

IMSISS Programme Master Thesis

BETWEEN THE EXPLOITATION AND BENEFIT:  
INTERNATIONAL AND NON-GOVERNMENTAL ORGANISATIONS  
IN INTELLIGENCE OPERATIONS

Student no.

UoG No 2338123S

DCU No 17116350

CU No 73993807

Word count: 22 268

Submission date: 2019-07-19

## ABSTRACT

In some operations, national intelligence agencies decide to use International and Non-governmental organisations (INGOs) as a cover for intelligence gathering or covert action. Publicised cases of such operations show that while it can be effective in achieving intelligence goals, these operations might bring negative consequences to both actors. Using INGOs in intelligence action can break international law, be regarded as immoral or ethically questionable by society, damage the reputation of INGO and reduce public trust in the intelligence community. As a result, intelligence agencies should avoid taking advantage of INGOs. However, if it is unavoidable, intelligence agencies should put all the necessary efforts, that these cases would stay classified.

## Table of Contents

<b>INTRODUCTION .....</b>	<b>- 3 -</b>
<b>LITERATURE REVIEW .....</b>	<b>- 5 -</b>
<b>CHAPTER 1 UNEQUAL RELATIONS: INTELLIGENCE AGENCIES AND INGOS .....</b>	<b>- 10 -</b>
1.1 HEARTS AND MINDS: FUNCTIONING AND FINANCING OF INGOS.....	- 12 -
1.2 NATURE OF INTELLIGENCE: PROCESSES AND INFORMATION GATHERING.....	- 16 -
1.3 REAL CASE SCENARIOS .....	- 20 -
<b>CHAPTER 2 LEGAL ISSUES.....</b>	<b>- 23 -</b>
2.1 INTERNATIONAL VS NATIONAL LAW.....	- 24 -
2.2 GENEVA CONVENTIONS .....	- 27 -
2.3 LEGAL QUESTIONS IN PRACTISE.....	- 30 -
<b>CHAPTER 3 MORAL DILEMMAS.....</b>	<b>- 32 -</b>
3.1 JUST INTELLIGENCE THEORY .....	- 34 -
3.2 CONSEQUENTIALISM.....	- 38 -
3.3 EVOLVING CODE OF CONDUCT.....	- 41 -
<b>CHAPTER 4 IMAGE OF INTELLIGENCE AND THE ROLE OF INGOS.....</b>	<b>- 44 -</b>
4.1 INCREASING TRANSPARENCY OF INTELLIGENCE WORK.....	- 46 -
4.2 INTELLIGENCE STRUGGLE: PUBLIC OPINION .....	- 49 -
4.3 PRACTICAL CONSIDERATIONS ABOUT BALANCING THE TRUST .....	- 52 -
<b>CONCLUSIONS.....</b>	<b>- 56 -</b>
<b>REFERENCES.....</b>	<b>- 60 -</b>

## Introduction

Intelligence agencies operate in a demanding and fast-changing work environment of high stakes. In order to meet demands from consumers and to ensure security, intelligence agencies might infiltrate certain entities or use them in covert action or false flag operations. In some cases, such intelligence activities involve International and Non-Governmental Organisations (INGOs). Empirical evidence, such as the CIA organised vaccination campaign in Pakistan<sup>1</sup>, shows that such operations might be successful in terms of intelligence needs, but bring negative consequences to other actors. This dissertation aims to research what issues are raised when the national intelligence bodies take advantage of these organisations and why. Analysing these operations will allow drawing conclusions and possible recommendations on how to improve this intelligence practice. The real case scenarios suggest, that while the involvement of an INGO in intelligence activities is not necessarily damaging, the publication of these cases can cause harmful effects.

INGOs discussed in this research are mainly humanitarian organisations, working in humanitarian assistance, medical, health care, educational and other related fields. Humanitarian action refers to ‘(w)ork and services undertaken for the advancement and the welfare of humanity without regard to race, religion, politics or profit’ (Gunn, 2012). Most often such INGOs operate under neutrality and impartiality mandate in war and armed conflict zones, territories that suffered natural disasters or developing countries, where humans face severe living conditions. These organisations could be particularly targeted by intelligence organisations as they have the capacity to collect sensitive information and get access to the places that most actors could not. To enable their operations to the dangerous areas INGOs keep contact with the stakeholders involved in the conflicts, which might include government militaries, non-governmental armed groups or other fighting parts. While these organisations might take extra efforts to ensure secure communication channels, have confidentiality

---

<sup>1</sup> Ukman, J., 2011. CIA defends running vaccine program to find bin Laden. [online] The Washington Post. Available at: [https://www.washingtonpost.com/world/national-security/cia-defends-running-vaccine-program-to-find-bin-laden/2011/07/13/gIQAbLcFDI\\_story.html?utm\\_term=.c18d674a0da3](https://www.washingtonpost.com/world/national-security/cia-defends-running-vaccine-program-to-find-bin-laden/2011/07/13/gIQAbLcFDI_story.html?utm_term=.c18d674a0da3) [Accessed 10 June 2019]

agreements for the employees and other security measures, they cannot be entirely immune from espionage and exploitation by various intelligence bodies.

This research excludes non-governmental political organisations and international governmental organisations, as in some cases they might have an agenda that contradicts the state policy. Hence they could be legitimately and unsurprisingly targeted and investigated by intelligence agencies as a threat to state security or a political regime. Furthermore, some cultural NGOs might be a tool of soft power meant to influence the minorities or marginalised groups of society politically. The examples include Russian financed NGOs in Baltic states<sup>2</sup>. These different kinds of INGOs also might share some similarities with humanitarian organisations; however, not always transparent funding can also carry a hidden agenda. Therefore, this research will focus on humanitarian INGOs due to their established status, mandate (it will be discussed in chapter 1), non-affiliation with governments and distinctive work, that involves the handling of sensitive information.

Although intelligence organisations have different structures and tasks, in this research, the terms intelligence, intelligence agency, body or community will be used interchangeably always referring to the national intelligence organisations and not private intelligence entities. The work by national intelligence bodies is the main subject of this research as these entities deal with state security matters and are closely related to their governments. Moreover, governmental intelligence agencies in democratic countries are accountable to society, and they are not motivated by financial profit.

Where the INGO and intelligence work principles get mixed up together is the phenomenon of Government-Organised Non-Governmental Organisations (GONGOs). GONGOs receive their funding mainly from governments the same as their goals and the directions on how to implement them (Naim, 2007). This research only addresses international and local NGOs that are not organised by governments. The Inter-government organisations such as the UN are also excluded, as they have a unique way of functioning and financing. While GONGOs and inter-

---

<sup>2</sup> A full investigation could be found at Jemberga, S., Salu, M., Černiauskas, Š., Pancerozas, D., 2015. Kremlin's Millions. Re:baltica [online] Available at: <<https://en.rebaltica.lv/2015/08/kremlins-millions/>> [Accessed 10 May 2019]

government organisations might follow a similar transparency path to INGOs, it faces an increased risk of being politically engaged or manipulated.

Although the cyber realm of espionage takes an increasingly more prominent part of intelligence activities, due to the limitations of scope, this study excludes cyber operations as they have different specifications than the operations discussed in this research. However, it is worth to mention that INGOs are also vulnerable to cyber-espionage and cyber-penetration by the national intelligence agencies. Therefore, some of the factors and consequences discussed in this work could be applied to cyber operations as well.

This thesis begins by discussing the literature and sources related to the research. The academic literature associated with the Anglo-American intelligence culture is more elaborate; hence, this thesis will be based mostly on the experiences of the UK and the U.S. intelligence communities. However, once possible, to provide a broader view, the research will include examples from the other intelligence agencies as well. Following the literature review, the first chapter will give an overview of the nature of intelligence and INGOs work. While at the core these entities have different goals, they share some comparable work methods as well. This chapter will also introduce readers to the three empirical cases that will be analysed and referenced throughout the entire study. Chapter 2 will examine the legal issues that arise in intelligence operations that involve INGOs. Even there is no unified international legislation concerning intelligence work; agencies can break different laws by taking advantage of INGOs. Chapter 3 will analyse the moral dilemmas of the discussed situations. Since society is responsible for granting legitimacy for intelligence, it is essential that intelligence agencies could defend their actions in public. Therefore, the moral ground for their operations is crucial. The final chapter will look at the importance of public opinion on the intelligence agencies and what effects the disclosure of these operations might have. The thesis will conclude by summarising findings and discussing the gaps identified by this research.

## Literature Review

Any research aiming to analyse certain aspects of intelligence operations will unavoidably face some lack of information. Due to the confidentiality and state matters involved in intelligence work, the academic literature discussing operational circumstances is limited. But scholars

have analysed structural and philosophical aspects of intelligence functioning quite deeply and broadly including intelligence work cycle, the relations with consumers or moral and legal issues involved. In this literature review, I will discuss the essential sources and academic literature that this research is based on and will identify the knowledge gap that this research aims to fill as well as limitations.

All the sources and literature used in this study could be divided into two main parts. First one, related to the INGO work and the second part related to the intelligence work. There is only a limited amount of researches discussing the similarities and differences between these two actors. Some observers compare INGOs to intelligence agencies by their ability to acquire information (DeMars, 2005; Laipson, 2005) and discuss intelligence produced by non-state agencies such as NGOs or IOs (Chesterman, 2013; Gentry, 2016). However academic field would be enriched by more studies examining possible connections, conflicts or collaborations between INGOs and the national intelligence bodies. While at the core, they fundamentally differ by their structural landscape and ultimate goals (DeMars, 2001), there are ways in which these two entities face similar challenges or tasks. For instance, deploying or protecting their employees in war zones or trying to forecast the course of armed conflict. Therefore, scholars could take a closer look at the interactions between these two actors. This research aims to fill a fraction of this gap and contribute to the growing amount of academic research related to intelligence work.

Literature discussing the functioning of the INGOs rarely include considerations of INGOs vulnerability for intelligence penetration or possibilities in collaborating with the state's security body. The most relevant researches for this study include those that examine the security issues that INGO workers face in the environments they operate (Williamson, 2011; Jackson and Aynte, 2013; Haver and Carter, 2016). Literature reveals that neutrality and impartiality are vital factors for their functioning and security (Giustozzi, 2008; Schneiker, 2015). This mandate is threatened if an INGO is used in an intelligence operation. The part of academic research about the INGOs connections with the government in an insecure context is related to the Counter Insurgency (COIN) strategies and INGOs collaboration with the military (Byman 2001; Giustozzi, 2008). Such researches also contribute to the deeper understanding of vulnerabilities that INGOs encounter while operating in insecure environments and the risks that arise from using them in intelligence work.

Another important category of sources is news articles and reports discussing wider challenges and providing empirical evidence of issues related to INGOs activities. It illuminates the restrictions, distrust and dangers that INGOs and their employees face from some governments (Freedom House, 2012; Human Rights Watch, 2015; Amnesty International, 2019). Analysing these sources helps to complete the picture of INGO functioning and difficulties they need to tackle in different countries, regimes and political circumstances. News articles also reveal the tension that exists between some governments and INGOs (The Times of India, 2014; NGO Monitor, 2016; The Times of Israel, 2019). Such media sources allow to find out what are the reasons for strict laws that some governments impose to non-profit sector organisations. Apart from legislative tools some governments also use intelligence agencies as an instrument to restrict INGOs activities or their influence. These sources allow to comprehend the complexity of relations between the governments, intelligence agencies and INGOs.

This research is also based on empirical evidence. Hence the crucial part of this thesis is the three disclosed cases of intelligence operations which involved INGOs. The examples that were disclosed in the news media illustrate the theoretical considerations of intelligence operations that take advantage of INGOs (BBC, 2008; Gambino, 2014; Cole, 2015). What concerns these cases, I was examining the reliability of the information, the websites that published them and their sources according to seven categories of criteria as proposed by Adam Wierzbicki (2018, p.75). Where possible, I did facts cross-checking and evaluations. My judgement is that, while some details or circumstances might be not completely precise, there are no strong indications that would suggest that these cases could be falsified or that the crucial facts could be distorted. Therefore, it gives a substantial base for the research.

The biggest part of the literature for this study comes from the academic writings about intelligence work. Intelligence field literature used in this research could be divided into four thematic groups. Firstly, papers discussing the nature of intelligence work, including the meaning of secrecy, operational decisions and methods of intelligence collection. Secondly, academic articles connected to the legal aspects of intelligence work. Thirdly, literature based on the ethical and moral considerations of intelligence. And finally, articles discussing the purpose of public relation strategy for intelligence reputation and public opinion as a factor influencing intelligence work.

The meaning and relevance of secrecy in intelligence is widely discussed from the different angles (Scott, 2004; Phythian, 2007; Gill, 2009; Warner, 2012; Diderichsen and Rønn, 2017). Some academics see secrecy as an old paradigm that defines intelligence, while others see it as a tool that can also bring advantage against the enemy in decision making. However, secrecy not always protects state secrets but also might cover intelligence failures or other abusive practices. Hence it should be balanced with intelligence accountability and oversight methods (Diderichsen and Rønn, 2017) and an ethical framework (Gill, 2009). All scholars agree on the main argument that intelligence has to keep a certain degree of secrecy to increase its operational abilities and ensure the protection of state secrets. However, the oversight tools are necessary to prevent the abuse of secrecy.

The secrecy issue is also related to the lack of public knowledge about intelligence work. Even intelligence professionals discussing this field, refer to fiction films or novels as a source of illustrative information (Hitz, 2005; Omand and Phythian, 2013). Books and entertainment industry might also contribute to the creation of misleading public image about intelligence. As a result, intelligence agencies might encounter challenges related to legitimacy, public trust and relations with policy-makers. Therefore, some intelligence agencies decide to implement a public relations strategy that will be addressed later.

Another area of research that is related to this thesis are works analysing international law and intelligence. Academics agree that there is no unified international legislation criminalising intelligence gathering and espionage (Fleck, 2007; Sulmsay and Yoo, 2007; Oman, 2010; Forcese, 2011; Beim, 2018; Pun, 2017;). It does not mean that there are no laws at all. Currently, intelligence work is regulated by other international laws that are related to military actions or international conventions. Hence, the legality of espionage sometimes is also defined as 'underdeveloped' (Forcese, 2011, p. 186). Moreover, the lack of International laws and enforcement bodies allows countries to compete in spying (Warner, 2012). One of the reasons why international legislation is not established could be the lack of universal definitions of intelligence and espionage (Sulmsay and Yoo, 2007; Omand, 2010). Unless all the actors agree upon the term of intelligence, international law will struggle to develop as otherwise rules could be interpreted and manipulated in many ways. Authors also underline that collection of intelligence could be seen as a self-defence act (Sulmsay and Yoo 2007; Forcese, 2011). Hence, it could be justified under the existing military laws and could not be punishable. This anarchic situation allows intelligence agencies to push the boundaries of their actions to the extreme



without a risk of being prosecuted. But it also limits governments' abilities to deter or constrain hostile foreign state intelligence operations inside their respective countries.

The similar situation is with the ethical codes in intelligence work. Moral and ethical questions take a significant part of the overall research in the intelligence field. However, intelligence agencies still struggle in creating fully developed codes of conduct. A lot of academic literature related to the ethical considerations of intelligence work is based on the cases of torture, as some controversial examples were leaked to the public and these cases were related to the violations of fundamental human rights. However, in the broader discussion, researchers often agree that there is a need for a clear ethical framework for intelligence work (Andregg and Gill, 2014). Currently, intelligence is conducted in an 'ethical realist terms' which means acting in line with the national interests is moral (Erskine, 2004). This way is problematic, as some actions that are directed towards protecting one's nation could be extremely immoral towards another nation. Scholars observe that the creation of codes of conduct for intelligence agencies is interfered by those who see ethics as an obstacle in intelligence work (Andregg and Gill, 2014). Moral standards in intelligence work are also encouraged by the changing environment, which increases the need to cooperate between the states (Herman, 2004). Countries that traditionally are considered foes might be forced to share intelligence in order to fight global threats such as terrorism. Hence, clear moral standards could assist the countries in working and collaborating on the same terms. Moreover, the establishment of intelligence work ethics might contribute to a more positive public image of intelligence.

With the increased volume of research and public information about them, intelligence agencies are more interested in pursuing a public communication strategy to shape their public image. The public communication strategy can help to create a balanced image of intelligence, which is crucial for the intelligence ability to perform the tasks (Magen and Gilboa, 2014). Others argue that the actual achievements and quality of intelligence are more important than the public communication strategy in the creation of the public image (Moran, 2013). However, the media plays a complex role in intelligence legitimisation and democratisation (Matei, 2014). Media becomes an intermediary between intelligence and society, which holds a power to influence public perception about intelligence. Since the media have restricted access to intelligence information, it can misrepresent its work. As a result, intelligence agencies are showing more initiative to tackle their public image. Moreover, public communication of intelligence agencies does not stop with self-representation but also calls for action and

collaboration in risk assessment (Petersen, 2019) and is also a crucial tool in recruiting talents (Collier, 2017). Therefore, intelligence organisations have to consider how their public image will affect their work. In this thesis, understanding the significance of public communications and relations in intelligence work will help to examine the long-term consequences of the publication of operations that involve INGOs.

