The Ethics of Economic Espionage

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 intelligence can include protecting the economic wellbeing 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 of the book to the specifics of economic espionage to argue that while states, businesses, or individuals do have a general right over their information which 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.

It will be argued, however, that the 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, which in turn can cause further harms to other economic actors, causing damages to ripple outwards across society and causing further harm to others who may not have acted in a way to be justifiably harmed.

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

Ross Bellaby, PhD, is a Senior Lecturer at the University of Sheffield's Politics Department. His main research examines the application of ethics to violence, with specific attention to developing ethical frameworks for intelligence activity.

INTRODUCTION

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 it necessarily involves violating the vital interests of others when intelligence policy or practice violates these vital interests in another 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 to

know if and when another's vital interests can be violated in order to secure one's own.[1] Cécile Fabre's recent book, *Spying Through a Glass Darkly*, does this 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 defense of others without thereby infringing their right'.[2] Intelligence is therefore permissible even though it harms others as a form of self-defense.

While in the intelligence community this is often framed as averting direct attacks against critical infrastructure or protecting human life, people can face a range of different threats that can 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, 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 to both "traditional concepts of national interest and politico-military security,"[5] as well as representing 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 U.S.'s economic advantage 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 on its use. Fabre applies the underlying argument of the book to the specifics of economic espionage to argue that while states, businesses, or individuals do have a general right over their information which 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 works generally 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 cause harm to those who have not acted in a way as to be justified targets. This is analogous to Joy Gordon's argument against economic sanctions where those who are the least involved and potentially the most vulnerable are harmed and its fails the principle of discrimination.[11] It will be argued that economic espionage aims to provide one's own a competitive advantage, but where this economic benefit espionage brings to one actor will necessarily come at the cost of another who has not necessarily done anything to warrant it. Economic espionage works to give one's own a competitive advantage over another by gathering information from competitors so that they can produce their goods or services at a greater rate, at a higher quality, and/or for a lower cost with the aim of increasing their market share at the expense of these competitors. [12] So when the intelligence community intervenes to achieve success for economic actors within their home state, they are 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 widely spread across society, more readily than other forms of intelligence activity, and will result in widespread harm on those who have done nothing to warrant it. Significant harms or costs to one economic actor will have repercussions on those secondary economic entities dependent on them, such as workers, buyers, and investors, which in turn can cause further harms to tertiary economic actors dependent on them and then their own workers, causing damages to ripple outwards across society and causing further harm to others who 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 centre of the tension in intelligence ethics is the conflict between there being aspects of the intelligence business that seem "notably disreputable"[14] and 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, defence and government, have all 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 which 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 fulfil 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 their 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 is harmed.[18]

The ethical justification for intelligence, therefore, recognizes both the need to 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 does this by arguing that the "main rationale for 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 defense of others. Cecile 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".[21] This duty created not only prevents violating an individual's right to life but also actively promotes others to avoid violating it and allows defenders to intervene when appropriate.

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 targets 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 one has 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, however, can be justified when it is done to protect people from more significant harms when it "targets a business whose activities, threaten a state's national security understood more broadly as comprising, not just as military security what is security, exquisite 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 discriminate between legitimate and illegitimate targets. While these additional criteria of proportionality and discrimination are mentioned in Fabre's chapter 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 represents an important threat to people's other vital interests such as their physical and mental wellbeing, and autonomy. This can be 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, 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 for people having the opportunity to in fulfil their autonomy and mental wellbeing through contributing economically. 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 one is 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" to justify targeting them.[31] One becomes a legitimate target—that is, has acted so that their normal protections have been waived—for example, by voluntarily suspending their rights such as by joining a particular profession or group.[32] Or they can forfeit them 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 agents 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 toward those who are ultimately innocent.[35] In unpacking this it can be argued that the ends are 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 it involves interests that are equal importance, but protects such 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 can be made. Firstly, a distinction can be made between economic espionage collected to inform or reassure political elites in comparison to espionage to collect information which is then used by the political elites for some policy or activity. While Fabre focuses on the former in the 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 as many of the known examples detail how the economic 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.

