting critical infrastructure, where there are high costs in terms of people's lives and general well-being. For example, Fabre puts forward the hypothetical case where "Green and Blue are at war, both kinetic and cyber. Corporation Weapons Inc. supplies Blue with military weapons and technology, while corporation InfoSys Inc. supplies its forces with IT resources." In this instance, she argues that if Blue is an unjust aggressor and Green is losing, then Green's leaders are morally justified in seeking to uncover relevant economic information about Weapons Inc. and InfoSys Inc. in the hope of "undermining

both firms by engaging in economic warfare.”⁴⁰ Fabre suggests that this point also applies to peacetime operations, stating that if Green has “good reasons to believe that the large multinational, ostensibly private corporation which is entrusted with the maintenance of its civilian nuclear reactors—Energy Inc.—has very close links with the regime of hostile state Blue,” then Green has a justification for seeking to obtain detailed operational information about the corporation. The argument is similar to the previous one—that “given that the health of its reactors is critical to Green’s national security broadly understood, Green’s leaders are justified in acquiring it against Blue’s wishes.”⁴¹ The central justification is that critical infrastructures play a pivotal role in people’s lives, by maintaining the state itself as well as often being a direct means for creating the necessary environment or provisions that allow for people to flourish. Therefore, if the purpose of the operation is to inform political elites in peacetime, reassuring them on the correct practice of a company that represents a key critical infrastructure agent, there is a clear justified gain, where the costs are limited to privacy violations.

However, these cases are mainly only concerned with informing political elites and do not fully consider the costs of using economic espionage in a competitive environment and the potential harm that can befall those who have done nothing to warrant it. Indeed, what is not clear in the scenarios outlined is whether a state can justifiably protect its own critical infrastructure when doing so would require harming another state’s critical infrastructure in the process. Suppose a new hypothetical where Blue and Red are both supplied by Oil Inc. from a third state, Green, and there is a fixed amount of supply that can be provided at any given time. Falling supplies cause an increase in oil prices, threatening the vital interests of both Red’s and Blue’s people, representing a broader societal-level threat to the political community as multiple systems shut down, resulting in a rise in the cost of living for people in both states and ultimately threatening the states’ abilities to function and the individual’s ability to fully flourish. The 2022 Russian invasion of Ukraine and the sudden and extensive European Union, United Kingdom, and United States responses demonstrate the quick and widespread measures states will take to secure their energy security, while the ensuing cost-of-living crises demonstrate the sensitivity of multiple systems to a single resource. Indeed, the global spike in oil prices following the Russian invasion played a key role in rising energy costs, inflation, slowing economies, and the restriction of resources for individuals in Europe and the United States.⁴² I would argue that the subsequent fuel poverty has had very real negative implications for people across a number of

societies, including access to resources, health, education, livelihood opportunities, and mental well-being.⁴³ In this hypothetical, Blue is concerned about such potential fallout and thus acquires secret information—whether operational, technical, or personal—that means it is able to force Oil Inc. to offer supply at a lower cost than that at which it offers Red such supply, and in doing so ends up taking more of the oil supply, resulting in less for Red and causing even-greater economic woes in that country. This kind of secret economic manipulation could have a justifiable reason in that Blue is facing an economic threat. But given that Blue's actions rely on critically damaging Red's own critical infrastructure; and that Red has not done anything to make its own position unjust; and that given the importance of oil in the continued existence of Red's people (thus giving it a general legitimate claim to a certain amount of oil), the impact is widely felt and is disproportionate.⁴⁴ The people ultimately harmed in the process are Red's citizens, who have not acted in such a way as to waive or forfeit their protective rights.