Due to the limited knowledge about operational details of intelligence work, qualitative research with inductive analysis is the most appropriate method for this research question. Sources and literature which was gathered and reviewed in this section allows deconstructing facts and delving deeper into the causes and consequences of such operations. This method will enable discovering underlying relations and will contribute to the growing volume of literature analysing less debated and examined aspects of intelligence work. However, investigating only disclosed cases creates a risk of falling into biased conclusions, as undisclosed operations might have different outcomes. To avoid this analytical trap, I will also discuss alternative circumstances, which might have brought different outcomes to those operations. Moreover, I will follow the assumption that most of the similar cases will stay disclosed; hence, looking at the possible results from that perspective as well.

## Chapter 1 Unequal relations: Intelligence agencies and INGOs

INGOs and intelligence agencies share some similarities in the ways they function. Both actors collect and analyse information. INGOs collect and gather information for a variety of reasons as to publicise human right abuses or organise aid in certain countries (DeMars, 2005, p.55). There are countries, like Romania, where the intelligence community even come together with NGOs and other stakeholders to collaborate in a security improvement (Graaff, 2016, p. 311). In some cases, they also share an interest in the same kind of information. There were real case scenarios when intelligence agencies provided INGOs with relevant information or assistance. However, it worked in the crises which did not have a political background (like natural disasters) (Laipson, 2005). In the armed conflict situations, information sharing becomes too complicated because of the different political views and the risk, that an INGO might lose the access to the population suffering from the conflict if it is perceived as affiliated with one or the other government. Moreover, such collaboration is determined to be unequal as intelligence agencies often have nothing to share with INGOs in exchange for information INGOs gather

in the field (DeMars, 2001). As a result, there are not many public cases of successful collaboration between these two entities.

At the core, these actors are different by their goals and ways to achieve them. While the information for the INGOs might be only the means, for intelligence agencies, it is often the ends (Laipson, 2005). They also operate under different mandates and declare a different set of values. Intelligence agencies serve governments and seek information that would assist policymakers in their decisions. To compare, INGOs try to obtain information that could allow them to deliver humanitarian aid, protect or support the vulnerable part of the population regardless of nationality or any political agenda. This underlines that intelligence agencies are initially tied to the political course of government and INGOs are apolitical actors operating by the humanitarian principles of serving vulnerable populations in spite of their views. Furthermore, INGOs, especially those, working in the armed conflict territories, see transparency and openness as essential tools enabling their work. Intelligence agencies, meanwhile, are often dealing with highly classified information and are protected by secrecy.

A mutually beneficial and non-exploitative relationship between the intelligence agencies and INGOs is still missing, especially in less democratic or non-democratic regimes. Some governments, like Azerbaijan, Belarus, China, Egypt or Russia, hold a strong distrust on INGOs, and it is best illustrated by the increasingly strict regulations that some of the governments impose on INGOs (Amnesty International, 2019). Some examples illustrate how governments dissatisfied with the agenda of human rights NGOs could seek to damage their reputation by unprovable espionage claims (NGO Monitor, 2016; The Times of Israel, 2019). Indian intelligence agency even issued a report blaming NGOs of anti-government activities (The Times of India, 2014). While indeed, some INGOs working in a human rights area might be interested in collecting and analysing specific information related to government action, it should not be juxtaposed to the espionage that foreign governments are pursuing. For this reason, INGOs are aware that intelligence agencies might target them. Such mutual mistrust is not beneficial to any side and brings challenges that this research is going to address.

This chapter will present the essential principles of how INGOs and intelligence bodies are functioning. It will help the reader to understand the possible conflicts that might arise between these two actors and their overlapping interests. The first section will illuminate the essential principles of INGOs' work. The following section will look at the national intelligence bodies'

work and the challenges they face. The last part will discuss some real case scenarios of intelligence operations connected to the INGOs and will lay a base for further analysis of this research.

### 1.1 Hearts and Minds: functioning and financing of INGOs

There are no precise calculations on how many INGOs are active worldwide. However, to some estimations, in 2010, 2.3 million non-profit organisations were operating in the U.S. alone (Blackwood et al., 2012). Often referred to as a third sector, INGOs implement activities in the areas that vary from environment protection or international development to civil society organisations and political think tanks. What makes INGOs stand out from private sector bodies is that they do not seek profit but work towards the public good instead. This feature brings INGOs closer to the governmental sector in terms of values. Moreover, international NGOs also have a distinctive feature of connecting partners from different states (DeMars, 2001). While numerous INGOs<sup>3</sup> are vulnerable to intelligence exploitation or penetration due to the variety of reasons (like posing a risk to the political regime or having access to hard-to-reach areas), this study will mainly discuss the INGOs operating in hostile environments, conflict territories or war zones as they are of particular interest to the intelligence organisations.

Humanitarian and aid organisations operating in hostile environments also implement a diverse range of activities. Some assist populations affected by armed conflicts and deliver medical services, provide shelter, food and essential items; others monitor human rights and assist internally displaced people or refugees. The examples of these organisations include CARE<sup>4</sup>,

---

<sup>3</sup> In particular, this could be applied for INGOs working in protecting human rights or exposing government abuse, corruption, and criticising undemocratic regimes.

<sup>4</sup> An international humanitarian organisation working in development and ending poverty. See: <https://www.care-international.org>

Doctors Without Borders<sup>5</sup>, ICRC<sup>6</sup>, IRC<sup>7</sup>, Save the Children<sup>8</sup> and others. Such organisations have a capacity to collect sensitive information about the social and military situation in a particular country or even access besieged cities and front-lines. These abilities are based on a fragile trust, that INGOs build with the fighting parties, governments involved in the conflict, local actors, communities and other stakeholders. Whether the INGO works in human rights, health or another field, its ability to implement the necessary tasks highly depends on getting access to the relevant information or people in need.

Enabling accesses is closely related to the image organisation has locally and internationally. Therefore, those organisations that act in conflict territories declare their adherence to the principles of neutrality and impartiality (MSF, 2019). Neutrality is perceived as not taking ‘sides in hostilities’ nor engaging ‘in controversies of a political, racial, religious or ideological nature’ and impartiality is defined as making ‘no discrimination as to nationality, race, religious beliefs, class or political opinions’ (ICRC, 2016). Following the principle of neutrality is perceived as a crucial element in developing acceptance, which warrants getting access to the beneficiaries in a conflict territory (Fast et al., 2013). The neutral and impartial organisation ensures community and the recipients of the aid that it is not related to any political power; therefore, could be trusted not to influence the course of the conflict by their work. These principles ensure that organisations are fully engaged in a humanitarian mission and do not carry a hidden agenda.

However, the research on the NGO security reveals that their neutral and impartial identity is essential but not enough to ensure the safety of the NGO’s staff and activities (Schneiker, 2013). There are more factors that play a role in successful INGOs’ operations in hostile environments. Ability to network with the national actors and local organisations allows INGOs to get better access to the conflict territories (Harver and Carter, 2016). The organisations that have less diplomatic capabilities or do not engage with the local actors are

---

<sup>5</sup> Better known as Medecins San Frontieres (MSF), is organisations working in emergency response and medical care areas. See: <https://www.msf.org>

<sup>6</sup> International Committee of the Red Cross is organisation operating according to international humanitarian law and providing assistance for victims of armed conflicts. See: <https://www.icrc.org>

<sup>7</sup> International Rescue Committee provides humanitarian assistance in crises situations. See: <https://www.rescue.org>

<sup>8</sup> An international organisation advocating children’s rights and providing assistance in emergencies. See: <https://www.savethechildren.net>

less likely to implement their operations successfully. To improve their ability to collaborate with the various actors and stakeholders, INGOs have to collect and analyse multiple sources of information. Furthermore, they might seek and maintain contacts with the individuals and groups that might be especially difficult to communicate with. INGOs operating in conflict territories often are in contact with militaries, but they also might need to communicate with the rebel groups, insurgents or terrorist organisations. This helps INGOs to negotiate access to the hard-to-reach areas and ensures that their aid delivery will safely reach beneficiaries. On the other hand, contact with the insurgents might damage INGOs reputation in the eyes of the local government or international community.

In some cases, INGOs delivering aid might be forced to take extreme measures as paying fees (in the form of registration or security tax) for getting access to a population in need. Examples include humanitarian organisations working in Al-Shabaab controlled areas in Somalia (Jackson and Aynte, 2013). It also creates a risk that a humanitarian organisation paying for a non-state actor to get access could be prosecuted under the counterterrorism laws. However, in these extreme instances, organisations explicitly declare that their primary goal is to alleviate the suffering of the population and that they might be forced to take drastic measures due to the humanitarian concerns. This situation illustrates that INGOs operating in hostile environments face not only security but moral and political issues as well, which places the humanitarian worker in a highly vulnerable position. As will be revealed in the following paragraph, such vulnerability could be utilised for the benefit of other actors.

Humanitarians face the danger of a particular nature. Because INGOs deliver much-needed aid and commodities to the conflict territories, it makes them a potential target (MacLeod, 2009). Sometimes INGOs are attacked because one or the other part of the conflict hopes to take over the aid and benefit from it. In other cases, they are targeted as perceived collaborators of the opposing side. Therefore, the trust and the image of INGO is extremely crucial. However, even some of the most trusted organisations sometimes suffer heavy casualties; when their aid deliveries are attacked, humanitarian workers are abducted or killed. While the number of attacks on humanitarian workers is rising, so is the overall number of humanitarians worldwide. Therefore, it is not possible to state that the situation is getting worse. However, there is a clear correlation between the number of humanitarian casualties and the intensity of violent context they operate in (Hoelscher et al., 2017). It shows that even employing various security strategies, INGOs are not immune to the threats evolving in a hostile environment.

Another reason increasing INGOs insecurity is the politicisation of humanitarian aid, which is related to military strategy and political background of the conflicts. Originated from the British counterinsurgency (COIN) efforts in Malaya ‘winning hearts and minds’ strategy could be described as a complex plan of action to gain more support for the military actions from the local population by providing non-military assistance (Thompson, 1966). This strategy is still used in some contexts today and raises issues for the INGOs working in the same areas. If the humanitarian aid is perceived as a tool of military counterinsurgency (COIN) strategy, it can endanger humanitarian workers and compromise the neutrality and impartiality mandate on which they operate (Williamson, 2011, p.1037). This confusion might happen in the areas, where the military employs the ‘winning hearts and minds’ as a part of COIN strategy and starts delivering goods or services. In that case, the population might have difficulties to distinguish between the aid distributed by neutral INGOs and the aid delivered by a foreign military. It leads to situations like in Afghanistan, where population perceives an INGO as politically influenced (Giustozzi, 2008, p.105). It negatively affects INGO’s ability to implement its activities and raises distrust. The organisation which is seen by the local population as an extension of foreign government might struggle to get access to the beneficiaries or lack support from the national actors in this way endangering its workers. This issue will be further addressed in Chapter 2, section 2 'Geneva Conventions'.

It is important to emphasise that although a lot of INGOs declare their neutrality, independence and non-affiliation with governments, they are still often partly financed by government-affiliated donors or receive governmental grants. It does not mean that they are obliged to perform the government’s requests. Even so, INGOs might decide to modify their activities to match specific requirements from the donors, for instance, increase operations in the areas that the donor perceives as of particular need. Government lobbying might be more expressed towards organisations working in soft-power related areas. However, humanitarian organisations have more objective criteria to define the priorities for their operations (for instance, where there are more people in need of food or medicine supplies etc.); therefore, they are less influenced by their donors. Moreover, to reduce possible bias, INGOs seek high transparency of funding and expenditure. For instance, an annual report is compiled by the International Committee of the Red Cross (ICRC), which presents the information about its donors and beneficiaries in great detail (ICRC, 2018). While local NGOs might have different means of accountability, it is a common practice by large organisations to publish their

financial reports. This kind of openness and transparency allows interested parties to see, where the money comes from and what programs in which countries are financed and implemented. It also helps to reduce the risk of the influence of the donors, as it clearly represents the humanitarian needs and the response actions taken by the organisation.

## 1.2 Nature of Intelligence: processes and information gathering

There is no one universal definition of intelligence. Instead, different definitions emphasise various aspects of intelligence. The broader understanding of intelligence allows making comparisons with other actors. Therefore, for this research, it is appropriate to think about intelligence as a means to develop knowledge and predictions about the other states, organisations or individuals that might influence the given country or pose a threat (Breakspear, 2013, p.688). While this definition does not identify intelligence work manner or final recipients, it highlights the essence of the information in intelligence activities. More specifically when we refer to the national intelligence bodies and their work, we imply information gathering and analysis which in the form of intelligence product is intended to assist policymakers or military personnel in making right decisions about the internal or external security matters or secure the state's secrets (counterintelligence).

Due to these features, INGOs could be compared to the state intelligence agencies in a sense that they also collect and analyse information so they could identify and influence various actors connected to the implementation of the INGO activities (Gentry, 2016). The critical differences between these two actors are the purpose and the outcome of information collection and the level of transparency they practice in their operations. For an intelligence agency accessing specific information might be the final goal while for an INGO, the information might be only the tool. INGO work is usually directed towards the public, while the recipients (often called 'consumers') of intelligence products are mainly politicians and decision makers. Furthermore, the lack of openness or to be more precise, secrecy is one of the most distinctive features of intelligence work.

There is an ongoing discussion in intelligence studies about the importance of secrecy, which was already addressed in the literature review. Summarising this discussion Michael Warner notices that secrecy as a need to protect the information and sources is closely related to the



short life span of the value (i.e. perishability) that the information might hold, and this perishability depends on fragility and timeliness (Warner, 2012, p.228). It also means that the riskier, secretive, potentially illegal or morally questionable methods of intelligence gathering or covert action are usually taken when the stakes are high, or intelligence agencies face strict time constraints. Secrecy also helps intelligence agencies to protect their sources and methods. Therefore, a lot of successfully implemented operations will stay undisclosed so it could be emulated in the future.

Secrecy is also connected to another peculiarity of intelligence work. There exists a lack of information in public knowledge concerning the activities that intelligence agencies implement (McCrisken and Moran, 2018). Such an information vacuum encourages speculations and imaginative interpretations about the means and ends of intelligence activities. Moreover, the fog that covers the intelligence work creates a situation when films and novels about intelligence agencies are perceived as factual information while in reality, the functioning of these agencies might be quite different (Hitz, 2005). Witnessing this, some intelligence communities try to increase openness, provide the public with more information about their work and even pursue public relations strategies like other government agencies (Moran, 2013). But even the society's knowledge and the volume of academic research concerning intelligence work methods are growing, there is a lot of unknowns for public and academia. It raises several issues concerning the image of intelligence communities that will be discussed in more details in the final chapter.

Similarly, to INGOs, national intelligence agencies also need to develop trust with their stakeholders. While primary consumers and stakeholders of intelligence are policymakers, society also has a role to play. The society which trusts and is willing to collaborate can be a great support to the intelligence community (Chiru, 2016). Moreover, society provides consent to intelligence work as a part of democratic processes (Gendron, 2005). Therefore, increasing transparency and creating a positive image of intelligence in public, serve strategic goals. Similarly, keeping controversial or negative information in secret from the public eye also contributes to safeguarding intelligence reputation. Hence, openness and transparency could bring benefit or damage depending on the context. As it will be argued in chapter 3, to reduce the risk of harm when certain operations are disclosed or leaked to the public, the intelligence agencies should always test their actions from the moral perspective. Nevertheless, there are

situations when to choose the morally acceptable decision could mean to lose. Some of those cases involve taking advantage of INGOs.

In normal circumstances, most of the intelligence comes from open sources (OSINT). Although intelligence field professionals agree, that while less or non-intrusive methods as open sources and technological espionage (such as signals (SIGINT) or imaginary (IMINT) intelligence) can be efficient in exposing enemies' capabilities, the information that is gathered by human assets (HUMINT) is more helpful in discovering enemy's intentions (Perry, 2009, p. 134). However, HUMINT operations are genuinely complex, riskier compared to some other methods, like SIGINT, and often raise legal and moral challenges. Apart from the competent and skilful case officers and agents, the success of the HUMINT gathering operation highly depends on the ability to access sources, the time given for the operation and the background knowledge of the operational environment (Wippl, 2016, p. 595). Developing a deep cover story, learning a foreign language and befriending possible informants could take an enormous amount of time and be extremely expensive. Therefore, it is not a surprise that intelligence organisations are looking for a quicker, less costly and more efficient ways to acquire relevant HUMINT. That is when the INGOs come to the sight as they often pursue long-lasting relationships with the local communities, hold extensive knowledge about the country or area and relevant language skills. As a result, infiltrating organisation, recruiting its employee or using such organisation as a cover is a tempting option, that intelligence agencies might choose to increase their chances of success.