Secondly, 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 a justified target or not. For example, wiretapping a specific target 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 those 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 just confined to those directly engaged but also with other actors who are dependent on these initial economic targets who are forced to suffer the impact of any resulting economic losses, which in turn can violate their vital interests as they lose access to resources or opportunities necessary to fulfil their continued existence or their ability to fully realize their autonomy. In turn, any failing promoted in these secondary economic actors can then be further passed on to 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, it does not necessarily mean those who are reliant on them are 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 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 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 is far greater than the simple sum of their individual harms. This is especially true for those in particular cultural, racial, or geographic groups, for whom the harm negatively affects social cohesion, wellbeing, and stability, which can then in turn cause further harms and loss of opportunities. For example, 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 an 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 not important nor foreseeable 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, it is also that those harmed have done nothing to warrant it. 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 significant value to be part of the justification.

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 as well as in the few known cases. 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 and economically significant actors as well as emerging startups. Something that will emerge is that of those known cases of economic espionage many are carried out against non-critical actors for non-critical returns,[39] which 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 wellbeing. 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, Fabre 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 argues that this point also applies to peacetime operations, stating that if Green has "good reason to believe that the large multinational, ostensibly private corporation which is entrusted with the maintenance of its civil nuclear reactors–Energy Inc.–has very close ties 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 the 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 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 concerned with only 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 their own critical infrastructure when doing so would require harming another state's critical infrastructure in the process. Suppose 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 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 threating 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, UK and US responses demonstrate the quick and widespread measures states will perform to secure their energy security while the ensuing cost of living crisis for many demonstrated the sensitivity of multiple systems to a single resource. Indeed, the spike in oil prices following the Russian invasion arguably played a key exacerbator for the rise in energy costs, inflation, slowing economies and restriction of resources for individuals.[42] The impact of the subsequent fuel poverty can be argued to have very real negative implications for people across a number of societies, including access to resources, health, education, livelihood opportunities, and mental wellbeing.[43] In the hypothetical outlined, concerned about such potential ramifications Blue acquires secret information—whether operational, technical, or personal—that means it is now able to force Oil Inc. to offer supply at a lower cost than it offers Red, 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, that Red has not done anything to make its own position unjust, and given the importance of oil in the continued existence of its people and so has 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 so 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 in 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 if the harms Blue inflicts on the innocent are proportionate to the gains it secures. The tension, therefore, is between the important benefit gaining extra oil can bring to Blue, its economy and society and the loss this would bring to Red. Taking oil as an example of a resource which is still highly valuable to many societies, and whose loss can cause wider economic ramifications that can have important negative effects across a variety of economic sectors and actors, and assuming that both Red and Blue are equally dependent on it, even though the extra oil would promote greater economic stability to Blue, this comes at a direct cost to Red that has the potential to cause deeper significant harms.

At this juncture, it might be thought 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 someone else, 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, research institutes and tech-developers in Silicon Valley, to large tech-companies such as Google, Adobe, IBM, Intel, and AMD, covering important but everyday industries, such as automotives, computers, steel, software development, service providers, artificial intelligence and chemical development.[46] For example, French Directorate-General for External Security (DGSE) 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. 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 that 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 cyber-attacks 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 attack 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 such an industry where its ability to maintain a competitive edge is vital to its continued survival, especially in terms of research and development. Such companies can represent an important local employer with a world-wide distribution, bringing in capital directly and indirectly to the local population and the nation itself, providing important regional stability, and education and employment opportunities. Their continued success is important to the local economy and those who reside there, and even represents a boon for the wider nation, but whose failure would not itself represent a threat to the critical infrastructure of the state or political community as a whole. For instance reports indicate

