The Terror of Counterterrorism

On the Restriction of the Right to Privacy in the Age of Security

Universiteit Leiden

Author: Liseth Aling
S1080040
Leiden University
Master Thesis

08-06-2015
Supervisor: Theresa Reinold
Second reader: Daniel Thomas

Abstract

After the attacks on the United States on September 11th 2001 security regimes all around the world were intensified in order to cope with the threat of international terrorism. As a result, compliance with human rights obligations was strained in certain states because of the new security measures. This thesis aims to contribute to existing literature regarding counterterrorism and human rights by investigating the effects of counterterrorism measures on the right to privacy. More specifically, it studies the counterterrorism framework of Denmark, the Netherlands and Great Britain in light of these states' different threat perceptions. The expectation is that a low level of threat perception results in non-restrictive measures, leaving the right to privacy intact, whereas a high level of threat perception results in more invasive measures that restrict the right to privacy of the state's citizens. The results only partly confirm this hypothesis. Great Britain's high threat perceptions have led to restrictive measures, and the Dutch low threat perception has led to relatively non-restrictive measures. However, Denmark also showed a relatively low threat perception, but has implemented fairly restrictive counterterrorism measures. This variation is attributed partly to different levels of securitization and to the varying characteristics of each state's collective memory regarding acts of terrorism.

Table of Contents

1. Introduction

After the 9/11 attacks on the United States and the following fight against terrorism initiated by the Bush administration, security measures were tightened all around the world (Murphy, 2012: 3). New counterterrorism policies aimed at constraining the movements of terrorists and other radical individuals were instigated in order to secure the populations of the Western countries that were perceived to be at the highest risk. This thesis sets out to investigate how these counterterrorism measures affected the fundamental human right to privacy in Denmark, Great Britain and the Netherlands.

This topic has become all the more relevant after the terrorist attacks on Charlie Hebdo in Paris on January 7th and the Copenhagen shooting on February 14th of this year. Both events triggered hot debates throughout Europe about the most effective ways to fight global terrorism and the possible consequences of these measures. In addition, the balance between basic human rights and freedoms such as the freedom of expression and the freedom of religion was put in the spotlight, even though it was already widely acknowledged that these so-called absolute rights can be a source of controversy. The recent events in world politics have strained the balance that was formerly largely maintained between seemingly incompatible rights. In light of this imbalance between fundamental rights, it is necessary to look at the way that Western democracies handle the balance between the individual right to privacy and the collective good of security.

Many studies, both quantitative and qualitative, have explored the balance between justice and security and the effects of security considerations on human rights (Gibson, 1998; Hudson and Ugelvik, 2012). This thesis will build on this body of literature by focusing specifically on one fundamental right and by investigating the link between counterterrorism measures and human rights effects. Also, many studies regarding the effects of counterterrorism measures on human rights and civil liberties are conducted in the United States (for example Davis and Silver, 2004), while European countries like the Netherlands, Great Britain and Denmark remain understudied, despite the relatively high terrorist risk in these countries. Van Leeuwen (2003) offered a comprehensive study of nine European states and their experience with terrorism and their resulting policies. However, in the meantime many events related to terrorism have taken place, especially in Europe, so the findings may no longer be completely up-to-date. This thesis aims to contribute to the existing literature on experiences with terrorism, threat perceptions and resulting counterterrorism measures by analyzing more recent events and states' consequent responses.

The objective of this thesis is thus to explore the effects of counterterrorism measures on the fundamental right to privacy in Denmark, Great Britain and the Netherlands. The choice of these cases was based on a number of factors, but the main reason is that these states show a variance in the severity of terrorism that they experienced, leading to varying threat perceptions. The Netherlands and Denmark have, without taking into account the most recent terrorist shooting in Copenhagen, so far not been subject to a serious terrorist attack that resulted in a large number of civilian casualties. The Copenhagen shooting is excluded from the analysis because it happened so recently and it therefore cannot be expected to have resulted in any concrete measures yet. As for Great Britain, on July 7 2005 a series of coordinated suicide bombings targeted at the city's public transport network during rush hour resulted in 52 deaths and left almost 1000 people injured (Cobain, 2010). In addition, Great Britain struggled with terrorism related to the Northern Ireland conflict for a long time, with the Irish Republican Army as the main source of threat (Ilardi, 2009). By analyzing these states that endured different levels of terrorism and will thus have different threat perceptions, this thesis aims to sketch a clear picture of the nature of counterterrorism measures that have been taken and their effects on the right to privacy in these three countries.

The findings of this thesis suggest that that in two of the three cases the level of threat perception resulted in responses that were expected: Great Britain's high threat perception resulted in relatively restrictive measures, whereas the Dutch lower threat perception consequently resulted in a lower level of restrictiveness. Denmark, however, does not conform to the expectations, as the country also maintained a fairly low threat perception but did to a certain extent implement somewhat to very restrictive measures. The explanations regarding this phenomenon that are brought forward in the discussion revolve around the nature of society's collective memory and varying levels of securitization.