The context in which intelligence agencies have to operate also plays a role. The methods of intelligence collection will highly depend on the regime and political structure of the country that poses a threat (Gendron, 2005, p.429). Less democratic and less open countries are more challenging for HUMINT operations. It is likely that an operation in such countries will be dangerous for agents and legally or morally questionable. Furthermore, the level of threat that the country poses also affects the methods and ways of intelligence gathering. If the state constitutes a minor threat, open source information might be sufficient to monitor it. However, if there is imminent danger of military actions, intelligence agencies will resort to secret operations. This will be illustrated by the real case scenario of an intelligence operation in North Korea.

As any other organisation intelligence agencies face various challenges on their daily work such as lack of expertise in certain areas, organisational challenges or time constraints (Wippl, 2016). The latter one is a crucial factor for developing the necessary skills and knowledge about particular countries or regions and implementing successful HUMINT operations. The lack of time is another reason why sometimes intelligence agencies decide to take advantage of the INGOs. Time constraints could force intelligence agencies to explore quicker ways to gain specific information, in that way compromising legal or moral rules. Furthermore, in hostile situations such as conflict territories, INGOs could be the only entities having access to the area. In such instances, intelligence agencies simply have not a vast amount of options but to exploit an INGO to achieve the security goals.

In order to understand the dynamics of the relations between the intelligence communities and INGOs, it is necessary to look at their connections with society and government. The scheme below illustrates the main links of this ecosystem (figure 1). While intelligence agencies do not have a direct impact on society, it highly contributes to the government's duty of providing security. Society, from its side, holds the public consent which validates intelligence work (it will be addressed in chapter 2). Therefore, intelligence agencies in a non-direct way are accountable to society as well. Similarly, INGOs and government are directly accountable to society. While the scheme presents four acting elements, it is essential to highlight that as intelligence is a part of a government so the INGOs could be seen as a part of society. As it was addressed previously, in rare cases, intelligence and INGOs also can collaborate by exchanging their expertise and assistance. However, it is not entirely equal partnership, but more advantageous to intelligence agencies, as the cases when INGOs are accepting support from the intelligence community are rare and mainly relate to intelligence assistance in the cases of abduction of INGO workers or other direct threats.

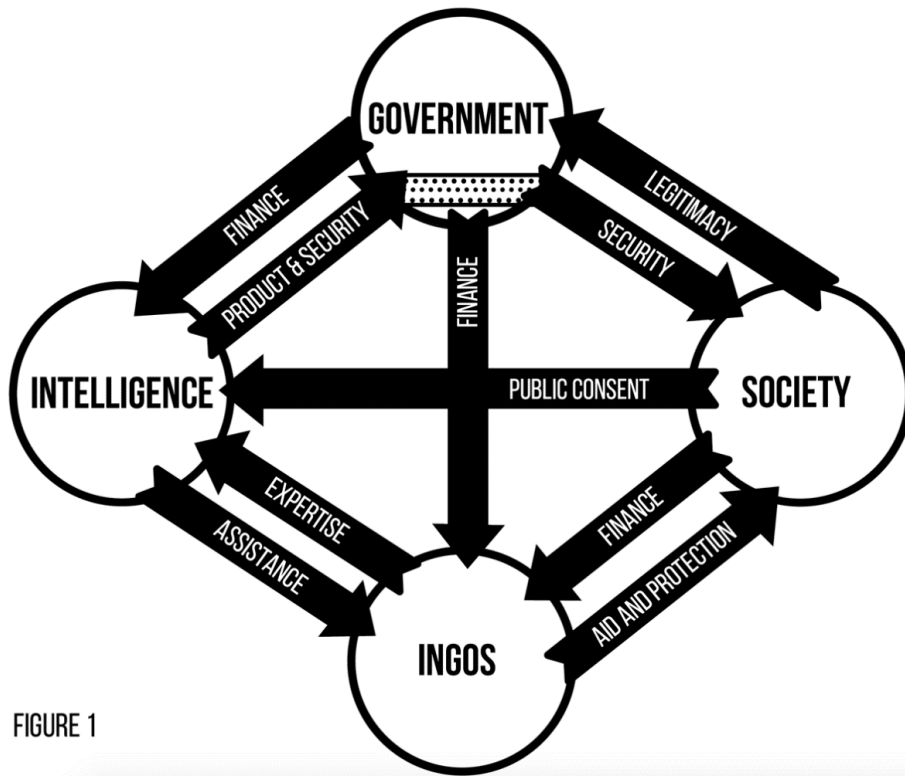


FIGURE 1

### 1.3 Real case scenarios

In real life, intelligence agencies can take advantage of INGOs during covert action, false flag or intelligence gathering operations. Covert action is described by Britt L. Snider as ‘activities that the CIA might undertake in other countries to accomplish a US foreign policy objective without the hand of the US government becoming known or apparent to the outside world’ (Snider, 2008, p.259). This definition reveals that the covert action is not always directly associated with the main objectives of intelligence agencies which are meant to protect the country and provide policymakers with the relevant information. Instead, covert action can be related to the broader policy or economic goals. While most states are engaged in espionage, not all of them perform covert action operations and seek to expand their political influence by covert means. Creating an organisation which would secretly carry out the political agenda is a well-known intelligence practice. The examples include propaganda, psychological (PSYOP) and informational operations during the cold war such as the Radio Free Europe and Radio Liberty (RFE/RL) that were established and funded by the CIA as a covert effort to influence populations under the Soviet control (Johnson, 2018). While covert action is not necessarily illegal, it is often seen as controversial by the public and could raise serious moral and ethical

considerations (Perry, 2009). One of the declassified covert action operations that will be referred to in this research is a fake vaccination campaign organised in Pakistan by the CIA.

During this operation, the CIA was hoping to get the DNA of people living in a highly guarded compound where the terrorist Osama bin Laden was supposedly hiding. The DNA was meant to help to confirm the identity of the terrorist. The Pakistani doctor who collaborated with the CIA helped to organise vaccination in a whole Abbottabad area. Since the compound was extremely guarded, only health workers were allowed to enter it. Therefore, the U.S. intelligence agency had to use humanitarian health workers cover to collect information from inside the compound. After this case was published in the media, it evoked strong reactions from the health sector professionals in the U.S. as well as the Taliban. Reasoning that health workers might be U.S. spies, the Taliban banned polio vaccination in the areas of their influence and control (Walsh and McNeil, 2012). Moreover, following the publication of this case INGO Save the Children have withdrawn from Pakistan the foreign national staff and several UN health workers vaccinating kids were killed in Pakistan (Buekens, et al. 2013). Further moral implications and other consequences of this operation will be discussed in chapters 2 and 3.

Similarly, to covert action, the false flag operations also are meant to deceive. False flag operations define intelligence actions when the organisation (or state) behind the operation or activity is pretending to be something else. The former chief of counterintelligence James M. Olson states that a false flag is an important tactic which allows intelligence to recruit potential informants (Olson, 2006, p.55). For instance, a person might think that he is providing information for a human rights NGO while in reality, he is working for a national intelligence organisation. In other cases, the humanitarian workers who are performing their duties could be unknowingly involved in espionage. The disclosed example of such scenario is of the Christian NGO called Humanitarian International Service Group (HISG) which was receiving financing from Pentagon in exchange for information and military equipment smuggling into North Korea (Cole, 2015). The missionaries who were going to North Korea were not aware of their double mission as only the head of HISG knew about the Pentagon inquiries. Sometimes such methods are unavoidable. But it also rises severe legal and moral issues that will be discussed in more details in the following chapters.

Another example, which is similar to the false flag operation, is Colombian military intelligence operation called “Jaque” (BBC, 2008). This operation was organised in order to release hostages held by the Colombian rebel organisation FARC. During this operation, one of the soldiers wore red cross emblem, pretending to be a humanitarian worker. This case illustrates the legal implications of such actions as the misuse of the humanitarian symbols is against the Geneva Conventions. The consequences related to this case will be analysed in more detail in chapter 2.

To sum up, these cases presented in this section set a precedent and allow fruitful analysis that could be of interest to the national intelligence agencies and INGOs.

The three introduced examples are the only cases available in the literature and reliable sources. And it also indicates the knowledge gap concerning such operations. The practice of using INGOs in intelligence operations is still widely practised as it emerged by some informal discussions with practitioners in the field. Apparently, intelligence agencies are putting a lot of efforts into keeping such cases highly confidential, which also contributes to safeguarding the reputation as the final chapter of this research will prove. Another hypothesis could be that INGOs are becoming less vulnerable, and as a result, intelligence agencies have fewer chances to take advantage. However, from my experiences working in the international humanitarian organisation operating in conflict territories and a local NGO in Afghanistan, I can state, that personnel of INGOs often have or can relatively easily acquire access to the sensitive information that could be valuable and not that easily accessible to intelligence agencies. But large international organisations, as well as small local NGOs, rarely have the capacity to perform in-depth background checks about their employees and thoroughly ensure the protection of the sensitive data. Furthermore, local NGOs are often less financially stable and could be more willing to accept monetary assistance in exchange for a favour.

This chapter has briefly introduced the main characteristics of both subjects that are at the core of this research. While the interactions between the national intelligence bodies and INGOs can be different, this research will look closely at the issues that arise when INGOs are being used in intelligence gathering operations or covert action.

## Chapter 2 Legal issues

Discussing the emergence of international constraining norms for emerging technology weapons, Brian M. Mazanec noticed, that the constraining norms are slow to be established in the cases, where states are interested in exploiting the emerging technology as they would benefit from it more than they would benefit from restricting or abandoning it (Mazanec, 2015, pp.178). This observation could partly explain the existing situation in the laws concerning the espionage. All states are performing intelligence activities to a different degree. Therefore, there are no states that would strongly advocate for the establishment of restrictive international laws regarding espionage. From some points of view, regulations of peacetime intelligence gathering could even increase the risks of war (Sulmsay and Yoo, 2007). Intelligence as a form of information allows countries to evaluate the dangers coming from other states. Hence, it is a crucial element of diplomatic relations that enables states to negotiate their disagreements or employ the tools of deterrence instead of starting military actions. Furthermore, the lack of consensus over the definition of intelligence also restrains from the development of international regulations (Sulmsay and Yoo, 2007). Although the unified international law concerning the intelligence work is missing, there are other laws that influence intelligence communities, and intelligence officers should dedicate special attention to these regulations while planning their operations and calculating possible consequences.

While looking at the laws that could be applied to intelligence work, it is essential to distinguish certain factors such as time (peacetime or wartime), the territory of action (national or foreign), purpose (defence, national-interest, economic profit, etc.) or a type of intelligence operation. The lines between some of these factors are not always clear; therefore, the application of laws in intelligence activities becomes even more complicated. From the one hand, intelligence gathering in a foreign country could be interpreted as a breach of the sovereignty that is guarded by Article 2(4) of the U.N. Charter (UN, 1945). On the other hand, espionage could be legally permitted as an act of self-defence (Forcese, 2011). In such intricate cases the context is crucial, whether the country is at war, is there evidence of the threat from the country being spied on, or what kind of information is being collected (military, economic, social etc.). Most cases of espionage are tackled according to the national laws of the country, that finds the suspected spy. While spies in most cases are prosecuted, the agencies that the spy was working for (for

instance, national intelligence agencies) are usually not involved in any legal trials<sup>9</sup>. To compare, in economic espionage cases, companies, along with individuals, have to take responsibility (Heaven and Kornweiss, 2018). Overall, the legal cases related to intelligence work distinguish from other lawsuits and are dealt with on an individual basis.

Regardless of the lack of international regulations, intelligence agencies still risk breaking the law and being prosecuted by the individual or organisation. It is also true in the operations that involve INGOs. This chapter will take a closer look at the laws that should be considered when planning such actions. The first section of this chapter will discuss international law that could be applied to intelligence activities and will juxtapose it to the national regulations of some countries. The next part will look specifically at the Geneva Conventions and International Humanitarian Law (IHL). Legal issues related to these laws will be illustrated by the case of Colombian military operation and the vaccination hoax. The last section will proceed with the analysis of the other real-life scenarios and the legal implications that it could evoke.

## 2.1 International VS national law

Due to the involvement of secrecy and deception, intelligence agencies rarely face trials for the operations or activities that are outside the law. Furthermore, what concerns the protection of state secrets, intelligence agencies tend to rely more on their counterintelligence efforts to fight espionage in their country instead of trusting the rule of law. Avoiding traditional legal systems also contributes to the security of intelligence work methods and the protection of the sources of information. Furthermore, once a lawsuit against an intelligence agency reaches a court, it might have a harmful effect on a reputation of the intelligence agency, or the ability to implement operations. This section will take a closer look at the laws that could affect intelligence agencies of any state and will juxtapose international and national regulations.

One of the main reasons why intelligence agencies are not often prosecuted is the lack of international regulations regarding the acts of espionage and intelligence collection. The variety of activities that intelligence agencies implement, often cross borders of different countries, legal systems and laws. Currently, no unified international law directly addresses

---

<sup>9</sup> However, in the case of human right abuses, a state is more likely to be prosecuted.



espionage actions. The common interpretation of the existing International Law asserts that espionage is not illegal during the wartime, as it is partly guarded by The Hague Regulations Respecting the Laws and Customs of War on Land, yet there are no clearly defined international laws that address intelligence gathering during the peacetime (Fleck, 2007). Cases connected to intelligence work are investigated, interpreted and assessed according to the national jurisdiction unless the case reaches international courts. If the case is related to the wartime intelligence actions, grave breaches or crimes against humanity, it is more likely that international courts will get involved in examining it.

During the peacetime, intelligence gathering and covert action operations face increased risk to violate human rights such as privacy. In that case, covert action could be punishable according to the international and regional human rights conventions (Fleck, 2007, p.693). In normal circumstances, intelligence agencies operating in democratic states would need to have court permission to collect information on citizens that could pose a threat to national security. Furthermore, an intelligence agency would need to bring substantial evidence to prove the need to violate the privacy of an individual. After the classified files were leaked by Edward Snowden, the mass surveillance program by the UK's intelligence agency GCHQ was concluded illegal by the European court of human rights (Privacy International, 2018). Such cases in practice are rare. Firstly, clear evidence of attribution is needed to convict a state of espionage and, it is highly challenging to gather it (Fleck, 2007, p.695). Most anticipated options to gather evidence are during the oversight process or if an employee of an intelligence agency decides to reveal classified files. Secondly, intelligence agencies can shield from the in-depth investigations by the protection of the state secrets. Therefore, unless intelligence officers take responsibility to disclose secret documents, the violations of human rights by intelligence agencies might go unnoticed. This also works to the advantage of intelligence agencies. Under the time pressure, mass surveillance could be the last resort solution providing crucial information and ensuring security. In such instances, the question about the balance of privacy and security becomes rather philosophical than legal.

Illegal intelligence activities can be illuminated during the oversight process. Intelligence oversight is meant to help intelligence agencies to function within the legal boundaries. Peter Gill describes the goal of intelligence oversight as 'to increase both its efficacy and propriety' (Gill, 2012, p.217). Laws, requirements and instruments of oversight vary significantly in different states. Some countries dedicate more resources to it, while others have a slightly loose

approach or no democratic control at all. Belgium, for instance, has established a unique body for intelligence oversight called Standing Intelligence Agencies Review Committee that has the power to monitor intelligence-gathering methods and investigate the complaints about the intelligence work from the population (Van Daele, 2016, p.35). It is an advanced and rare example of oversight, as it also allows the population to play a role and submit the observations about the intelligence activities for further investigation. In the U.S., the Congress supervises policy related issues while Federal judges perform judicial oversight of intelligence work and in that way balance between state security and protection of human rights (Manget, 2007). This method allows to increase transparency and still ensures the protection of the classified information. However, even with the oversight methods in place, the extraordinary circumstances under which intelligence often operate can cause various breaches of the law intentionally or unintentionally.

The national laws of intelligence work and espionage that are in place in many countries are meant to provide guidance for intelligence functioning. National intelligence laws define the rights and responsibilities of government intelligence agencies and intelligence work oversight. For instance, in the U.S. the executive order no 12333 rules that intelligence collection has to be 'consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded' (CIA, 1981). Espionage laws usually aim to protect state secrets and are more directed towards the individual rather than institutional responsibility. State secrets connected to intelligence work are particularly strongly protected by law in countries like the U.S. and UK (Lefebvre, 2019). Although there are some differences between the national laws of various states but most of them, have criminalised espionage on their territory regardless of whether it is wartime or not (Fleck, 2007 p.702). Countries seek to discourage espionage by implying heavy penalties for acts of espionage. Although it seems that capital punishment for the espionage is disproportionate in many ways (Norwood, 2002), a lot of the countries that still have not banned the death penalty can apply it to a spy as well (Hood, 2008). Moreover, it could be questioned whether it is right to punish a person who was performing the duties (a spy), instead of the institution that is planning and organising espionage (an intelligence agency or other government bodies). Since the differences in national laws exist, intelligence organisations should be prepared to act under the national laws of the country that the operation is set in.