that the most frequently targeted are such private companies within industries including aerospace, bio-technology, computer software and hardware, transportation, energy research, materials, automotives, and where the information taken 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] Individual companies can represent an important economic actor, though individually their losses will not represent the critical threat as in the oil case. For example, an American company called EMC, was hacked by a state-sponsored Chinese perpetrator, taking data that could be used to breach defences 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] Costs to these types of private economic actors have a calculated financial annual cost of up to $400 billion, with job losses estimated to be at 6 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] While estimates from the EU think tank ECIPE estimate economic espionage to cost up €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 great investment cost, new technology that will make them 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 their inventory at a profitable price.[56] Failure 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 one's 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 cause harm to those who are reliant on that business as well, 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 are 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 your own companies through financial support is different from causing harm to a competitor to ensure your own success. It is fine to pay for your own patients to receive medical treatment, but it is unjustified to steal money from someone else when that theft is going to make them equally or more ill. There is an important ethical distinction between killing and letting 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 these 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, undermine current business plans and profit projections, forcing companies to recoup research costs by passing them onto the consumer, and weaken military alliances and trade coalitions, promoting international instability.[58] As such, "when conducted systematically or on a large scale it 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 are needed to bring success to one's own, 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 non-direct. So construed, economic espionage appears to be a victimless crime: steal information and no one is directly hurt, while bringing 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.