In response, some readers might object that those harms are a foreseeable but unintended casualty of Blue's actions, and so the doctrine of double effect could offer some cover for Blue. The doctrine of double effect argues that actions with foreseeable damage can be permitted when the harm is not directly intended, is not a means to achieving the end, and is proportionate with the damage it causes. With economic espionage, the objective is to provide information so that home companies or institutions can have an advantage in a system that relies on a competitive advantage. The failure of the opposition is not only foreseen but necessary. Moreover, the doctrine of double effect only holds true if the harms Blue inflicts on the innocent are proportionate to the gains it secures. The tension, therefore, is between the important benefit that gaining extra oil can bring to Blue, its economy, and its society and the required loss this would bring to Red.

At this juncture, it might be argued that all is fair in a competitive system, and that the capitalist market causes harm to people all the time. However, there is a difference between allowing harm to happen and directly causing it by one's intervention in order to support oneself.⁴⁵ Indeed, in a system where economic espionage is predominantly concerned with providing a competitive advantage and/or where economic gains will often come at a loss for another party, these wider implications need to be more explicitly included in the calculation. It is therefore not apt to say that Red's innocent citizens are collateral damage. I argue that it is more accurate to say that in this case Red's people are sacrificed for Blue's gain even though they have not acted in any way so as to justify being harmed.

What this case demonstrates is that the appropriation of economic information via espionage will naturally have far-reaching consequences that necessarily cause harm.

Private Economic Actors, Both Big and Small

A second area of economic espionage includes targeting private companies, ranging from small research and development start-ups; to research institutes and tech developers in Silicon Valley; to large tech companies such as Google, Adobe, IBM, Intel, and AMD that cover important but everyday industries, such as automobiles, computers, steel, software development, service provision, artificial intelligence, and chemical development.⁴⁶ For example, France's Directorate-General for External Security used penetration operations against IBM, Texas Instruments, and Corning Glass on behalf of Compagnie des Machines Bull; Japan targeted Silicon Valley in the 1980s looking for information on technological developments; and Romania targeted Mercedes-Benz in Stuttgart.⁴⁷ The CIA has also been criticized for targeting the French government over its negotiating strategy in relation to its international telecommunications strategy.⁴⁸ And during the Japanese-U.S. automotive trade talks, the "U.S. trade representative Mickey Kantor and his team of negotiators came to the table armed with information that the CIA and NSA had gathered," and the "CIA and NSA were eavesdropping on the Japanese delegation including Japan's Prime Minister Ryutaro Hashimoto."⁴⁹ Numerous (sometimes-anecdotal) reports refer to the rise of cyberattacks against tech companies being carried out by Russia, China, and North Korea.⁵⁰ For example, in 2010, Operation Aurora involved a series of cyberattacks from China that targeted the U.S. private sector, including Google. The attacks resulted in China having access to the emails of Chinese human rights activists as well as the source code to Google's proprietary systems.⁵¹

Take a scenario, therefore, involving a significant local employer from an industry where its ability to maintain a competitive edge is vital to its continued survival, especially in terms of research and development. Such a company might be an important local employer with worldwide distribution, bringing in capital directly and indirectly to the local population and the nation itself and providing important regional stability and education and employment opportunities. The company's continued success is important to the local economy and those who reside in the region, and even represents a boon for the wider nation, but its failure would not itself present a threat to the critical infrastructure of the state or

political community as a whole. For instance, reports indicate that the most frequently targeted private companies are those within industries such as aerospace, biotechnology, computer software and hardware, transportation, energy research, materials, and automotives. In these types of companies, the information taken by espionage operations can include proprietary and confidential business information such as “customer lists and information, product development data, pricing data, sales figures, marketing plans, personnel data, bid information . . . and strategic planning.”⁵² Each of the companies can represent an important economic actor, though individually its losses will not present a critical threat, as in the oil case. For example, an American company called EMC was hacked by a state-sponsored Chinese perpetrator, which took data that could be used to breach defenses of some systems guarded with its technology. The cyber intrusion resulted in “the loss of 700 jobs, including jobs from its Austrian subsidiary, and the loss in stock value of more than \$1 billion.”⁵³ Calculated annual financial costs to these types of private economic actors can reach \$400 billion, with job losses estimated to be at six million, while “the financial drain from such losses is considerable in lost market share, evaporating profits, increased information recovery costs, and continued security overheads.”⁵⁴ Estimates from the EU think tank European Centre for International Political Economy estimate economic espionage to cost up to €60 billion in economic growth and up to 289,000 jobs in the EU.⁵⁵