In the case, if an operation is discovered, intelligence agencies can vindicate themselves from the espionage claims by self-defence (Fleck, 2007, p.699). Most activities implemented by intelligence organisations could be done for the sake of national security. However, there are no universal objective criteria to judge whether the action is indeed fundamental to security. The example of the CIA vaccination campaign is worth a mention. A senior U.S. official commenting about this case was quoted saying that “(i)f the United States hadn’t shown this kind of creativity, people would be scratching their heads asking why it hadn’t used all tools at its disposal to find bin Laden” (Ukman, 2011). The question remains, whether the terrorist was so dangerous that it was worth breaching the law and risking to cause a health crisis. It is impossible to judge that with the limited information available to the public. However, the lesson from this precedent is clear; intelligence agencies can and will try the boundaries of laws, to increase the efficiency of their actions. And since there are no international laws in place, there are no effective tools to discourage intelligence agencies from intrusive operations in foreign states.

## 2.2 Geneva conventions

In a broad sense, Geneva Conventions with its supplementary protocols provide legal guidance and protection to states and individuals in time of war or armed conflict. It is also a part of International Humanitarian Law (IHL), which aims to 'limit the effects of armed conflict' (ICRC, 2004). Geneva Conventions also safeguards humanitarian work principles, and that is the reason why Intelligence agencies should take it into account while planning operations that somehow involve INGOs working in the humanitarian field. Although currently, there are no established practices and implications for breaching Geneva Conventions, some articles describe the obligation to prosecute criminals, but it only applies to the grave breaches committed during the war (Elst, 2000). The precise interpretation of the grave breaches and the process of prosecution highly depends on the national legislation of every state. Therefore, in some cases, intelligence agencies could decide to disregard Geneva Conventions if the stakes are high and alternative options are missing.

In other cases, the breaches could be done unknowingly. The Colombian hostages' rescue operation is a clear example. The Article 38(1) of the 1977 Additional Protocol I to Geneva

Conventions state that '(i)t is prohibited to make improper use of the distinctive emblem of the red cross, red crescent or red lion and sun' (ICRC, 1949). One of the soldiers was wearing the red cross emblem during the military intelligence operation. Therefore, this act violates IHL, and it could have severe consequences for the humanitarians working under this emblem in the future. It could damage the trust in the organisation and its workers and limit access to the people in need. Operation Jacque also illustrates the powerlessness of the IHL. There were no legal implications for the Colombian military intelligence or the individual soldier. The situation was solved by the official Colombian President apology to the International Committee of the Red Cross (BBC, 2008). This example could encourage other intelligence agencies to have a more relaxed approach to breaking Geneva Conventions or IHL. As a consequence, the image of humanitarian organisations might suffer.

Further investigations of the hostages' rescue operation proved that the soldier who was wearing a red cross emblem decided to do it on his own without the orders from the higher officials (BBC, 2008). This condition shifts responsibility from the Colombian military intelligence to the individual soldier. It could also explain why no further legal actions were taken about the violation. Moreover, the operation was praised for reaching the goal without using a military force (McDermott, 2008). In this context punishing a soldier who misused the red cross emblem would diminish the degree of excellence of this operation. Taking legal implications is vital for discouraging future breaches of the convention. Misuse of humanitarian symbols could spread distrust of INGOs and restrict humanitarian actions in an insecure environment. As a consequence, it might limit an INGOs ability to reach beneficiaries or endanger the lives of humanitarian workers who operate in hostile environments.

As it was mentioned in Chapter 1, INGOs highly depend on the trust and their image as neutral and impartial. Therefore, misuse of the emblem under the governmental or political incentives can create serious issues. Moreover, the threat that INGO will be seen as a tool of foreign military strategy is real and well manifested in some countries that are part of the global counterterrorism plan. The INGO falling under the COIN shadow might lose its credibility, financing and access to the beneficiaries or even might be attacked, its workers could be abducted or killed. While guarding the distinguished emblems of the humanitarian workers, Geneva Conventions also protect their reputation and mandate. In this way, it helps to ensure that humanitarians are not associated with the COIN strategy. If this rule is breached and not punished, it could have serious implication in the future.

This Colombian military operation provides two important lessons for intelligence organisations. If due to operational reasons, it is impossible to avoid using humanitarian cover, it is better to establish a new organisation purely for the purpose of the cover, instead of using well-known organisations. It might be a costly and time-consuming option, but it would prevent from causing damage to the real INGO working in the humanitarian field if the operation becomes public. In this way, INGO's mission and workers will be protected. Although such a scenario might not prevent the breach of international law and still might damage the reputation of humanitarians in a broader sense, it might preserve the image of a particular organisation and its long-term objectives. Secondly, if using an existing INGO is unavoidable, there should be taken all possible precautions, to keep such operation unpublicised. The motivating reason for this should be not the fear of being prosecuted under the IHL or other international law, but other harmful consequences that the publication might evoke for both intelligence agency and INGO. The better understanding of the fragility and the value of the humanitarian INGOs should foster intelligence efforts to find different solutions to access information, places or people. Eventually, disturbing the work of humanitarians also harms the principles, that intelligence agencies of democratic countries aim to protect.

There are more ways in which Geneva Conventions and IHL could conflict with the COIN strategy or intelligence operations. According to IHL, the humanitarian aid distributed to those in need 'cannot be manipulated to serve military goals' (Williamson, 2011, p.1037). The CIA vaccination campaign could be an example of this breach. Since the vaccination hoax was primarily meant to get access to a compound and to collect DNA samples of bin Laden's relatives, it means it is a military operation with a state security goal and potentially could be interpreted as a breach of IHL as vaccines were delivered only in the area of interest of the CIA. It could be argued that IHL is only applied in the time of war and regarding this case, it could not work as Pakistan (where the compound was located) and the U.S. were not officially at war. From the other hand, the U.S. announced a global war on terror that was addressed towards the terrorist organisations and their leaders, including bin Laden, who was hiding in Pakistan.

There are several considerations concerning this case that could have been changed in order to reduce possible contradictions with the laws. Firstly, they could have tried to vaccinate only people in a compound and avoid involving too many innocent people. However, the

vaccination campaign had to be credible. Therefore, it was decided to vaccinate people in the whole area. In that case, they could have invested more, and performed follow-up vaccination shots and any relevant health check-ups, so that people involved would have the same benefits as from a regular vaccination program. Finally, taking care, that such case would never be disclosed to the public, CIA should have prepared a plan to protect the Pakistani doctor who was involved in the operation, as the case was leaked when he was captured by the Pakistani intelligence agency.

The question of whether the CIA vaccination campaign could be punishable under international law is rather a complex issue, which is not the main topic of this theses. What it also reveals, that legal considerations are closely related to the question of moral dilemmas. While intelligence oversight might not be enough to ensure that all the operations will be within the law, it is essential that the intelligence officers would take full responsibility in preventing adverse outcomes which could be tried and punished under the national or international law. Testing the operational decisions not only against the existing laws but also to the moral standards could contribute to decreasing the likeliness of the punishable acts.

### 2.3 Legal questions in practise

The legal issues of intelligence work came back to the spotlight after the 9/11, once the public debates about the CIA human rights abuses and torture caused a storm in media. The side advocating for exceptions to intelligence agencies in the law often state that fighting terrorism, according to laws, is a disadvantage because terrorists are not following the same laws. There is also an opposing part claiming, that if we operate outside the rules, we are no better than terrorists we are fighting. Both sides emphasise the complexity of the task that intelligence agencies face in trying to perform their best without breaking any laws. However, intelligence agencies in democratic countries are meant to follow the same democratic laws that apply to any organisation or individual. Furthermore, following the laws can help intelligence officers to avoid adverse outcomes or prevent the loss of public trust.

The Colombian military intelligence operation is not the only example that involves an INGO and raises legal issues. For instance, the previously mentioned case of HISG operating in North

Korea also underlines the possible violations of human rights. The political regime in North Korea is known for disrespect to the fundamental human rights and the precedents of ill-treatment of foreign citizens, especially American citizens, are frequent (Ripley, 2017). Therefore, the workers of HISG were unknowingly put at the grave risk. If the North Korean government had discovered the espionage activities by the HISG team, the humanitarians might have faced severe consequences such as life imprisonment or even capital punishment. It could be acceptable to take this risk under personal responsibility while being fully informed about the means and goals of the operation. However, it is unlawful to place a person in this position without her consent. Putting the clueless NGO workers at such dangerous conditions and not providing them with details about the actual goal of their mission potentially violate human rights. People, responsible for planning and implementing this operation, could face a trial.

It is also possible that taking into account all the existing evidence and background information, such violations of human rights would be partly permissible. For instance, in the case of European Convention, the European Court of Human Rights is entitled to consider circumstances and nature of derogation from human rights and make a final judgement according to the factual information (Garraway, 2007). That means that providing substantial evidence, that the operation was necessary for the state security, could acquit from human rights violation charges. For an intelligence agency, planning a risky activity, it is worth consulting international documents to see if an operation breaches any international norms. It is also essential to weigh the risks while evaluating the possible consequences. If intelligence organisation analysed relevant information and concluded that North Korea is posing an imminent threat, certain violations of international law might seem permissible. However, the laws could be questionable and interpreted in different ways.

Apart from the violations of the IHL, discussed in the previous section, the CIA vaccination case also draws attention to the potential legal implications related to human rights. It is unknown, whether the health workers who were sent to the compound were informed about the actual mission, as entering the house of the terrorist could be dangerous for the health workers. Moreover, although the doctor was involved in the process to oversee and make vaccination campaign real, not all the steps of the operation were correctly implemented. While sources contradict, whether it was polio or hepatitis vaccine and whether the kids or adults were vaccinated, it is clear that there were no follow-up shots, which is necessary in some cases

for the immunity system to benefit from vaccination. Therefore, it is also possible that people in the Abbottabad area were victims of negligent health care, which could be interpreted as a violation of human rights as well.

Due to the lack of tools and practices of International law enforcement and challenges in attribution it is not very likely that any national intelligence agency would face a trial as a consequence of the breach of law during their operations. However, even the legal trials are not plausible national intelligence communities should try to adhere to existing laws for several reasons. Firstly, following the rules, could reduce the risk of possible adverse outcomes, including damage to other actors involved in the operations. Secondly, it could protect the reputation of the intelligence community if the operation is publicised. Once the breaches of the law become public, it might augment the negative attitude towards intelligence work and decrease public support. This aspect will be analysed in more detail in Chapter 4. Finally, intelligence agencies of the democratic countries are expected to act according to the law as it is a part of their social contract that grants their legitimacy. As a result, while legal punishment might not affect intelligence agency, it is still essential that they would try to operate within the national and international law.

To sum up, depending on the country, national intelligence agencies can be more or less restricted by the national laws, since international regulations of espionage are still not well established. Therefore, while considering to implement an operation which involves an INGO, intelligence agencies might not weight legal implications as possible consequences. However, thinking about Geneva Conventions and human rights regulations could assist an intelligence community in making publicly defensible decisions. However, breaches of the law vary in severity. Hence, in extreme situations moral justifications or the success of the operation might be even more determinant than laws.

### Chapter 3 Moral dilemmas

If we perceive laws as a commonly accepted and formalised norms of behaviour, then legal and moral issues are not that distinct. The commonly accepted values are encoded into laws while commonly accepted customs define moral behaviour. Various conventions and legislative documents frame laws, but the moral norms are evolving and changing with the



emergence of the new traditions. Therefore, moral issues closely depend on the social, cultural or even religious background of the society.

In a broad sense, morality is defined as ‘certain codes of conduct put forward by a society or a group (such as a religion) or accepted by an individual for her own behaviour’ (Gert and Gert, 2016). ‘Ethics’ can, within this system of morality itself, refer to actual moral principles’ (Crisp, 2011). While both concepts have a variety of related descriptions in this research, the term ‘moral’ will be used referring to the broader understanding of commonly accepted principles and behavioural challenges. The term ‘ethical’ will apply to the defined set of rules belonging to specific moral codes.

Moral issues are unavoidable in intelligence work. They are encoded into the nature of intelligence work; as a consequence, the attention should be towards diminishing but not eradicating these questions (Omand and Phythian, 2013). In addition, different ethical codes should be applied to different areas of intelligence work such as methods, context and targets of intelligence gathering (Walsh and Miller, 2016). Although some dogmas could be called universal (e.g. that killing is immoral), the extreme variations exist (e.g. torture or even killing might be considered morally justifiable in certain circumstances). The variety of perceptions of morality create a challenge for intelligence officers operating in different backgrounds.

To find guidance in moral dilemmas, intelligence officers might need to consult various sources such as Machiavelli, Kant, Aristotle, Cicero, the literature of realpolitik or utilitarianism thinkers, writings by St Thomas Aquinas or even Bible and Veritatis Splendor (Olson, 2006). Different philosophical practices and concepts offer diverse solutions for moral dilemmas. However, even all the philosophers might not be able to give a clear answer to the intelligence officer trying to balance between righteousness and success. Therefore, intelligence professionals try to look at the established norms of behaviour, such as just war theory and construct their unique code of conduct.

This chapter will look at the moral dilemmas that arise in the intelligence operations which involve INGOs and will analyse what justifications and methods could help to avoid overestimations and prevent from causing harm. The first part of this chapter will discuss an application of ‘just war theory’ to the intelligence field and its strengths and weaknesses. It will also look at the real case scenarios related to this theory. The second section will look at the

application of consequentialism, as it is one of the most popular concepts applied in the security theories. And finally, the last part of this chapter will conclude by analysing other methods that intelligence agencies try to use for moral guidance and will discuss their application in intelligence operations.

### 3.1 Just Intelligence theory

Just Intelligence as a way to guide intelligence officers in their moral dilemmas originated from the Just War theory. Just Intelligence must be based on the principles of ‘just cause, legitimate authority, right intention, last resort, proportionality and discrimination’ (Bellaby, 2012). Judging the intelligence operation by these principles can assist officers in making more morally acceptable decisions. However, the critics of this theory emphasise, that military actions and intelligence gathering should not be guided by the same principles due to the difference in the nature of these two activities. Furthermore, the consequences of military action are more severe than the ones of an intelligence operation. In addition, some principles of this theory could be interpreted in many varying ways.

The most crucial and problematic of this theory is the principle of just cause. The challenge presented by this principle is how to justify riskier intelligence collection methods, like HUMINT operations, if there is a lack of relevant information to prove the existence of the threat. And often, the information which could prove that threat is not accessible or needs to be gathered by controversial or dangerous methods that even might undermine human rights. The HISG and Pentagon case highlights this situation. North Korea is one of the most closed countries in the world. It is a stiff challenge for intelligence professionals to gather information inside this country. Despite that, in 2017, the Worldwide Threat Assessment of the U.S. intelligence community estimated that North Korea poses ‘a complex and increasingly grave national security threat to the United States and its interests’ (Office of the Director of National Intelligence, 2017). With this in mind, endangering a group of missionaries travelling to North Korea could be justifiable for the purpose of crucial intelligence gathering. Of course, other factors, such as the odds of success, are also important. On the other hand, the question remains, what kind of intelligence was available before this operation was implemented, to support the

just cause. Sufficient evidence should be collected before preparing an operation that put humanitarian workers at grave risk without their consent.

Critics of the Just Intelligence theory highlight the fact that intelligence collection, unlike war actions, is often related to emerging threats rather than an already identified enemy (Diderichsen and Rønn, 2017). It creates an issue associated with the just cause principle illustrated by the North Korean case. The limits of actions that could be morally acceptable in the case of war and self-defence are not the same as moral limits for the intelligence gathering towards the perceived threat. In reality, it is comparatively easy to manipulate the just cause due to the knowledge monopoly that intelligence agencies hold in their respective countries. While politicians could (and indeed should) question the sources and credibility of the information presented, it is not always possible to cross check it. The famous examples of such one-sided and biased information presented to consumers include the case of Iraq and weapons of mass destruction<sup>10</sup>. To summarise, unless the threat is well documented, investigated and imminent, intelligence agencies should act more reserved and choose methods that match existing ethical standards. After all, looking back at the publicised intelligence failures, none of them was an outcome of reserved intelligence gathering operations or reluctance to break moral standards to access information.

The justness of cause also could be questioned in the CIA vaccination campaign. The most critical factor that could defend the harm potentially caused by this operation to the health sector is whether Osama bin Laden was still a dangerous criminal, or was it only an act of revenge for his previous crimes. Considering other factors should also help to evaluate the just cause. For instance, if the goal of the CIA would be to capture and question bin Laden to prevent a destructive attack, that could be a strong justification for breaching moral boundaries. However, as we know the operation following the vaccination campaign killed bin Laden (Brown, 2012). There is not much public information available to evaluate the danger posed by this terrorist at the time the operation was conducted. Moreover, it depends on the intelligence community, what information will be presented, and it is always possible that they will try to support their version of events and prove the just cause as a legitimate reason.