[1] Ross Bellaby, *The Ethics of Intelligence: A New Framework* (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 Bellaby, "Redefining the security paradigm to create an intelligence ethic," *Intelligence and National Security* 37, no.6 (2022), pp.863-873.
[4] Michael Quinlan, "Just Intelligence: Prolegomena to an Ethical Theory," *Intelligence and National Security* 22, no. 1 (2007), 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 (2015), p.99.
[6] Cécile Fabre, *Spying Through a Glass Darkly,* University Press, p. 81.
[7] Hedieh Nasheri, *Economic Espionage and Industrial Spying* (Cambridge: Cambridge University Press, 2005), p. 1.
[8] Evan Potter, ed., *Economic Intelligence and National Security* (McGill-Queen's University Press*,* 1998), p. 1.
[9] Loch Johnson, *Secret Agencies: U.S. Intelligence in a Hostile World* (Yale University Press, 1998), p. 152.
[10] Cécile Fabre, *Spying Through a Glass Darkly,* University Press, p. 85.
[11] Joy Gordon, "Economic Sanctions, Just War Doctrine, and the 'Fearful Spectacle of the Civilian Dead,'" *CrossCurrents* 49, no.3 (1999), p.398. Also see Joy Gordon, "Smart Sanctions Revisited," *Ethics and International Affairs* 25, no.3 (2011), pp. 315-335; Joy Gordon, "A Peaceful, Silent, Deadly Remedy: The Ethics of Economic Sanctions," *Ethics and International Affairs* 13, (1999), pp. 123-142; Elizabeth Ellis, "The Ethics of Economic Sanctions: Why Just War Theory is Not the Answer," *Res Publica* 27, (2021), pp. 409-426.
[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 (2016) pp.761-763; Brian Champion, "A Review of Selected Cases of Industrial Espionage and Economic Spying, 1568-1945," *Intelligence and National Security* 13, no.2 (1998) p. 124; Mark E.A. Danielson, "Economic Espionage: A Framework for a Workable Solution," *Minnesota Journal of Law, Science & Technology* 10, no. 2 (2009), p. 504; Chris Carr & Larry Gorman, "The Revictimization of Companies by the Stock Market who Report Trade Secret Theft under the Economic Espionage Act," *The Business Lawyer* 57, no.1 (2001) p. 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 (1998) pp. 137-138; Evan Potter, ed., *Economic Intelligence and National Security* (McGill-Queen's University Press*,* 1998), p. 1.
[13] Distinctions can be made between 'costs', 'damages', 'harm' and 'wrongful harm'. For the purpose of this paper, harm is referring to violations of people's vital interests, which can be detailed separately as to whether it is then a wrongful harm as it is inflicted unjustly or wrongfully. See Joel Feinberg, *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] Michael Quinlan, "Just Intelligence: Prolegomena to an Ethical Theory," *Intelligence and National Security* 22, no.1 (2007) p. 1
[15] David Omand, "Reflections on Secret Intelligence" in *The New Protective State: Government, Intelligence and Terrorism* edited by Hennessy, P. (London: Continuum, 2007) p. 116
[16] Michael Herman, "Ethics and Intelligence after September 2001," *Intelligence and National Security* 19, no.2 (2004) p.342; David Omand, "The Dilemmas of Using Secret Intelligence for Public Security," in *New Protective State: Government, Intelligence and Terrorism* edited by Peter Hennessy, (London: Continuum, 2007) p. 148; Quinlan, "Just Intelligence", p.1
[17] Joel Feinberg, *Moral Limits of the Criminal Law,* p. 62
[18] Martha Nussbaum, *Women and Human Development: The Capabilities Approach* (Cambridge: 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 (2014), pp. 142-153; David Omand and Mark Phythian, "Ethics and Intelligence: A Debate," *International Journal of Intelligence and CounterIntelligence* 26, no. 1 (2013), pp. 38-63; David Omand, "The Dilemmas of Using Secret Intelligence for Public Security," in *New Protective State: Government, Intelligence and Terrorism*, Peter Hennessy, ed., (London: Continuum, 2007), p. 157.
[20] Fabre, *Spying Through a Glass Darkly*, p. 81
[21] Cecile Fabre, *Cosmopolitan War* (Oxford: Oxford University Press, 2012) p. 63
[22] See Mark E.A. Danielson, "Economic Espionage: A Framework for a Workable Solution," *Minnesota Journal of Law, Science & Technology* 10, no. 2 (2009), p. 503; 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*; Ross Bellaby, "Justifying Cyber-Surveillance," *Journal of Military Ethics* 15, no. 4 (2016), pp. 299-319.
[28] Fabre, *Spying Through a Glass Darkly*, p.83
[29] See Martha Nussbaum, *Women and Human Development*; Timothy Weidel, "Moving Towards a Capability Meaningful Labor,' *Journal of Human Development and Capabilities* 19, no. 1 (2018), pp. 70-88.
[30] Geneva 1949; 1977 *Geneva Protocol II Additional to the Geneva Convention of 1949: The Protection to of Victims of Armed Conflicts Section* Chapter 11 'Protection of Civilian Population' Article 51 §2; Michael Moore *Placing Blame: A Theory of Criminal Law* (Oxford: Oxford University Press, 2010) p.87; Jeffrie G. Murphy, "Legal Moralism and Retribution Revisited," *Criminal Law and Philosophy*, 1 (2007) p. 1
[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, 30.
[35] Ibid., p.20
[36] Ibid., p.82
[37] Ibid., p.76.
[38] For example see, Christina Heatherton and Jordan T. Camp, *Policing the Planet: Why the Policing Crisis Led to Black Lives Matter* (Verso Books, 2016); David A. Harris, "Driving While Black and Other Traffic Offences: The Supreme Court and Pretextual Traffic Stops," *The Journal of Criminal Law and Criminology* 87, (1999), pp. 544-582; Randall Kennedy, *Race Crime and the Law* (New York: Patheon, 1997); Annabelle Lever, "Why Racial Profiling is Hard to Justify: A Response to Risse and Zeckhauser," *Philosophy and Public Affairs* 33, no.1 (2005), pp. 94-110; and Matthew Robinson, "The Construction and Reinforcement of the Myth of Race Crime," *Journal of Contemporary Criminal Justice* 16, (2000), pp. 133-156; 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 (2018), pp. 1-14; Gerry McCartney, Chik Collins and Mhairi Mackenzie "What (or who) causes health inequalities: Theories, evidence and implications?," *Health Policy* 113, no.3 (2013), pp. 221-227.
[39] See Chris Carr & Larry Gorman, "The Revictimization of Companies by the Stock Market who Report Trade Secret Theft under the Economic Espionage Act," *The Business Lawyer* 57, no.1 (2001), p.27.
[40] Fabre, *Spying Through a Glass Darkly*, 82
[41] Ibid., 82.