In this type of scenario, a competitor has developed, at a great investment cost, new technology that will make it more efficient. There is an argument, therefore, that political elites could provide for regional and national economies through their intelligence organizations by taking this technological advancement from the competitor without the physical and financial burden of the research and development. As a result, the company provided with the intelligence can bring to market the product at a cheaper rate, ultimately undercutting the competitor’s ability to sell its inventory at a profitable price.⁵⁶ The inability to advance can cause harm to a political community when those companies fail to be competitive and fail in the market, and so there could be a justifiable reason to act. It can be argued that providing such economic information allows for one’s own economy to be more stable and successful when it gives its private actors a competitive edge, which, in turn, can provide greater provision for people’s vital interests.

However, stealing that information and causing a competitor to fail as a result will also cause harm to those who are reliant on that business, and by doing so the

intelligence actor is placed as a direct causal factor in the subsequent harm that then befalls these dependents who are illegitimately harmed. A state promoting the strength of its own companies through financial support is not the same as causing harm to a competitor to facilitate the success of that state's economic actors. Again, those companies that are negatively impacted when an intelligence actor undercuts their costly competitive advantage are themselves not isolated islands but rather interconnected agents whose loss of economic security can cause further economic harms when they cease to be economic contributors. Those dependent on such companies are directly harmed by the loss of the income, and then these unemployed individuals cease to be able to financially contribute to their local and even national economies.

This emphasizes the previous point regarding collateral damage, and the limitations of the doctrine of double effect become starker. In cases where companies are in a competition for the same market share, promoting the strength of one's own companies through financial support is different from causing harm to a competitor to ensure one's own success. It is fine to pay for medical treatment for your own patients, but it is unjustified to steal money from someone else when that theft is going to make that person equally or more ill. There is an important ethical distinction between killing someone and letting them die.⁵⁷ Stealing that information and causing the competitor to fail as a result will cause harm to those who are reliant on that business, and doing so places one as a direct causal factor in the subsequent harm that then befalls those dependents who are illegitimately harmed.

In addition, persistent and wide-ranging attacks can place far-reaching and underlying economic burdens on economic actors both at the local and societal level. Economic espionage can significantly erode the value of the target state's assets, disrupt trade between target states and potential buyers, discourage innovation, destroy competitive advantage and stifle economic momentum, and undermine current business plans and profit projections, thereby forcing companies to recoup research costs by passing them onto the consumer and weakening military alliances and trade coalitions, which promotes international instability.⁵⁸ As such, "when conducted systematically or on a large scale [economic espionage] can erode a country's economy by removing the competitive edge of its private companies, undermining the return on those companies' investments in research and design . . . and transferring large amounts of wealth (in the form of valuable information) to foreign competitor companies who have not made such

investments.”⁵⁹ So, while it could be argued that carrying out such practices is needed to bring success to one’s own economy, there are costs suffered by those who have not forfeited their normal protective rights.

CONCLUSION

The ethical costs associated with economic espionage might initially feel low because of the way the impact is often disaggregated and nondirect. So construed, economic espionage appears to be a victimless crime: you can steal information and directly hurt no one, while bringing a benefit to the population of the intelligence actor’s community. But, in practice, the costs are real and impact people in ways that directly alter their everyday lives. Therefore, the principles of discrimination and proportionality need greater attention, the result of which raises the bar on economic espionage significantly.