---

<sup>10</sup> More about this case in Phythian, M. 2018, "Intelligence Failure as a Mutually Reinforcing Politico-Intelligence Dynamic: The Chilcot Report and the Nature of the Iraq WMD Intelligence Failure", *British Yearbook of International Law*.

While Just Intelligence offers a specific framework for solving moral issues, the real boundaries of intelligence actions still depend on the moral values of the society in which the agency exists. 'In a democratic and pluralistic society, intelligence work is legitimised by public consent and is morally justifiable only if it conforms with the moral criteria that reflect a society's accepted values' (Gendron, 2005, p.402). Intelligence agencies are part of the society that they are meant to protect. Therefore, the principles of right intention and proportionality could be interpreted differently in every country, depending on the values and beliefs of society. In the vaccination case, it is possible that the public wish for revenge provided the U.S. intelligence community with the consent necessary for taking more extreme measures to hunt down the terrorist. It could be seen as a symbolic act of restoring national pride, that many individuals would identify as of the highest importance. Although it might have a lower significance in terms of national security, it is still worth the risk if the society provides consent to such operations.

A more liberal approach to intelligence gathering is also determined by the common perception. According to David L. Perry 'espionage and covert action are usually not perceived to be as damaging and provocative as acts of military aggression and partly for that reason are not kept in reserve by states as measures of last resort' (Perry, 2009, p.96). And the security and life of individuals, as well as prevention of war, is often presented as the highest goal that needs the sacrifice. However, the equation often gets more complicated in the actual intelligence work when the question is not if the life will be saved but whose life will be saved or how many lives could be sacrificed for the benefit of the rest of population. Historical examples illustrate that.

In 1940, British decided not to warn the city of Coventry about the upcoming attack, to protect their capability to read German codes, and it resulted in 300 deaths from the Luftwaffe bombing (Olson, 2006, p.188). Although it is argued that the British ability to read the code saved more lives, the moral justice aspect of such a decision could hardly be evaluated even if the principle of proportionality could be applied. The sacrifice for the 'greater good' could be criticised as the situation could always be read from different perspectives. It is hard to imagine that the inhabitants of Coventry would agree to the destruction of their town and deaths of fellow citizens as a reasonable price for possibly more successful military actions in the future. This

case illustrates that while the Just Intelligence principle cannot be just to everyone, the principle of proportionality is crucial.

Proportionality principle rules that the greater is the threat, the more ethically flexible methods could be used in intelligence work. One of the common factors to identify the grave danger 'includes the potential for widespread loss of life' (Gendron, 2005, p.422). This principle applies to the Colombian military operation. Although misuse of the humanitarian emblem is a breach of law according to Geneva conventions, the goal of this operation was to save hostages, and, according to some reports, one of them was in a critical condition (Aljazeera, 2008). Saving lives of abducted people could be identified as proportional to the minor breach of the Geneva Conventions. However, more often, the 'loss of life' could be overestimated identifier in Just Intelligence, as often precise information is needed in order to calculate possible atrocities. Intelligence gathering, unlike war, is more related to emerging threats. It deals with the future, which is indeed something hypothetical and not real, and it often lacks some bits of information. Therefore, the work methods respectively should be less extreme, risky or immoral comparing to war actions.

The last principle of discrimination is related to the immunity of non-combatants. In traditional conventional war, military personnel wear uniforms and could be clearly distinguished from civilians who must not be targeted<sup>11</sup>. But intelligence personnel often work undercover, not to mention, that people who possess strategic information related to state security can be simple civilians. Some researchers identify five categories of legitimate intelligence targets as (I) ordinary citizens, (II) people in possession of critical information but unknowing about its value, (III) people possessing and having limited knowledge about the value of information, (IV) people who possess and are fully knowledgeable about the strategic information and (V) people in the game, such as intelligence professionals (Pfaff and Tiel, 2004). The personnel of INGOs' are likely to belong to the categories two, three and four depending on the level of their knowledge and the kind of work they do.

Since humanitarians operate under neutrality and impartiality mandate, they should be spared from intelligence operations and should not be targets of espionage even if they possess strategic military information. However, Just Intelligence theory partly legitimises

---

<sup>11</sup> This rule does not necessarily apply to asymmetrical or hybrid warfare.

humanitarians as a target. From the one hand, INGO workers are regular citizens such as employees, for instance, working in a company manufacturing defence systems. Therefore, they could be legitimate targets as anyone else. From the other hand, the parallel to the Just War theory could be applied. In war, humanitarian workers are not targeted, not only because they assist the population in need and wounded soldiers of any side, but they also do not pose any military or strategic threat to the course of a war. Similarly, even they can sometimes possess vital information (for instance, when the passage will be open for delivering humanitarian aid to a besieged city), they do not use this information to influence the development of the conflict. As a result, they should be excluded as non-targets.

Overall, the principles of Just Intelligence are useful to test various moral issues of intelligence operations. However, there is a need to clarify and unify the interpretations of specific aspects. Otherwise, it could become a tool to justify any morally questionable actions rather than guide the intelligence community. It should be adapted in a way that it would better reflect the nature of intelligence work, as it significantly differs from the military actions.

### 3.2 Consequentialism

It is important to remember that intelligence agencies often work under time and other constraints and sometimes in a close relationship with their consumers. It could be that the pressure from the policy-makers more often leads intelligence officers to consequentialist thinking. While there is a variety of consequentialism interpretations and forms, the common definition states, that if the consequences of an action are beneficial to the majority of people, then this action is morally right. However, the notions of 'majority' and 'benefit' are subject of discussion. William H. Shaw observes that '(C)consequentialism is not a complete ethical theory because it does not specify what is good or bad' (Shaw, 2014, p. 21). Instead, it provides a framework that could be used in examining ethical considerations.

Comparing to the Just Intelligence theory or other ethical codes, it is more flexible as it does not propose clear rules. Moreover, any activities that 'maximise the good' could be morally acceptable (Erskine, 2004). Therefore, in some cases, consequentialism tolerates the behaviour that would be totally immoral judging by the other ethical theories. For instance, Christian

ethical rules could not justify killing a person, and other solutions (as capturing or life imprisonment) would be more acceptable. But in consequentialist theory, torture or killing could be justified if it prevents a big calamity. In addition, the consequentialist framework is related to public consent as well. If the more significant part of society supports the goal, and it is reached in a timely manner, the public might be more mellow towards the means of achieving it. Similarly, the policy-makers are also more likely to support an intelligence action if the main goal is beneficial to the majority of people as their legitimacy is also granted by the public.

One of the issues with the consequentialist thinking in intelligence work is, that it is not clear what consequences it should measure. It is likely that different estimation would come for the consequences of intelligence gathering operation (I), the consequences of the disclosure of intelligence gathering operations (II), or the consequences of political decisions as a result of intelligence gathering (III). All three cases raise different dilemmas, and it could allow different ethical boundaries. For instance, if it is presumed that what will become publicly known is the final result of the operation (e.g. the killing of bin Laden), but not the means and details of achieving it (vaccination hoax), intelligence officers could be encouraged to make riskier decisions and not always correctly evaluate possible secondary outcomes.

When judging the operation, according to consequentialist theory, the odds of success are extremely important. But in some circumstances, even unsuccessful operations prove to be morally justifiable. For instance, there is no consensus whether the CIA actually managed to get the DNA of the people who lived in a compound with a Bin Laden during the vaccination operation. Some evidence even suggests that they did not succeed to get DNA, which was a primary goal of the operation and the secondary aim in the long-term strategic plan. The strategic goal was to get more evidence that it was a hiding place of the terrorist and the information that the health workers gathered from their visit to a compound contributed to the confirmation of that fact (Cozine, 2013). As a result, even the HUMINT operation did not achieve a primary goal of collecting the DNA; it still contributed to the strategic goal of increasing the calculated odds that bin Laden was in the compound. If bin Laden was posing imminent danger or planning a terrorist attack, this operation and the consequences that followed could be described as morally acceptable from the consequentialist point of view.

From the moral perspective, the vital question remains, whether the operational outcomes balance the consequences caused after the Pakistani doctor was detained, interrogated by Pakistan's intelligence services and disclosed the knowledge about the operation resulting in a vaccination ban by the Taliban. From the one hand, vaccination in developing countries often faces scepticism (Nature, 2011). Therefore, it would be unfair to state that the Taliban's prohibition and the killings of health workers were a direct outcome of the publication of the CIA operation. From the other hand, the Taliban's actions concerning the vaccination are more related to this case, as the Taliban is an enemy of the U.S., and this organisation is also a target of CIA espionage. Reacting to the negative developments in the health sector after this case was published, the deans of twelve prestigious medical schools in the U.S. sent a letter to President Obama (Buekens, M.P. et al., 2013). Reacting to this letter, White House issued a response, stating that vaccination is not going to be used as a part of intelligence operations in the future (Gambino, 2014). It shows that considering the aftermath of the disclosure, the government acknowledged the negative consequences and took moral responsibility. This case illustrates, that while all the possible outcomes and developments could be hardly predictable, there is a need for ethical evaluation not only of direct but also indirect consequences.

The North Korean case could also be seen as an operation based on consequentialist thinking. Currently, the U.S. Intelligence community defines North Korea as one of the most challenging countries for intelligence operations (Klimas, 2017). Still, the potential threat from this country exists. Therefore, the consequentialist theory could easily justify even extremely challenging measures to gather intelligence from North Korea. Looking at the HISG example, it is not entirely clear whether the operation was successful, as there is a lack of publicly available information. If it succeeded to gather information from North Korea that the intelligence community was hoping, the operation could be morally justifiable. However, if the operation did not or only partly succeed, endangering humanitarian workers would be less tolerable.

To sum up, while consequentialist thinking might not be the best way to help intelligence professionals to distinguish between right and wrong, it can provide additional guidance in evaluating moral dilemmas. However, consequentialism is not likely to be a useful theory to defend intelligence actions in public.



### 3.3 Evolving code of conduct

Reacting to the shifting security issues and the boundaries that intelligence agencies are sometimes forced to cross, The EU parliamentary Assembly raised an idea of the European code of intelligence ethics as '(i)t is essential to strike the right balance between our concept of freedom and our need for security' (Parliamentary Assembly, 2005). This should not be an impossible task, as an analogical set of rules exists for police work. However, the exceptionalism thinking that exists in intelligence work and the nature of intelligence activities might prove such code of conduct idle. It is always possible to imagine a critical situation when breaking the rules will be the only way to protect the so-called 'greater good'. On the other hand, if such code of conduct would be internationally applied and followed, that could encourage more intelligence agencies to collaborate. Currently, one of the main intelligence sharing challenges are violations of human rights or democratic principles that prevent countries from collaboration (Sepper, 2010). The universal code of conduct could contribute to reducing violations and allowing intelligence exchange. But looking at the application of rules of war and IHL, it seems that international applications of intelligence work ethics are hardly probable. Some countries lack intentions to adhere to the international rules, and there are no established reliable tools of enforcement to propagate them.

While an international code of conduct seems less achievable, regional or national intelligence codes of ethics could be established. It would help to find a balance between the protection of human rights and the implementation of security and would also assist in intelligence oversight. Most importantly, establishing the code of conduct would also contribute to guarding intelligence reputation and public consent, and it would help to defend intelligence actions if a controversial case is disclosed to the public. The trust between the intelligence community and society can be damaged by the immoral actions of intelligence (Pfaff and Tiel, 2004). If the operation that contradicts society's ethical norms is disclosed, it can cause public outrage and have negative effects on future intelligence work. It is observed that mutual trust between society and the government concerning security is lacking (Omand, 2010, p.263). The lower society's trust in intelligence might complicate governments ability to ensure security as well. Hence intelligence code of conduct would not only help to ensure a positive public image of intelligence but would also strengthen the trust between society and government. The implications for the intelligence reputation that arise from the disclosed morally questionable intelligence actions will be discussed in the following chapter.

EU Parliamentary assembly is not the only one to suggest that Intelligence should take an example from the police community and put more efforts into the creation of a unified ethical code. Some scholars see the mission of intelligence agencies as providers of 'social peacekeeping' (Diderichsen and Ronn, 2017). Such definition only supports the idea that intelligence needs the clearly defined ethical rules to follow, so the means of guarding the society would not contradict with the public values. For instance, the Australian intelligence community follows the code of conduct that is common for all public service (Phillips, 2016). However, it is rather general guidance of good conduct which does not help in an extreme situation when the stakes are high. Regardless of what ethical rules the intelligence agencies decide to follow, the ultimate decision is still highly influenced by the personal values and attitude of the individuals in power. As a result, establishing the code of conduct for a national intelligence community would also contribute to reducing the effects of the individual decision making and could prevent some of the negative consequences.

The argument that certain ethical codes, like deontological one, can limit intelligence's ability to protect society is a valid one. Due to the nature of intelligence work, there is a need for a special code of conduct that would balance the security needs with moral laws. However, the rules still should be clearly defined, as leaving some flexibility in moral dilemmas could easily lead to exceptionalism or consequentialist approach, which permits some extreme actions. Correspondingly, if Kant's categorical imperative principle would be applied to intelligence work, most of the operations would hardly pass the moral test. Categorical imperative could not allow sacrificing the lives of a few hundred people for the strategic military advantage as it states that humans should not be treated only as means but also ends. For example, in the case of HISG, the humanitarian workers were clearly treated as a means but not the ends. As it was discussed in chapter 2, from the legal point of view, it was a human rights abuse as well. The complexity, that intelligence agencies face on their daily tasks is one of the main reasons why creating a code of conduct is such a challenging task.

Practise often profoundly differs from theory, hence due to the time constraints or lack of human resources intelligence officers might not be able to perform an in-depth analysis of the moral dilemmas if there is a ticking bomb that needs to be neutralised. Therefore, in order to be handy, the intelligence code of conduct should be simple and focused. The good example is the moral considerations crystallised by David Omand into two main elements. First, whether

the action performed in secret could be defended in public and second, whether the tactical action is actually helping to achieve the strategic goal (Omand, 2010, p.287). These two questions cover the variety of risks that intelligence agencies might face while employing ethically questionable methods. On the other hand, the CIA vaccination campaign might seem like a morally acceptable operation before it was implemented. However, it is difficult if not impossible, to predict if the case will be disclosed or evaluate the damage inflicted to the INGOs or the health sector by the publication. As it was discussed in the first chapter, the trust that an INGO builds with the local community and other stakeholders is essential to their work, and the aftermath of the operation had direct consequences to this trust.

The cases analysed in this research only confirm the need for an intelligence code of conduct. Nevertheless, the creation might take some time due to the complexity of issues involved in intelligence work. Some researchers suggest that such a code of conduct should not be prescriptive but more aspirational (Phillips, 2016, p.55). It would assist intelligence officers in navigating the moral issues but would not restrict their ability to prevent crimes. But the balance is yet to be found. If we think about Maslow's hierarchy of needs, security takes the second most important position after the psychological needs, and security in this theory is defined as the lack of harm (Taormina and Gao, 2013). Therefore, from a certain perspective, protecting the nation from the terrorist threat, but causing harm in other areas as an outcome does not satisfy the main goal of providing security in a broad sense. Choosing moral ways of conduct is likely to be an interest of the government, intelligence agencies and society.

The CIA, in its Twitter account, presents itself as a 'Nation's first line of defence. We accomplish what others cannot accomplish and go where others cannot go' (Twitter, 2019). From the public relations point of view, this is simply a catchy line that tries to evoke patriotic feelings and fuel curiosity. However, stating that they go to the places where others cannot go, already raises a question, whether it is legally and morally defensible. Going back to the previously mentioned point, that public provides legitimacy to the government and its institutions, it is clear that the moral codes to which intelligence agencies function also depend on public perception of intelligence. Declaring that the intelligence community is ready to break the rules for the national interest could also be seen as a part of a code of conduct if society approves it.

Finally, it would be a valuable practice for the society, consumers and intelligence professionals to accept the fact that sometimes a particular piece of information is inaccessible. This would reduce the pressure to succeed and commit immoral actions to reach the goal. Australian decision to create a common code of conduct to all public service workers shows that despite the secrecy aspects intelligence agencies are just one of the government institutions. It does not place intelligence work in exceptional position but helps to draw boundaries and even lower the expectations that consumers might have regarding the intelligence product. From the society's point of view, intelligence code of conduct could also increase the trust, as the cases in authoritarian states prove, that the limitless power of intelligence agencies could increase the insecurity rather than the opposite<sup>12</sup>.