[42] Julien Le Roux, Bela Szörfi and Marco Weißler, "How Higher Oil Prices Could Affect Euro Area Potential Outpu," *European Central Bank Economic Bulletin* 5, (2022), pp. 1-105; World Bank, "Russia's invasion of Ukraine: Implications for Energy Markets and Activity," *Global Economic Prospects: Special Focus, 2* June 2022.

[43] Christine *Liddell and Chris Morris,* "Fuel poverty and human health: A review of recent evidence," *Energy Policy* 38, no.6 (2010), pp.2987-2997*;* Marmot Review Team*, "*The Health Impacts of Cold Homes and Fuel Poverty," *Friends of the Earth and the Marmot Review Team* (2011). Available at http://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 Goldblatt, "Fuel Poverty, Cold Homes and Health Inequalities in the UK" *Institute of Health Equity* (2022) available at https://www.instituteofhealthequity.org/resources-reports/fuel-poverty-cold-homes-and-health-inequalities-in-the-uk/read-the-report.pdf; Yiming Xiao, Han Wu, Guohua Wang, 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 (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 paper, as the focus of the question here is the whether the actions of Blue are ethically justified when it will knowingly and necessarily cause critical harm to Red through its intervention.

[45] Judith J. Thomson, "Turning the Trolly," *Philosophy & Public Affairs* 36, no.4 (2008), pp. 359-374

[46] Danielson, "Economic Espionage," p. 505.

[47] Johnson, *Secret Agencies,* p. 153.

[48] Nasheri, *Economic Espionage and Industrial Spying,* p. 21

[49] Ibid., 22.

[50] Brenda I. Rowe, "Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire," *Security Journal* 33 (2020), p. 64.

[51] Jothy Rosenberg, "Security in Embedded Systems," in Augusto Vega, Pradip Bose, and Alper Buyuktosunoglu, eds., *Rugged Embedded Systems: Computing in Harsh Environments* (Morgan Kauffman, 2017).

[52] Chris Carr & Larry Gorman, "The Revictimization of Companies by the Stock Market," pp. 27-28

[53] PricewaterhouseCoopers "The Scale and Impact of Industrial Espionage and Theft of Trade Secrets Through Cyber**,"** *European Commission* (2018) p. 28.

[54] Nasheri, *Economic Espionage and Industrial Spying*, p. 58; Brian Champion, "A Review of Selected Cases of Industrial Espionage and Economic Spying, 1568-1945," *Intelligence and National Security* 13, no. 2 (1998), p. 124.

[55] Hosuk Lee-Makiyama**,** "Stealing thunder, Cloud, IoT and 5G paradigm for protecting European commercial interests. Will Cyber espionage be allowed to hold Europe Back in the global race for industrial competitiveness?," *European Centre for International Political Economy* (2018) Available at: http://ecipe.org/publications/stealing-thunder/?chapter=all

[56] For example, in the industrial espionage of Gillette Vs Davis case in 1997, where Davis leaked extensive trade secrets to competitors that could have represented a fatal blow to Gillette, as they had ploughed $750 million into the development and if they did not achieve their return the company would have failed. See Mark Maremont and Joseph Pereira, "Gillette Engineer Indicted for Stealing Trade Secrets" *The Wall Street Journal,* 26 September 1997, available at https://www.wsj.com/articles/SB875205465477700500

[57] Judith J. Thomson, "Turning the Trolly", *Philosophy & Public Affairs* 36, no.4 (2008), pp. 359-374; Helen Frowe, "Killing John to save Mary: a defence of the moral distinction between killing and letting die*",* in Campbell, J., O'Rourke, M. and Silverstein, H. (eds.) *Topics in Contemporary Philosophy: Action, Ethics and Responsibility.* (MIT Press, Cambridge, Massachusetts, 2010); Philippa Foot, *Moral Dilemmas: and Other Topics in Moral Philosophy,* (Oxford: Oxford University Press, 2002) pp. 78-87.

[58] Mark E.A. Danielson, "Economic Espionage" p. 507.

[59] Rowe, "Transnational State-Sponsored Cyber Economic Espionage," p. 65.