NOTES

- ¹ Ross W. Bellaby, *The Ethics of Intelligence: A New Framework* (Abingdon, U.K.: Routledge, 2014), p. 6.
- ² Cécile Fabre, *Spying through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence* (Oxford: Oxford University Press, 2022), p. 29.
- ³ Ross W. Bellaby, “Redefining the Security Paradigm to Create an Intelligence Ethic,” *Intelligence and National Security* 37, no. 6 (2022), pp. 863–73.
- ⁴ Michael Quinlan, “Just Intelligence: Prolegomena to an Ethical Theory,” *Intelligence and National Security* 22, no. 1 (2007), pp. 1–13, at p. 7.
- ⁵ Rory Cormac, “Secret Intelligence and Economic Security: The Exploitation of a Critical Asset in an Increasingly Prominent Sphere,” *Intelligence and National Security* 29, no. 1 (January 2014), pp. 99–121, at p. 99.
- ⁶ Fabre, *Spying through a Glass Darkly*, p. 81.
- ⁷ Hedieh Nasheri, *Economic Espionage and Industrial Spying* (Cambridge, U.K.: Cambridge University Press, 2005), p. 1.
- ⁸ Evan H. Potter, ed., introduction to *Economic Intelligence & National Security* (Montreal: McGill-Queen’s University Press, 1998), p. 1.
- ⁹ Stansfield Turner, quoted in Loch K. Johnson, *Secret Agencies: U.S. Intelligence in a Hostile World* (New Haven, Conn.: Yale University Press, 1998), p. 152.
- ¹⁰ Fabre, *Spying through a Glass Darkly*, p. 85.
- ¹¹ Joy Gordon, “Economic Sanctions, Just War Doctrine, and the ‘Fearful Spectacle of the Civilian Dead,’” *CrossCurrents* 49, no. 3 (Fall 1999), pp. 387–400, at p. 398. See also Joy Gordon, “Smart Sanctions Revisited,” *Ethics & International Affairs* 25, no. 3 (Fall 2011), pp. 315–35; Joy Gordon, “A Peaceful, Silent, Deadly Remedy: The Ethics of Economic Sanctions,” *Ethics & International Affairs* 13 (March 1999), pp. 123–42; and Elizabeth Ellis, “The Ethics of Economic Sanctions: Why Just War Theory Is Not the Answer,” *Res Publica* 27, no. 3 (2021), pp. 409–26.
- ¹² Melanie Reid, “A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing with this Global Threat?,” *University of Miami Law Review* 70, no. 3 (Spring 2016), pp. 761–63; Brian Champion, “A Review of Selected Cases of Industrial Espionage and Economic Spying, 1568–1945,” *Intelligence and National Security* 13, no. 2 (Summer 1998), pp. 123–43, at p. 124; Mark E. A. Danielson, “Economic Espionage: A Framework for a Workable Solution,” *Minnesota Journal of Law, Science & Technology* 10, no. 2 (Spring 2009), at p. 504; Chris Carr and Larry Gorman, “The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act,” *Business Lawyer* 57, no. 1 (November 2001), pp. 25–53, at pp. 26, 30; Karen Sepura, “Economic Espionage: The Front Line of a New World Economic War,” *Syracuse Journal of International Law and Commerce* 26, no. 1 (Fall 1998), pp. 137–38; and Potter, introduction to *Economic Intelligence & National Security*, p. 1.