This chapter has illuminated the main moral dilemmas and challenges that intelligence faces and how it is relevant in the operations which involve INGOs. It also gives a perspective on how moral and legal aspects are interconnected. While intelligence tries to adapt and transform existing ethical codes used in related fields, the unique nature of this profession calls for a more specialised approach. The following chapter will look at the effects of morally and legally questionable actions and resonance that the operations involving INGOs could evoke in the public sphere.

#### Chapter 4 Image of Intelligence and the role of INGOs

It is difficult to imagine that there will be a top-secret that will never get disclosed. Although not all countries have declassification procedures in place, any state could experience the unauthorised disclosures of its secrets by whistle-blowers, investigative journalists or human rights groups. In this time of history, we learn more about the intelligence operations implemented during the second world war. It is not difficult to imagine that in the future, more cases and classified information from the 'war on terror' will be published and discussed. It is

---

<sup>12</sup> The classic example is Soviet intelligence agency KGB and its successor agency FSB which (apart from other goals) is tasked with securing political regime and is using extrajudicial power to achieve it. See Bateman, A., 2016. "The KGB and Its Enduring Legacy". *The Journal of Slavic Military Studies*, vol. 29, no. 1, pp. 23-47.

very likely that the image of the intelligence communities will depend on those stories. Although in the short term, intelligence agencies are more concerned about achieving the goal, in the long run, it will be questioned 'how' they achieved it. Therefore, in this chapter, I will explore what impact the disclosure of the operations involving INGOs might have on the image of intelligence. Both entities that are the objects of this research highly depend on their public image and reputation. The importance of image for INGOs was already discussed in chapter 1. In this chapter, I will analyse in details the public image of intelligence agencies and what effects it might have for their functioning.

In clandestine operations and covert action, countries seek to stay anonymous and unidentified. If secret intelligence action is publicly attributed to a particular country, it often is perceived as a failure. In those cases, plausible deniability is a useful practice that can save the image of a state. However, the newest developments in communication technology made information more accessible to regular citizens; therefore, plausible deniability is more often jeopardised (Cormac and Aldrich, 2018). If there is sufficient and incontrovertible evidence showing that the operation was implemented by the national intelligence agency, denying it might further damage the image of that state and its intelligence. Consequently, while planning their operations or covert action activities, intelligence organisations should simultaneously prepare their communications strategy for different outcomes and evaluate possible consequences.

In the first section of this chapter, I will discuss the dilemma of secrecy and transparency that all intelligence communities functioning in liberal democracies face. Understanding this will allow us to perceive the public communication challenges of intelligence agencies. The second part will look at the formation and purpose of public opinion concerning intelligence. It will analyse what target audience intelligence public relations (PR) tries to reach and why. Finally, the last section of this chapter will examine the issues that are raised when the cases of intelligence operations involving INGOs are disclosed.

#### 4.1 Increasing transparency of intelligence work

In democratic countries, intelligence agencies function as one of the governmental institutions, without the exceptional powers or hidden agenda<sup>13</sup>. Hence, they have to meet the requirements that apply to any other institution. The secretive nature determined that intelligence agencies were historically less open compared to other government bodies. But the changes in media and new demands from civil society affected intelligence agencies as well. An important turning point, and in some sense even the new era, in the discussion of intelligence oversight and transparency emerged after the Snowden's disclosures. It sparked new debates in western countries not only about the privacy and mass surveillance but also about the oversight of intelligence agencies and their accountability. Media played a crucial role in shedding light on the leaked documents, informing the public about the ongoing investigations and the course of the events that followed.

Furthermore, the role of media in intelligence matters is becoming more significant. Florina Cristiana Matei defines five functions that media performs in intelligence democratisation. It is 'informing the public; liaising government with the citizens; helping boost government legitimacy; exercising informal external oversight of the government; and providing a "learning" environment for elected officials and the public' (Matei, 2014, p.78). All these functions not only serve in strengthening democratic processes between citizens, governments and intelligence agencies but also contribute to better society's understanding of intelligence work and increasing transparency. Media becomes an intermediary and a platform for dialogue between institutions and people.

Naturally, intelligence agencies want to control and oversee the information that is disclosed to the public. However, this want is not simply fuelled by the need to create a consistent and positive image of intelligence, but also to be able to continue the work in the same manner and protect their sources. Joffrey T. Richelson concludes that sometimes the government's desire to keep secrets is 'legitimate, but sometimes it is instead the desire to avoid revelations of failed policies or programs, or misconduct' (Richelson, 2012, p.666). Without access to the classified information, it is impossible to judge whether the government is not abusing the need for

---

<sup>13</sup> In less or non-democratic countries, intelligence agencies might be tasked to protect the political regime and might be exploiting their powers.

secrecy. Some examples illustrate that the issue is growing bigger. For instance, there were more prosecutions of whistle-blowers under the Obama administration than under previous presidents all together (Ackerman and Pilkington, 2015). It is also probable that the number of whistle-blowers was growing in recent years and the establishment of platforms, that could grant at least partial anonymity to the leakers, like wiki-leaks, encouraged more people to reveal secret information. However, if there will be no questionable or compromising material, there will be fewer people who decide to blow a whistle.

Therefore, the good image of intelligence is closely related to the improvement of work ethics, successful operations, openness (even limited) to public and prepared public relations strategy. It is still a common practice in many governments to classify more information than it is needed (Richelson, 2012). Finding the right balance between openness and successful work is challenging but not impossible. To understand, why intelligence agencies tend to keep more information in secret than it is necessary, we need to investigate the relation between operational success and secrecy. To illustrate this relation, I will present a table (see below).

Suppose, that the most important aspect is to achieve the goal of the operation; therefore, success in achieving the goal could be identified as plus two points, while unsuccessful operation would constitute minus two points. Although secrecy is a relevant factor it takes a secondary position compared to the operational goals; therefore, it will be awarded plus one point if the operation stays classified and minus one point if it is disclosed. These simple calculations shown at the table reveal that successful operation, regardless if it is disclosed or not, does not bring negative effects on the reputation of an agency. It could be argued that disclosure of the successful operation could even win more support to intelligence agency from the public; however, it is possible that intelligence will try to deny the operation for the sake of protection of its methods, or due to the plausible deniability strategy<sup>14</sup>.

	<b>Disclosed (-1)</b>	<b>Undisclosed (+1)</b>
<b>Successful (+2)</b>	1	3
<b>Unsuccessful (-2)</b>	-3	-1

---

<sup>14</sup> More about plausible deniability: Cormac, R., Aldrich, R.J., 2018. "Grey is the new black: covert action and implausible deniability". *International Affairs*, vol. 94, no. 3, pp. 477-494.

The table also shows that an unsuccessful operation which is disclosed contributes to the negative image of the intelligence community. 'The exposure of covert collection activities can jeopardise the reputation of an agency and deprive it of ministerial and public support' (Gendron, 2005, p.421). While ministerial support is more related to the financial and practical matters, public support goes back to the trust and legitimacy issues which are crucial in democratic states. Therefore, the management of public relations is closely linked with the image and functioning of an intelligence agency. Furthermore, while the success of the operation is essential, keeping unsuccessful operations disclosed is equally crucial not only for the sake of an intelligence agency but also to avoid causing damage to other actors that were involved in the operation.

It is possible to argue that, what should bring more support for the intelligence work is not the way operation was conducted, but the strategic goal that was achieved. Operational success might not always lead to a strategic goal. However, while sometimes there is no damage in disclosing the details of the operation, there are rarely ever possibilities to publish more information regarding the background or context related to the operation. This creates a situation, where the public is almost never able to see the full picture and comprehend the real long-term achievements of intelligence work. Therefore, intelligence agencies have to choose specific ways of communicating about their efforts and accomplishments.

Publicising success stories from intelligence work is a significant element of their communication strategy. There is a direct connection between increased legitimacy and publications of successful intelligence operations (Matei, 2014). Society is more favourable of intelligence if it is efficient and can meet the expectations raised by policy makers and the public. Furthermore, the functioning of intelligence agencies could be compared to social enterprises (Chiru, 2016). However, serving the public good and contributing to the security of the state is not enough. Intelligence agencies also have to keep contact with society and communicate about their progress and achievements, so the public would be informed about the good deeds done for its sake.

Increasing transparency and reporting to the public about intelligence work helps to maintain a positive public image. Christopher Richard Moran observes, that '(t)he value of the public relations is diminished if it is not backed up by the disclosure of supporting secret materials' (Moran, 2013, p.351). Disclosure of the intelligence successes allows society to grasp the



importance of intelligence and trust, that the work methods used are not all shady, immoral or lawless. The disclosure of successful operation is very likely to bring a positive impact from the public relations point of view. On the other hand, if the public will be fed only successful operations, it will resemble propaganda rather than the public relations strategy. Therefore, intelligence agencies should also consider disclosing some unsuccessful or partly failed operations so that the public could see a more realistic image of intelligence. It could be a risky decision and not necessarily beneficial; however, if society is left out in total obscurity or only with the one-sided information, it might encourage unauthorised leaks and speculations.

It is also possible to argue that if intelligence is fully functioning according to the existing norms and regulations of a country, there should be no leaks of information. Unauthorised disclosures could be beneficial for exposing misconducts and abuses by government or even save lives (Richelson, 2012, p.657). Knowing, that negligent attitude or ignorance could result in unauthorised disclosures, might motivate intelligence communities to strive for perfection and work methods that adhere to the legal and moral rules of the country. On the other hand, information leaks can cause irreversible damage to the intelligence, other actors involved, society, security and also the leakers, as the cases of Julian Assange, Chelsea Manning and Edward Snowden have revealed. Due to the limitations of this research, it is impossible to discuss all the reasons and motivations that encourage unauthorised disclosures. However, it is essential to highlight that the operations discussed in this thesis, where either leaked to media or became public without the authorisation. And while the true motivations of the leakers might be unknown, it is very likely, that the operations seemed problematic or controversial to the people who decided to disclose them.

#### 4.2 Intelligence struggle: public opinion

The first section of this chapter presented factors in which publicity through media and public opinion influences intelligence. This section will further discuss the audiences that might be targeted by intelligence agencies, different PR strategies that might be employed and possible outcomes. Strategic intelligence communication is still a developing field, which encounters some scepticism, but should not be underestimated as well.

As it was aforementioned, the nature of intelligence work determines that society does not know particular details about intelligence work. When intelligence agencies do not pursue the PR strategy and are not providing at least limited knowledge to society about their work methods, successes and failures, other actors might and will try to do it. Without relevant access to information, journalists or activists might create and publish stories that do not match reality or discredit intelligence communities. Understanding this, intelligence agencies try to release more information to the public, be more accessible and follow the existing public communication trends when it is possible.

CIA could be taken as an example of one of the most open intelligence agencies. It is present in four social media channels (Facebook, Twitter, Flickr and YouTube), where it communicates about the news and historical events related to intelligence work, announces vacancies or encourages citizens to inform the agency if they get to know information related to the state security. Such a presence in social media feeds society's curiosity and increases trust in the agency. At the early stage of intelligence PR development, it was perceived more as education rather than communication matter (Hulnick, 1999). Consequently, the CIA website is also equipped with the "Library" section, which allows academics and students of the field to access a variety of documents, reports and unclassified files (CIA, 2019). Therefore, the agency is not merely trying to increase its openness while addressing the general public, but it also encourages scholars interested in the intelligence field to deepen their knowledge and understanding, in this way supporting the image of a committed and reliable organisation.

Public communication also has a broader purpose. The positive image of the intelligence community in public also helps to strengthen the morale inside the intelligence organisation (Moran, 2013). If intelligence officers see that society understands and appreciates their work, they will be more motivated to keep high standards and give extra efforts in their daily work. On the contrary, if public criticises intelligence work methods and perceives the agency as immoral, it would have negative consequences on intelligence personnel. Low morale could encourage information leaks or even defection. In addition, the negative image of intelligence would also limit the ability to attract new talents. As a result, while communicating to the general public, intelligence agencies have to consider not only how the intelligence representation will be perceived by the general public, but also how this representation will affect serving intelligence officers and potential recruits or collaborators.

Not all intelligence agencies follow a similar communication strategy. As a contrast to the CIA, the British MI6 takes a more usual approach and does not engage with the public or media. In their website there is a form that people can fill if they want to pass some information but in the 'Media enquiries' section MI6 explains that they do not have a press office and to protect their work they 'never comment on operations, staff, agents, or relations with foreign intelligence services' (SIS, 2019). However, it is possible that the organisation uses other, indirect ways to establish its public image as an essential and trustworthy organisation. Such tools could be authorised leaks or official statements made by consumers or publishing of authorised history (Security Service, 2019). It might seem that the agency which is related to the world famous series of James Bond films do not need a public communication strategy. However, even this organisation, from time to time have to license its officers to give interviews to bust the myths created by the film industry (Johnston, 2006). In those rare cases of publicity, the agency wants to deliver an important message, that it acts according to the national laws.

General public and policy-makers are not the only audiences that intelligence agencies are communicating to. Other intelligence bodies inside and outside the country are also a target group that could be encouraged to collaborate by successful stories published in media (Magen and Gilboa, 2014, p.489). Correspondingly, if operational information is leaked, where immoral or illegitimate actions are exposed, other intelligence agencies might distrust it and be unwilling to collaborate. Furthermore, if the agency cannot prevent unauthorised leaks, it will reduce its reliability. Besides, once the operation in a foreign country is disclosed, it can significantly complicate future operations and relations with that state. Such examples can have long term effects that will restrict intelligence work. As a result, intelligence agencies need to plan and examine how their public image will help or interfere the relations with the foreign intelligence communities.

Unwanted publicity is another common issue that intelligence organisations face. Occasionally the media exposes some intelligence failures or unsuccessful operations. In such cases, intelligence agencies are often portrayed in dark colours and unilaterally. The best way to respond to such unwanted publicity is to disclose some information that would expand society's knowledge about intelligence operations and their mission in securing the state. Planning the strategic communication campaign, which would allow society to see the more complex picture

and better perceive the challenges of intelligence work, would be another great solution from the complicated situation created by whistle-blowers or media.

Intelligence agencies need to handle sensitive information in the world of high stakes. As a result, public communication could be seen as a curse or a powerful tool for agencies that deal with secret and delicate matters. It is clear, that all audiences that intelligence agencies target want to see them as competent, reliable and professional organisations acting according to the laws. It is true that the best way to maintain such an image is to be one. But in critical situations, having a proper communication strategy in place could save an organisation from more significant issues.

#### 4.3 Practical considerations about balancing the trust

These days we are surrounded by the products of professional PR strategies from a chocolate bar to a presidential candidate; it all relies on a well-researched, planned and implemented public relations campaigns. But even the most talented PR strategists might struggle to fix the reputation of an organisation, which continuously falls in scandalous situations. Therefore, adhering to moral rules and acting according to the law, is extremely important for the reputation of the intelligence community. Nathan J. Phillips argues, that ‘by carrying-out its work ethically, intelligence agencies are more likely to be seen as beneficial in standing-up for liberal democratic principles by increasing public support’ (Phillips, 2016). Intelligence agencies will gain more support if, in public, they will speak the values that they apply in secret. However, in practice, it is a puzzling task. The society is never homogeneous even in a small country. Hence the values vary. Intelligence agencies have to prioritise and guess what actions they will be able to defend publicly, without losing the public trust.

This section will discuss in more details the broader impact to intelligence and non-governmental sector, caused by the publication of the operations involving INGOs. The analysis of the three disclosed cases will reveal the factors that determined the aftermath of the actions. It will lead to the proposed ways of conduct for intelligence agencies, that could reduce the likelihood of harmful outcomes.

Moral, legal and reputational issues that were evoked by the publication of these operations reveal several conclusions. First of all, humanitarian and non-governmental organisations are often seen as entities striving for high moral standards and oriented towards the public good. Some of the humanitarians working in extreme conditions even risk their lives for helping other people, what could be perceived as the highest sacrifice. Such a selfless service and representation of highest ideals could be compared to the work of religious leaders and community. And some of the humanitarian workers also belong to religious groups. A former CIA employee in one of the interviews said that media or religious figures and peace corps are not used for the disguise reasons by the CIA as they are too vulnerable (Wired, 2019). It is difficult to judge whether it could be an official position by CIA, a guiding principle which could be disregarded or only a statement made for the purpose of public opinion. In any case, not using media, religious and humanitarian actors for the cover should be a rule. Exploiting their vulnerabilities places intelligence agencies in the antagonist position and might damage intelligence image which can be very challenging to restore. Taking the public image into the equation is an essential part of evaluating the outcomes of the operation.

If intelligence misconduct related to INGOs becomes public, it might be a good strategy to admit it, apologise and provide an explanation of why using an INGO was regarded as an appropriate strategy. In this way, the society and humanitarian community could appreciate intelligence struggle and efforts for a good cause and be more forgiving. Colombian military operation illustrates this situation very well. Of course, the advantageous circumstance was that the hostages' rescue operation was successful. Therefore, the misuse of an emblem and the possible damage done to the red cross workers were of lower importance.