- ¹³ Distinctions can be made between “costs,” “damages,” “harm,” and “wrongful harm.” For the purpose of this essay, harm refers to violations of people’s vital interests, which can be detailed separately according to whether it then becomes a wrongful harm inflicted unjustly or wrongfully. See Joel Feinberg, *The Moral Limits of the Criminal Law*, vol. 1, *Harm to Others* (Oxford: Oxford University Press, 1984), p. 37. Costs and damages are more widely conceived and can include all types of losses inflicted, which, in turn, may or may not be harms.
- ¹⁴ Quinlan, “Just Intelligence,” p. 1.
- ¹⁵ David Omand, “Reflections on Secret Intelligence,” in Peter Hennessy (ed.), *The New Protective State: Government, Intelligence and Terrorism* (London: Continuum, 2007), at p. 116.
- ¹⁶ Quinlan, “Just Intelligence,” p. 1; David Omand, “The Dilemmas of Using Secret Intelligence for Public Security,” in Hennessy, *The New Protective State*, pp. 142–69, at p. 148; and Michael Herman, “Ethics and Intelligence after September 2001,” *Intelligence and National Security* 19, no. 2 (Summer 2004), pp. 342–58, at p. 342.
- ¹⁷ Feinberg, *The Moral Limits of the Criminal Law*, p. 62.
- ¹⁸ Martha C. Nussbaum, *Women and Human Development: The Capabilities Approach* (Cambridge, U.K.: Cambridge University Press, 2000), p. 73.
- ¹⁹ Quinlan, “Just Intelligence,” p. 2; Bellaby, *The Ethics of Intelligence*, p. 24; Angela Gendron, “Just War, Just Intelligence: An Ethical Framework for Foreign Espionage,” *International Journal of Intelligence and CounterIntelligence* 18, no. 3 (2005), pp. 398–434; Kevin Macnish, “Just Surveillance? Towards a Normative Theory of Surveillance,” *Surveillance & Society* 12, no. 1 (March 2014), pp. 142–53; David Omand and Mark Phythian, “Ethics and Intelligence: A Debate,” *International Journal of Intelligence and CounterIntelligence* 26, no. 1 (2013), pp. 38–63; and Omand, “The Dilemmas of Using Secret Intelligence for Public Security,” p. 157.
- ²⁰ Fabre, *Spying through a Glass Darkly*, p. 81.
- ²¹ Fabre discusses this right to defend others more extensively in other works, arguing that the victim’s fundamental interest in surviving an attack is “protected by a prima facie power to transfer that right to a third party . . . to claim otherwise is to impose an arbitrary restriction on V’s [the victim’s] ability to promote this fundamental interest of hers.” The duty created not only prevents violating an individual’s right to life but also actively promotes the avoidance by others of violating that right and allows defenders to intervene when appropriate. See Cécile Fabre, *Cosmopolitan War* (Oxford: Oxford University Press, 2012), p. 63.
- ²² See Danielson, “Economic Espionage,” p. 503; and Fabre, *Spying through a Glass Darkly*, p. 72.
- ²³ Fabre, *Spying through a Glass Darkly*, p. 73.
- ²⁴ Bellaby, *The Ethics of Intelligence*, p. 23.
- ²⁵ Fabre, *Spying through a Glass Darkly*, p. 77.
- ²⁶ *Ibid.*, p. 83.
- ²⁷ See Bellaby, *The Ethics of Intelligence*; and Ross W. Bellaby, “Justifying Cyber-Intelligence?,” *Journal of Military Ethics* 15, no. 4 (2016), pp. 299–319.
- ²⁸ Fabre, *Spying through a Glass Darkly*, p. 83.
- ²⁹ See Nussbaum, *Women and Human Development*; and Timothy Weidel, “Moving towards a Capability for Meaningful Labor,” *Journal of Human Development and Capabilities* 19, no. 1 (2018), pp. 70–88.
- ³⁰ International Committee of the Red Cross, “The Geneva Conventions of August 12, 1949”; and Art. 13, “Protection of Civilian Population,” in Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, “Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II),” §2, June 8, 1977; Michael S. Moore, *Placing Blame: A Theory of Criminal Law* (Oxford: Oxford University Press, 2010), p. 87.
- ³¹ Thomas Nagel, *The View from Nowhere* (Oxford: Oxford University Press, 1986), p. 162.
- ³² Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: Basic Books, 2000), p. 145.
- ³³ Fabre, *Spying through a Glass Darkly*, p. 81.
- ³⁴ *Ibid.*, pp. 19–20. See also p. 30.
- ³⁵ *Ibid.*, p. 20.
- ³⁶ *Ibid.*, p. 82.
- ³⁷ *Ibid.*, p. 76.
- ³⁸ See, for example, Jordan T. Camp and Christina Heatherton, eds., *Policing the Planet: Why the Policing Crisis Led to Black Lives Matter* (London: Verso Books, 2016); David A. Harris, “Driving while Black’ and All Other Traffic Offenses: The Supreme Court and Pretextual Traffic Stops,” *Journal of Criminal Law and Criminology* 87, no. 2 (1997), pp. 544–82; Randall Kennedy, *Race, Crime, and the Law* (New York: Pathone, 1997); Annabelle Lever, “Why Racial Profiling Is Hard to Justify: A Response

- to Risse and Zeckhauser,” *Philosophy & Public Affairs* 33, no. 1 (January 2005), pp. 94–110; Matthew Robinson, “The Construction and Reinforcement of Myths of Race and Crime,” *Journal of Contemporary Criminal Justice* 16, no. 2 (May 2000), pp. 133–56; Santiago Lago, David Cantarero, Berta Rivera, Marta Pascual, Carla Blázquez-Fernández, Bruno Casal, and Francisco Reyes, “Socioeconomic Status, Health Inequalities and Non-Communicable Diseases: A Systematic Review,” *Journal of Public Health* 26 (February 2018), pp. 1–14; and Gerry McCartney, Chik Collins, and Mhairi Mackenzie, “What (or Who) Causes Health Inequalities: Theories, Evidence and Implications?,” *Health Policy* 113, no. 3 (December 2013), pp. 221–27.
- ³⁹ See Carr and Gorman, “The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act,” p. 27.
- ⁴⁰ Fabre, *Spying through a Glass Darkly*, p. 82.
- ⁴¹ *Ibid.*, p. 82.
- ⁴² Julien Le Roux, Béla Szörfi, and Marco Weißler, “How Higher Oil Prices Could Affect Euro Area Potential Output,” *Economic Bulletin Boxes* 5 (2022), European Central Bank, pp. 1–105; and World Bank Group Publications, “Russia’s Invasion of Ukraine: Implications for Energy Markets and Activity,” *Global Economic Prospects* (June 2022).
- ⁴³ Christine Liddell and Chris Morris, “Fuel Poverty and Human Health: A Review of Recent Evidence,” *Energy Policy* 38, no. 6 (June 2010), pp. 2987–97; Marmot Review Team, *The Health Impacts of Cold Homes and Fuel Poverty* (London: Friends of the Earth, 2011), www.instituteofhealthequity.org/resources-reports/the-health-impacts-of-cold-homes-and-fuel-poverty/the-health-impacts-of-cold-homes-and-fuel-poverty.pdf; Alice Lee, Ian Sinha, Tammy Boyce, Jessica Allen, and Peter Goldblatt, *Fuel Poverty, Cold Homes and Health Inequalities in the UK* (London: Institute of Health Equity, 2022), www.instituteofhealthequity.org/resources-reports/fuel-poverty-cold-homes-and-health-inequalities-in-the-uk/read-the-report.pdf; and Yiming Xiao, Han Wu, Guohua Wang, and Shangrui Wang, “The Relationship between Energy Poverty and Individual Development: Exploring the Serial Mediating Effects of Learning Behavior and Health Condition,” *International Journal of Environmental Research and Public Health* 18, no. 16 (August 2021), pp. 1–14.
- ⁴⁴ Green could decide to restrict oil to Blue, Red, or both, but whether Green’s actions are justified or not is a separate ethical debate. Interesting discussions on whether Green necessarily has to offer oil or whether there is an expectation to have a certain amount of access to a fundamental resource in the international economic system are outside the scope of this essay, as the focus here is on whether the actions of Blue are ethically justified when it will knowingly and necessarily cause critical harm to Red through its intervention.
- ⁴⁵ Judith Jarvis Thomson, “Turning the Trolley,” *Philosophy & Public Affairs* 36, no. 4 (Fall 2008), pp. 359–74.
- ⁴⁶ Danielson, “Economic Espionage,” p. 505.
- ⁴⁷ Johnson, *Secret Agencies*, p. 153.
- ⁴⁸ Nasheri, *Economic Espionage and Industrial Spying*, p. 21.
- ⁴⁹ *Ibid.*, p. 22.
- ⁵⁰ Brenda I. Rowe, “Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire,” *Security Journal* 33 (March 2020), pp. 63–82, at p. 64.
- ⁵¹ Operation Aurora, *Council on Foreign Relations*, January 2010, available at www.cfr.org/cyber-operations/operation-aurora. Also see Jothy Rosenberg, “Security in Embedded Systems,” chap. 6 in Augusto Vega, Pradip Bose, and Alper Buyuktosunoglu, *Rugged Embedded Systems: Computing in Harsh Environments* (Cambridge: Morgan Kaufman / Elsevier, 2017).
- ⁵² Carr and Gorman, “The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act,” pp. 27–28.
- ⁵³ PricewaterhouseCoopers, *The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber* (Luxembourg: Publications Office of the European Union, 2018), p. 28 (boldface removed).
- ⁵⁴ Nasheri, *Economic Espionage and Industrial Spying*, p. 58; and Champion, “A Review of Selected Cases of Industrial Espionage and Economic Spying, 1568–1945,” p. 124.
- ⁵⁵ Hosuk Lee-Makiyama, *Stealing Thunder: Cloud, IoT and 5G Will Change the Strategic Paradigm for Protecting European Commercial Interests. Will Cyber Espionage Be Allowed to Hold Europe Back in the Global Race for Industrial Competitiveness?* (ECIPE Occasional Paper No. 2/18, European Centre for International Political Economy, 2018), ecipe.org/publications/stealing-thunder/?chapter=all.
- ⁵⁶ This, for example, happened in the industrial espionage tried in the *Gillette v. Davis* case in 1997, where Davis leaked extensive trade secrets to competitors that could have represented a fatal blow to Gillette, as the company had ploughed \$750 million into development and if it did not achieve the return, it would have failed. See Mark Maremont and Joseph Pereira, “Gillette Engineer Indicted