In some instances, like the CIA vaccination case, the public desire for the success of the strategic goal could grant the population's support for more problematic or even unlawful intelligence actions. At the time, this operation was implemented, bin Laden was the number-one enemy of the nation, and it is very likely that the U.S. society understood that fighting terrorists need unconventional decisions and even possibly illegitimate actions. Noticing this approval from the public, the U.S. intelligence agencies were able to take more controversial actions without risking their reputation. It could be seen as a special case that could be compared to a war situation. But in normal circumstances, society expects the intelligence community to function by the same rules as any other government institution. The exceptionalism thinking that was common in the emerging state of democratic intelligence

agencies is not compatible with the increased transparency and accountability that is currently seen. As a result, intelligence agencies might benefit from the close observation of social mood and changes in public morale.

It is possible that intelligence agencies decide to exploit INGOs, as a last resort, while trying to meet the unrealistic expectations from the consumers or the public. The mismatch of the actual intelligence capabilities and the expectation coming from outside create a 'performativity gap' (Petersen, 2019). What would help to avoid crisis influenced by performativity gap would be communicating to society and consumers about the real capacity of intelligence and avoiding mystification and attribution of supernatural powers to intelligence agents. It is possible that fictional products (such as books and films) related to intelligence work also contribute to rising expectations from the public. If society would be better informed about the real challenges that the intelligence community encounters, it would reduce the unrealistic hopes. If a crisis situation arises, and the public knows that intelligence performed all the necessary actions to prevent it, there will be no blame on intelligence agencies and no adverse consequences to the trust between society and intelligence.

Discussing the shifting work environment for the U.S. intelligence, Charles Cogan observed that intelligence officers are becoming hunters rather than gatherers, as the actions involved in their tasks are more aggressive (Cogan, 2004). Indeed, asymmetrical warfare and terrorist threats summon extraordinary measures. It is also the case with the threats coming from undemocratic countries such as North Korea. If mass media frames a risk coming from a specific country as a growing imminent threat, it also contributes to legitimising less moral and legal actions. After the HISG espionage story was leaked to the media, the attention was drawn more to the fact, that the organisation was funded by the Pentagon (misuse of the public fund), instead of the fact, that the missionary workers were facing grave risks if they were to be discovered as spies in North Korea. Furthermore, the question remains, if the publishing of this story did any good. It is not likely that the intelligence agencies terminated the practice of using INGOs in their operations, nor that this exposure caused any significant reaction from the U.S. society. However, the information could have reached North Korea and caused further implication of INGOs trying to work there.

It leads to the next observation. In a discussion about the image of intelligence, it is important to remember that the operations discussed in this thesis carry consequences not only for

intelligence bodies but for INGOs as well. And it is possible to argue that revealing information about such operations evokes severe and unpredictable effects on INGO work and credibility. Intelligence agencies should consider it their partial responsibility to protect the reputation of the entities involved in the operation. Therefore, all extra efforts should be put in protecting the material related to the operations involving humanitarian organisations. If such information is likely to be disclosed, all the measures to preserve at least the identity of an INGO should be taken.

The final equation of whether to declassify the successful operation for the benefit of increasing public support to the intelligence community should involve considerations of possible effects to the whole non-governmental sector. Public trust is a crucial element for humanitarians working in conflict territories. And cases as the HISG espionage in North Korea could spread distrust in smaller INGOs by showing that some organisations are not able to ensure transparent funding and could be easily manipulated by the donors or even influenced and used by intelligence.

Thirdly, intelligence agencies should aim for eliminating exploitation of INGOs from their tool kits. It would ensure that intelligence agencies would not suffer the increase of negative public opinion as a consequence of taking advantage of the humanitarians and missionaries. And it could open up possibilities for cooperation.

There is a potential for intelligence and INGOs to find a proper way to support each other in a collaborative manner. INGOs, especially those working in the humanitarian field, have skills and competencies that would be possible to share with the intelligence community without breaking their neutrality and impartiality mandate. The critical condition for that is trust and mutual understanding. Intelligence agencies have to fully perceive the sensitive position of INGOs and support them instead of taking advantage. In exchange for specific information or competences, intelligence agencies could support INGOs in critical situations, such as the abduction of INGO workers or share some analytic knowledge or tools. Mutual agreement and exchange are vital to creating an equal partnership between the two players. In any case, it is crucial that they would follow their own codes of conduct without exceptions and would not compromise ethical standards. Ultimately, both entities are a part of society, and they aim to help and assist it. Finally, supporting INGOs could also contribute to a better public image of intelligence organisations.

To conclude, even if an operation fails and is disclosed, there are ways and PR tools that can help intelligence agencies to rescue their reputation. Indisputably, the most beneficial strategy is to follow strict ethical and legal guidelines, so that neither intelligence officers or policymaker nor society on no grounds could doubt the credibility of the intelligence work methods. Since taking advantage of INGOs raises a lot of issues, and the current trends suggest that no intelligence actions will stay disclosed forever, it would be advisable to avoid such controversial operations. However, in the circumstances, when exploiting INGOs is needed, extra measures to keep such action from the public eye must be taken to avoid damaging the reputation of the non-governmental sector.

## Conclusions

Even in certain circumstances, the interests of national intelligence agencies and INGOs overlap, these two entities significantly differ in their manners of action. While INGOs often choose open and transparent ways of operating, intelligence agencies are restricted to secrecy. In addition, INGOs enable their operations through the mandate of neutrality and impartiality while an intelligence community is serving one particular government on the grounds of national interest. Furthermore, the pressure from intelligence product consumers might lead intelligence agencies to more perilous or controversial work methods. Taking into account the challenges and complexity of intelligence work, it is unsurprising, that some operations unavoidably face moral, legal and other kinds of dilemmas that could not be resolved effortlessly. These issues are also manifested in the operations that take advantage of INGOs and use them as a cover for intelligence gathering, in false flag operations or covert action.

Regardless of the limitations created by the lack of knowledge about the particular circumstances of the intelligence operations, the three disclosed cases provided substantial grounds for this research. Therefore, the study has identified several important aspects of the relations between the national intelligence agencies and INGOs and the consequences it might inflict.

Internationally, the legal environment concerning intelligence activities is still developing. Nevertheless, there are laws (for instance, international human rights law or international



humanitarian law) that could potentially be breached during the intelligence operations that involve INGOs. While it is unlikely that any legal action could be taken against an intelligence agency, they should still look at those legislations due to possible influence on the reputation of intelligence. If the operational material is leaked or declassified, the image of intelligence might not suffer adverse consequences if the operations were conducted according to existing laws or at least do not involve grave breaches. Moreover, following existing laws could contribute to reducing unfavourable effects.

In addition, humanitarian law aims to protect organisations active in war zones. Therefore, it is essential to draw attention to the outcomes to INGOs while planning intelligence actions. Humanitarian organisations in conflict territories highly depend on their mandate of neutrality and impartiality; therefore, if such organisation is used in the intelligence operation, it could disrupt humanitarian work in those areas. Causing harmful effects to INGOs could also reduce public support for intelligence work.

From the ethical perspective, intelligence agencies should calculate possible effects for humanitarian workers and organisations as well. Defending this kind of operation in public could be challenging as it might not only carry severe consequences for INGOs and their reputation but also lead to further negative outcomes such as a health crisis, a ban of their activities or abduction and killings of humanitarians. The publication of these operations and the side effects they evoke could negatively affect the image of intelligence. The understanding of the key functioning principles of INGOs would allow the intelligence community to avoid causing damage to the humanitarian mandate.

In addition, the findings of this research also contribute to the argument that intelligence agencies need to develop a clear code of conduct. It would guide intelligence professionals in making well-researched decisions and could reduce the harmful effects of intelligence operations. The establishment of national or, where possible, regional intelligence codes of conduct that would recommend excluding humanitarian organisations from being used in operations, could prevent unpredictable ramifications.

The most significant risk of these operations come from the publicity. Disclosure of intelligence exploitation of INGO can affect the reputation of all the actors involved. While the reputation of intelligence could be restored, there also is a possibility for unexpected side

effects, as it happened with the CIA case and the Taliban's ban on vaccination. Intelligence agencies could take additional preventive measures to ensure that such cases would stay secret. However, with the recent trends, technological development and public demand for transparency, it is not possible to ensure that a case could be fully secure from the public eye. Hence, the practice of taking advantage of INGOs for intelligence needs is not recommended due to all the possible risks. Furthermore, illegal, controversial or morally unacceptable practice could evoke negative attitude inside the intelligence community and even encourage information leaks.

Moreover, intelligence legitimacy is a crucial factor in such operations. Secrecy is one of the reasons why society and intelligence have complicated relations. Society needs to grant legitimacy to perceived actions, and intelligence has to show accountability for their activities without disclosing the information. Hence, society will keep questioning the lawfulness and morality of the work methods that intelligence community chooses. And intelligence agencies will need to convince society that their methods are appropriate by revealing some operational material. Although intelligence is operating on the grounds of a public good, it is a subjective term. Therefore, taking advantage of vulnerable or imperfect parts of society is unfavourable, but sometimes the only practice that could prevent a grave threat. Nevertheless, society takes responsibility for drawing boundaries for intelligence actions. While in some instances public could approve using INGOs in intelligence operations, it remains a risky choice.

Finally, increasing awareness between policy-makers and society about the actual intelligence capabilities could help to reduce unrealistic expectations and could contribute to reducing pressure for intelligence agencies. It could also help to eliminate such practices as taking advantage of INGOs.

This thesis also proves that there is a need for further research in this area. Other, currently undisclosed intelligence operations, that involve INGOs might illuminate a variety of risks that were not discussed in this thesis. In addition, more investigation into this subject could lay a base for a better perception of the relations between these actors. For both, the INGOs and intelligence agencies, it could be beneficial to engage in a dialogue, explaining their needs and capabilities. It is possible that INGOs and intelligence agencies could find a way to support one another (especially in the zones of armed conflict) without compromising their mandates

and codes of conduct. However, INGOs should also be aware that they could be targeted and exploited by intelligence; therefore, taking precautions is crucial.

To summarise, this research identifies several potential risks that intelligence operations, taking advantage of INGOs might face. However, apart from the legal and moral issues and side effects, the significant threat comes from making information about such operations public. Therefore, intelligence agencies should only involve INGOs in their operations if all the other tools and recourses are exhausted. Intelligence organisations should also try to keep these cases undisclosed. If this kind of operation gets disclosed, intelligence could use plausible deniability strategy to reduce the damage done to the INGOs reputation or admit misconduct and provide more details to the public explaining why it was necessary to take such measures.

## References

Ackerman, S., Pilkington, E., 2015. Obama's war on whistle-blowers leaves administration insiders unscathed. *Guardian*, [online] 16 March. Available at:

<<https://www.theguardian.com/us-news/2015/mar/16/whistleblowers-double-standard-obama-david-petraeus-chelsea-manning>> [Accessed 8 April 2019]

Aljazeera, 2008. Betancourt rescued in Colombia. [online] 3 July. Available at:

<<http://www.aljazeera.com/news/americas/2008/07/20087222144816584.html>> [Accessed 28 November 2018]

Amnesty international, 2019. Global assault on NGOs reaches crisis point as new laws curb vital human rights work. [online] Available at:

<<https://www.amnesty.org/en/latest/news/2019/02/global-assault-on-ngos-reaches-crisis-point/>> [Accessed 25 Mar 2019]

Andregg, M.M., Gill, P., 2014. Comparing the Democratization of Intelligence. *Intelligence and National Security*, vol. 29, no. 4, pp. 487-497.

Bateman, A., 2016. The KGB and Its Enduring Legacy. *The Journal of Slavic Military Studies*, vol. 29, no. 1, pp. 23-47.

BBC, 2008. Betancourt rescuer wore Red Cross. [online] 17 July. Available at:

<<http://news.bbc.co.uk/1/hi/world/americas/7510423.stm>> [Accessed 25 Oct 2018]

Beim, J., 2018. Enforcing a Prohibition on International Espionage. *Chicago Journal of International Law*, vol. 18, no. 2, pp. 647-672.

Bellaby, R., 2012. What's the Harm? The Ethics of Intelligence Collection. *Intelligence and National Security*, vol. 27, no. 1, pp. 93-117.

Blackwood, A., Roeger, K., Pettijohn, S.L., 2012. The Nonprofit Sector in Brief: Public Charities, Giving and Volunteering, 2012. *Urban Institute*, [online] Available at:

<[https://www.urban.org/research/publication/nonprofit-sector-brief-public-charities-giving-and-volunteering-2012/view/full\\_report](https://www.urban.org/research/publication/nonprofit-sector-brief-public-charities-giving-and-volunteering-2012/view/full_report)> [Accessed 16 May 2019]

Breakspear, A., 2013. A New Definition of Intelligence. *Intelligence and National Security*, vol. 28, no. 5, pp. 678-693.

Brown, A., 2012. Osama Bin Laden's death: How it happened. *BBC News*, [online] 10 September. Available at: <<https://www.bbc.com/news/world-south-asia-13257330>> [Accessed 8 April 2019]

Browne, K.J., 2017. The paradox of peacetime espionage in international law: from state practice to first principles. *Australian International Law Journal*, vol. 23, pp. 106.

Buekens, M.P. et al., 2013. Public Letter to President Obama. *John Hopkins Bloomberg School of Public Health*, 6 January 2013 [online] Available at: <<https://www.jhsph.edu/news/news-releases/2013/Klag%20letter%20to%20President%20Obama.pdf>> [Accessed 17 May 2019]

Byman, D., 2001. Uncertain partners: NGOs and the military. *Survival*, vol. 43, no. 2, pp. 97-114.

Chesterman, S., 2013. One nation under surveillance: a new social contract to defend freedom without sacrificing liberty. Oxford University Press, Oxford.

Chiru, I., 2016. Engaging Public Support and Awareness in Intelligence: The Demands and Challenges to Developing an Intelligence Culture. *International Journal of Intelligence and Counterintelligence*, vol. 29, no. 3, pp. 503-514.

CIA, 1981. Executive order 12333. [online] Available at: <<https://www.cia.gov/about-cia/eo12333.html>> [Accessed 28 November 2018]

CIA, 2019. Library. [online] Available at: <<https://www.cia.gov/library>> [Accessed 8 April 2019]

Cole, M., 2015. The Pentagon's Missionary Spies. *The Intercept*, [online] 26 October. Available at: <<https://theintercept.com/2015/10/26/pentagon-missionary-spies-christian-ngo-front-for-north-korea-espionage/>> [Accessed 25 Feb 2019]

Collier, J., 2017. Getting Intelligence Agencies to Adapt to Life Out of the Shadows. *Council on Foreign Relations*, [blog] 05 April. Available at: <<https://www.cfr.org/blog/getting-intelligence-agencies-adapt-life-out-shadows>> [Accessed 28 May 2019]

Cormac, R., Aldrich, R.J., 2018. Grey is the new black: covert action and implausible deniability. *International Affairs*, vol. 94, no. 3, pp. 477-494.

Cozine, K., 2013. Teaching the Intelligence Process: The Killing of Bin Laden as a Case Study. *Journal of Strategic Security*, vol. 6, pp. 80-87.

Crisp, R., 2011. Ethics and metaethics. Ethics. *Routledge Encyclopedia of Philosophy*, Taylor and Francis, Routledge.

DeMars, W.E., 2001. Hazardous Partnership: NGOs and United States Intelligence in Small Wars. *International Journal of Intelligence and Counterintelligence*, vol. 14, no. 2, pp. 193-222.

DeMars, W.E., 2005. NGOs and transnational networks: wild cards in world politics. Pluto Press, London.

Diderichsen, A., Rønn, K.V., 2017. Intelligence by consent: on the inadequacy of Just War Theory as a framework for intelligence ethics. *Intelligence and National Security*, vol. 32, no. 4, pp. 479-493.

Elst, R., 2000. Implementing Universal Jurisdiction Over Grave Breaches of the Geneva Conventions. *Leiden Journal of International Law*, vol. 13, no. 4, pp. 815-854.

Erskine, T., 2004. 'As Rays of Light to the Human Soul'? Moral Agents and Intelligence Gathering. *Intelligence and National Security*, vol. 19, no. 2, pp. 359-381.

Fast, L.A., Freeman, C.F., O'Neill, M., Rowley, E., 2013. In acceptance we trust? Conceptualising acceptance as a viable approach to NGO security management. *Disasters*, vol. 37, no. 2, pp. 222-243.

Fleck, D., 2007. Individual and state responsibility for intelligence gathering. *Michigan Journal of International Law*, vol. 28, no. 3, pp. 687.

Forcese, C., 2011. Spies without borders: international law and intelligence collection. *Journal of National Security Law & Policy*, vol. 5, no. 1, pp. 179.