for Stealing Trade Secrets,” *Wall Street Journal*, September 26, 1997, www.wsj.com/articles/SB875205465477700500.

⁵⁷ Thomson, “Turning the Trolley”; and Helen Frowe, “Killing John to Save Mary: A Defense of the Moral Distinction between Killing and Letting Die,” in Joseph Keim Campbell, Michael O’Rourke, and Harry S. Silverstein (eds.), *Action, Ethics and Responsibility* (Cambridge, Mass.: MIT Press, 2010), pp. 47–66; and Philippa Foot, *Moral Dilemmas and Other Topics in Moral Philosophy* (Oxford: Oxford University Press, 2002), pp. 78–87.

⁵⁸ Danielson, “Economic Espionage,” p. 507.

⁵⁹ Rowe, “Transnational State-Sponsored Cyber Economic Espionage,” p. 65.

Abstract: The ethical value of intelligence lies in its crucial role in safeguarding individuals from harm by detecting, locating, and preventing threats. As part of this undertaking, intelligence can include protecting the economic well-being of the political community and its people. Intelligence, however, also entails causing people harm when it violates their vital interests through its operations. The challenge, therefore, is how to reconcile this tension, which Cécile Fabre’s recent book *Spying through a Glass Darkly* does by arguing for the “ongoing and preemptive imposition of defensive harm.” Fabre applies this underlying argument to the specifics of economic espionage to argue that while states, businesses, and individuals do have a general right over their information that prevents others from accessing it, such protections can be forfeited or overridden when there is a potential threat to the fundamental rights of third parties. This essay argues, however, that Fabre’s discussion on economic espionage overlooks important additional proportionality and discrimination concerns that need to be accounted for. In addition to the privacy violations it causes, economic espionage can cause harms to people’s other vital interests, including their physical and mental well-being and autonomy. Given the complex way in which the economy interlinks with people’s lives and society, harms to one economic actor will have repercussions on those secondary economic entities dependent on them, such as workers, buyers, and investors. This, in turn, can produce further harms on other economic actors, causing damages to ripple outward across society.

Keywords: economic espionage, ethics, intelligence, proportionality, discrimination