Freedom House, 2012. Factsheet: Russia's NGO Laws. [online] Available at: <[https://freedomhouse.org/sites/default/files/Fact%20Sheet\\_0.pdf](https://freedomhouse.org/sites/default/files/Fact%20Sheet_0.pdf)> [Accessed 28 May 2019]

Gambino, L., 2014. CIA will not use vaccination schemes for spying, says White House official. *The Guardian*, [online] 20 May. Available at: <<https://www.theguardian.com/world/2014/may/20/cia-vaccination-programmes-counterterrorism>> [Accessed 20 November 2018]

Garraway, C.H.B., 2007. State intelligence gathering: conflict of laws. *Michigan Journal of International Law*, vol. 28, no. 3, pp. 575.

Gendron, A., 2005. Just War, Just Intelligence: An Ethical Framework for Foreign Espionage. *International Journal of Intelligence and Counterintelligence*, vol.18, no. 3, pp. 398-434.

Gentry, J.A., 2016. Toward a Theory of Non-State Actors' Intelligence. *Intelligence and National Security*, vol. 31, no. 4, pp. 465-489.

Gert, B., Gert, J., 2016. The Definition of Morality. *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta (ed.), [online] Available at: <<https://plato.stanford.edu/archives/fall2017/entries/morality-definition/>> [Accessed 21 May 2019].

Gill, P., 2009. Security Intelligence and Human Rights: Illuminating the 'Heart of Darkness'? *Intelligence and National Security*, vol. 24, no. 1, pp.78-102.

Gill, P., 2012. Intelligence, Threat, Risk and the Challenge of Oversight. *Intelligence and National Security*, vol. 27, no. 2, pp. 206-222.

Giustozzi, A., 2008. Koran, Kalashnikov, and laptop: The Neo-Taliban insurgency in Afghanistan. Columbia University Press, New York, NY.

Graaff, B., 2016. Handbook of European intelligence cultures. Rowman & Littlefield Education, A division of Rowman & Littlefield Publishers, Inc. Lanham.

Gunn, S.W., 2012. Dictionary of Disaster Medicine and Humanitarian Relief, 2nd edn. Springer, London, New York.

Haver, K., Carter, W., 2016. What It Takes: Principled pragmatism to enable access and quality humanitarian aid in insecure environments. Report from the Secure Access in Volatile Environments research programme: SAVEResearch.net, *Humanitarian Outcomes*, November.

Heaven, A., Kornweiss, R. B., 2018. U.S. Charges Chinese and Taiwanese Companies with Trade Secret Theft, Continues Vigilant Prosecution of Chinese Economic Espionage. *Crowell & Moring's Trade Secrets Trends* [online] Available at: <  
<https://www.crowelltradesecretstrends.com/2018/11/u-s-charges-chinese-and-taiwanese-companies-with-trade-secret-theft-continues-vigilant-prosecution-of-chinese-economic-espionage/>> [Accessed 17 May 2019]

Herman, M., 2004. Ethics and Intelligence after September 2001. *Intelligence and National Security*, vol. 19, no. 2, pp. 342-358.

Hitz, F.P., 2005. The Myths and Current Reality of Espionage. *International Journal of Intelligence and Counterintelligence*, vol. 18, no. 4, pp. 730-733.



Hoelscher, K., Miklian, J., Nygård, H.M., 2017. Conflict, Peacekeeping, and Humanitarian Security: Understanding Violent Attacks Against Aid Workers. *International Peacekeeping*, vol. 24, no. 4, pp. 538-565.

Hood, R., Hoyle, C., 2008. The death penalty: a worldwide perspective. Oxford University Press, Oxford.

Hulnick, A.S., 1999. Openness: Being Public About Secret Intelligence. *International Journal of Intelligence and Counterintelligence*, vol. 12, no. 4, pp. 463-483.

Human Rights Watch, 2015. China's new foreign NGO law will help silence critics. [online] 13 April. Available at: <<https://www.hrw.org/news/2015/04/13/chinas-new-foreign-ngo-law-will-help-silence-critics>> [Accessed 25 May 2019]

ICRC, 1907. Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907, [online] Available at: <<https://ihl-databases.icrc.org/ihl/INTRO/195>> [Accessed 25 Mar 2019]

ICRC, 1949. Geneva Conventions of 1949 and Additional Protocols, and their Commentaries. [online] Available at: <<https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/INTRO/365?OpenDocument>> [Accessed 28 November 2018]

ICRC, 2004. What is IHL? [online] Available at: <[https://www.icrc.org/en/doc/assets/files/other/what\\_is\\_ihl.pdf](https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf)> [Accessed 28 November 2018]

ICRC, 2016. Fundamental Principles of the Red Cross and Red Crescent Movement. [online] Available at: <<https://www.icrc.org/en/document/fundamental-principles-red-cross-and-red-crescent>> [Accessed 30 Jan 2019].

ICRC, 2018. Annual Report 2017. [online] Available at: <<https://www.icrc.org/en/document/annual-report-2017>> [Accessed 29 Jan 2019].

Jackson, A., Aynte, A., 2013. Talking to the other side: Humanitarian negotiations with Al-Shabaab in Somalia. [online] Available at: <<https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/8744.pdf>> [Accessed 25 Mar 2019]

Jemberga, S., Salu, M., Černiauskas, Š., Pancerovas, D., 2015. Kremlin's Millions. Re:baltica [online] Available at: <<https://en.rebaltica.lv/2015/08/kremlins-millions/>> [Accessed 10 May 2019]

Johnson, A.R., 2018. Managing Media Influence Operations: Lessons from Radio Free Europe/Radio Liberty. *International Journal of Intelligence and Counterintelligence*, vol. 31, no. 4, pp. 681-701.

Johnston, P., 2006. MI6 licensed to thrill listeners to Radio 1. *The Telegraph* [online] 16 November. Available at: <<https://www.telegraph.co.uk/news/uknews/1534306/MI6-licensed-to-thrill-listeners-to-Radio-1.html>> [Accessed 8 April 2019]

Klimas, J., 2017. Why North Korea is a black hole for American spies. *Politico* [online] 8 September. Available at: <<https://www.politico.com/story/2017/09/08/why-north-korea-is-a-black-hole-for-spies-242473>> [Accessed 28 November 2018]

Krause, M., 2014. The good project: humanitarian relief NGOs and the fragmentation of reason. The University of Chicago Press, Chicago.

Laipson, E.B., 2005. Can the USG and NGOs Do More: Information-Sharing in Conflict Zones. Vol. 49, No. 4 [online] Available at: <[https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no4/USG\\_NGOs\\_5.htm](https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no4/USG_NGOs_5.htm)> [Accessed 29 Jan 2019].

Lefebvre, S., 2019. What do judges say on the protection of intelligence secrets? *Intelligence and National Security*, vol. 34, no. 1, pp. 62-77.

MacLeod, D.T., 2009. Leveraging Academia to Improve NGO Driven Intelligence. *Journal of Conflict Studies*, vol. 29, no. 1, pp. 107-120.

Magen, C., 2018. Israel's intelligence services and the media: four decades of a complex tango. *Israel Affairs*, vol. 24, no. 5, pp. 799-818.

Magen, C., Gilboa, E., 2014. Communicating from Within the Shadows: The Israel Security Agency and the Media. *International Journal of Intelligence and Counterintelligence*, vol. 27, no. 3, pp. 485-508.

Manget, F.F., 2007. Another System of Oversight: Intelligence and the Rise of Judicial Intervention. [online] Available at: <<https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol39no5/html/v39i5a06p.htm>> [Accessed 28 November 2018]

Matei, F.C., 2014. The Media's Role in Intelligence Democratization. *International Journal of Intelligence and Counterintelligence*, vol. 27, no. 1, pp. 73-108.

Mazanec, B.M., 2015. The Evolution of Cyber War: International Norms for Emerging-Technology Weapons. Potomac Books, Lincoln, NE. Available from: ProQuest Ebook Central

McCrisken, T., Moran, C.R., 2018. James Bond, Ian Fleming and intelligence: breaking down the boundary between the 'real' and the 'imagined'. *Intelligence and National Security*, vol. 33, no. 6, pp. 804-18.

McDermott, J., 2008. Ingrid Betancourt hails Colombian military rescue operation. *The Telegraph*, [online] 3 July. Available at: <<http://www.telegraph.co.uk/news/worldnews/southamerica/colombia/2239227/Ingrid-Betancourt-hails-Columbian-military-rescue-operation.html>> [Accessed 12 June 2019]

Moran, C.R., 2013. The Last Assignment: David Atlee Phillips and the Birth of CIA Public Relations. *The International History Review*, vol. 35, no. 2, pp. 337-355.

MSF, 2019. Who we are. [online] Available at: <<https://www.msf.org/who-we-are>> [Accessed 29 Jan 2019].

Naim, M., 2007. What is a gongo? How government-sponsored groups masquerade as civil society. *Foreign Policy*, no. 160, pp. 96.

Nature, 2011. Don't blame the CIA. [online] Available at:  
<<https://www.nature.com/articles/475265a>> [Accessed 28 November 2018]

NGO Monitor, 2016. Implications of NGO Espionage for European Funders. [online] Available at: < <https://www.ngo-monitor.org/press-releases/implications-of-ngo-espionage-for-european-funders/>> [Accessed 25 Mar 2019]

Norwood, R., 2002. None dare call it treason: the constitutionality of the death penalty for peacetime espionage. *Cornell Law Review*, vol. 87, no. 3, pp. 820.

Office of the Director of National Intelligence, 2017. Worldwide Threat Assessment of the US Intelligence Community. [online] Available at:  
<<https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SF%20-%20Final.pdf>> [Accessed 8 April 2019]

Olson, J.M., 2006. Fair Play: The Moral Dilemmas of Spying. Washington, DC: Potomac Books.

Omand, D., 2010. Securing the state. Oxford University Press, Inc, New York, New York.

Omand, D., Phythian, M., 2013. Ethics and Intelligence: A Debate. *International Journal of Intelligence and Counterintelligence*, vol. 26, no. 1, pp. 38-63.

Parliamentary Assembly, 2005. [online] Available at:  
<<http://www.assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17360>>  
[Accessed 8 April 2019]

Perry, D., 2009. Partly Cloudy: Ethics in War, Espionage, Covert Action and Interrogation. Lanham, Md., Scarecrow Press.

Petersen, K.L., 2019. Three concepts of intelligence communication: awareness, advice or co-production? *Intelligence and National Security*, vol. 34, no. 3, pp. 317-328.

Pfaff, T., Tiel, J.R., 2004. The ethics of espionage. *Journal of Military Ethics*, vol. 3, no. 1, pp. 1-15.

Phillips, N.J., 2016. "We're the ones that stand up and tell you the truth": Necessity of ethical intelligence services. *Salus Journal*, vol. 4, no. 2, pp. 47-61.

Phythian, M., 2007. The British experience with intelligence accountability. *Intelligence and National Security*, vol. 22, no. 1, pp. 75-99.

Phythian, M., 2018. Intelligence Failure as a Mutually Reinforcing Politico-Intelligence Dynamic: The Chilcot Report and the Nature of the Iraq WMD Intelligence Failure. *British Yearbook of International Law*.

Privacy International, 2018. UK mass interception law violates human rights - but the fight against mass surveillance continues. [online] Available at:  
<<https://privacyinternational.org/feature/2267/uk-mass-interception-law-violates-human-rights-fight-against-mass-surveillance>> [Accessed 25 Mar 2019]

Pun, D., 2017. Rethinking espionage in the modern era. *Chicago Journal of International Law*, vol. 18, no. 1, pp. 353-391.

Richelson, J.T., 2012. Intelligence Secrets and Unauthorized Disclosures: Confronting Some Fundamental Issues. *International Journal of Intelligence and Counterintelligence*, vol. 25, no. 4, pp. 639-677.

Ripley, W., 2017. North Korean Official: Take Hydrogen Bomb Threat 'Literally'. *CNN*, [online] 26 October. Available at: <<http://edition.cnn.com/2017/10/25/politics/north-korea-us-hydrogen-bomb-threat/index.html>> [Accessed 28 November 2018]

Schneiker, A., 2015. Humanitarian NGO Security Networks and Organisational Learning: Identity Matters and Matters of Identity. *Voluntas: International Journal of Voluntary and Nonprofit Organizations*, vol. 26, no. 1, pp. 144-170.

Scott, L. 2004. Secret Intelligence, Covert Action and Clandestine Diplomacy. *Intelligence and National Security*, vol. 19, no. 2, pp. 322-341.

Security Service, 2019. MI5 - The Authorised Centenary History. [online] Available at: <<https://www.mi5.gov.uk/mi5-the-authorised-centenary-history>> [Accessed 30 May 2019]

Sepper, E., 2010. Democracy, human rights, and intelligence sharing. *Texas International Law Journal*, vol. 46, no. 1, pp. 151.

Shaw, W.H., 2014. Consequentialism, War, And National Defense. *Journal of International Political Theory*, vol. 10, no. 1, pp. 20-37.

SIS, 2019. Media Enquiries. [online] Available at: <<https://www.sis.gov.uk/contact-us-advice.html>> [Accessed 8 April 2019]

Snider, B.L., 2008. The agency and the hill: CIA's Relationship with Congress, 1946-4004. Center for the Study of Intelligence Central Intelligence Agency, Washington, DC 20505.

Sulmasy, G., Yoo, J.C., 2007. Counterintuitive: intelligence operations and international law. *Michigan Journal of International Law*, vol. 28, no. 3, pp. 625.

Taormina, R.J., Gao, J.H., 2013. Maslow and the Motivation Hierarchy: Measuring Satisfaction of the Needs. *The American Journal of Psychology*, vol. 126, no. 2, pp. 155-177.

The Times of India, 2014. Foreign-funded NGOs stalling development: IB report. [online] 12 June. Available at: <<https://timesofindia.indiatimes.com/india/Foreign-funded-NGOs-stalling-development-IB-report/articleshow/36411169.cms>> [Accessed 25 Oct 2018]

The Times of Israel, 2019. AG rejects right-wing appeal against Breaking the Silence. [online] Available at: <https://www.timesofisrael.com/ag-rejects-right-wing-appeal-against-breaking-the-silence/> [Accessed 25 Oct 2018]

Thompson, R., 1966. Defeating Communist insurgency: experiences from Malaya and Vietnam. Chatto & Windus, London.

Twitter, 2019. CIA. [online] Available at: <https://twitter.com/CIA> [Accessed 8 April 2019]

Ukman, J., 2011. CIA defends running vaccine program to find bin Laden. *The Washington Post*, [online] 13 July. Available at: [https://www.washingtonpost.com/world/national-security/cia-defends-running-vaccine-program-to-find-bin-laden/2011/07/13/gIQAbLcFDI\\_story.html?utm\\_term=.c18d674a0da3](https://www.washingtonpost.com/world/national-security/cia-defends-running-vaccine-program-to-find-bin-laden/2011/07/13/gIQAbLcFDI_story.html?utm_term=.c18d674a0da3) [Accessed 10 June 2019]

UN, 1945. U.N. Charter. [online] Available at: <http://www.un.org/en/sections/un-charter/chapter-i/index.html> [Accessed 28 November 2018]

Van Daele, D., 2016. Belgium: A Modern Legal and Policy Framework for Intelligence Service with a Long Tradition. In: Graaff, B.d. & Dawson Books, *Handbook of European intelligence cultures*, Rowman & Littlefield Education, Inc, Lanham.

Walsh, D., McNeil D.G., 2012. Gunmen in Pakistan Kill Women Who Were Giving Children Polio Vaccines. *The New York Times*, [online] 18 December. Available at: [http://www.nytimes.com/2012/12/19/world/asia/attackers-in-pakistan-kill-anti-polio-workers.html?\\_r=0&mtrref=www.healthmap.org&gwh=0EE80F57FBC087413C711965B54E6E69&gwt=pay](http://www.nytimes.com/2012/12/19/world/asia/attackers-in-pakistan-kill-anti-polio-workers.html?_r=0&mtrref=www.healthmap.org&gwh=0EE80F57FBC087413C711965B54E6E69&gwt=pay) [Accessed 12 June 2019]

Walsh, P.F., Miller, S., 2016. Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden. *Intelligence and National Security*, vol. 31, no. 3, pp. 345-368.

Warner, M., 2012. Fragile and Provocative: Notes on Secrecy and Intelligence. *Intelligence and National Security*, vol. 27, no. 2, pp. 223-240.

Wierzbicki, A., 2018. *Web Content Credibility*. Springer International Publishing, Cham.

Williamson, J.A., 2011. Using humanitarian aid to 'win hearts and minds': a costly failure? *International Review of the Red Cross*, vol. 93, no. 884, pp. 1035-1061.

Wippl, J.W., 2016. Observations on Successful Espionage. *International Journal of Intelligence and Counterintelligence*, 29:3, pp. 585-596.

Wired, 2019. Former CIA Chief of Disguise Breaks Down 30 Spy Scenes from Film & TV. *WIRED*, [video online] Available at: <<https://www.youtube.com/watch?v=mUqeBMP8nEg>> [Accessed 21 May 2019]