This thesis will commence with an outline of relevant theories and concepts, after which two hypotheses will be presented. It will then go on to outline the data and methods that are used in this thesis, followed by an explanation of the choice of cases. Then, the operationalization of the variables 'threat perception', 'counterterrorism measures' and 'right to privacy' will follow. The next chapters will then consist of an outline of European Union and United Nations measures, as these have been highly influential for all three states. The three case studies will then be presented, followed by an analysis and discussion of the results. The final chapter consists of a brief conclusion.

2. Theoretical Framework and Hypotheses

Discussions regarding security and justice are great in number, and there are many sides to it. There are those who perceive justice and security as two values that have to be in balance with each other, meaning that as one is enhanced the other will decrease. On the other hand there are authors who argue that this image of security and justice being two sides of a scale is misleading, and that these two social goods must be reconciled rather than balanced. This section will briefly outline the two sides of this debate, concluding that in the current era states are charged with the task of eliminating fear in addition to protecting its citizens from actual harm. Following this notion, this section will introduce a number of theories and paradigms that help explain why states are increasingly invasive in their attempts to enhance the security of their populations. Lastly, a discussion on threat perception and their causes is included as this concept is closely related to the theories and paradigms of this section, and can thus provide useful insights into the investigation of the effects of counterterrorism measures on the right to privacy.

First it is important to outline what exactly security is. Unfortunately there is no unified answer to this question, but a number of interpretations of security exist. There is the interpretation of security as a necessary condition for freedom: only when people live in a secure world can they exercise their rights and liberties (Mitsilegas, 2012). This idea dates back to the first liberal thinkers, notably John Locke, who visualized the state as an entity that could only exist if its constituents gave their express consent to give up some of their freedom in return for security provided by the state. If security could not be provided, the existence of the state would be superfluous as its sole purpose is to protect the life, liberty and property of its citizens (Locke, 1960). The provision of security is thus the foundation of the legitimacy of the state. In this line of thinking security is the first social good that needs to be in place for a society to perpetuate itself.

The classical interpretation of the right to security is that of a negative right to be free from interference of the state (Lazarus, 2007: 333). In this sense the right to security is a safeguard to intrusive state behavior and is supposed to protect the citizens' personal integrity and property. When interpreted in this way, the right to security is relatively "easy" for the state to comply with because it merely calls for non-interfering state behavior rather than for positive duties. But despite the relative clarity of this classical understanding of the right to security and the restraints it places upon state behavior, modern society increasingly calls for a more active interpretation of this right (Lazarus, 2007). However, when moved beyond this basic interpretation of the right to security, it becomes a little more vague.

The obvious counterpart of a negative right to security is a positive right to security, which calls for a proactive attitude of the state to protect its citizens from harm in addition to refraining it from interfering (Fredman, 2007). In fact, the interpretation of the right to security of person as a positive right is mostly invoked nowadays (Buhelt, 2012). This means that the state is viewed to be responsible for the well being of its citizens and for the absence of harm to the end that citizens can enjoy life in freedom, insofar as this can be achieved through human agency (Fredman, 2007: 308). This argument can then be taken a step further by arguing that in addition to the freedom of actual harm, to be free from fear of harm constitutes the same right, as a life lived in fear cannot be claimed to be a life lived in freedom. The state then becomes the prime actor responsible for the absence of fear of bodily harm and the assurance that people can fulfill their human potential (Fredman, 2007).

The assurance to be free from fear and the additional responsibilities that this notion bestows upon the state is an important aspect in the debate regarding human rights and security, as it incorporates a whole new set of measures and assurances into the body of security measures. To be free from violence is one thing, but to be free from fear of violence is an entirely different thing, as the latter involves subjective feelings of insecurity and vulnerability that differ per person. The agents that are responsible for eliminating feelings of fear thus have to tackle a whole array of fears and vulnerabilities. This makes the threat of terrorism rather abstract and unclear, as not only actual threats should be discerned, but also less concrete sources of fear. Baumann (2006) has dubbed this unspecified kind of fear 'liquid fear', as it has no clear cause or ground. According to Buhelt (2012: 188), this type of fear is what drives most democracies of the current age, as state agents are charged with the task to eliminate perceptions of insecurity and anxiety that are scattered and lack a clear source.

This focus on fears and vulnerabilities was elaborately mapped out by Beck (1992). According to Beck, modernity has produced 'risk societies'. These are societies in which there is a pervasive awareness of risks surrounding human life, as the social production of wealth is increasingly accompanied by the social production of risks (1992: 19). This mechanism is distinctly a product of modernity, as modern wealth is more or less evenly distributed in modern states. This wealth, especially technological wealth, produces risks as a side effect, resulting in a focus on the negative sides of contemporary societies rather than on the benefits. A clear example is that of modern industry: in earlier periods the word 'industry' invoked images of more employment, greater opportunities and inventions and overall increased wealth. Nowadays 'industry' is often used in relation to environmental degradation, pollution and bad working

conditions (Hudson, 2003: 43). In short, "in the risk society the unknown and unintended consequences come to be a dominant force in history and society" (Beck, 1992: 22).

A key aspect of modernity, which finds its roots in the Enlightenment, is the fact that modern society has the ability to reflect upon itself, causing a focus on the problems that arise from this modern society. As a result of this reflexivity, there is a widespread expectation that the recognized problems will be countered. In short, citizens of modern societies expect total safety and security from the risks that are distinguished from the production of technological wealth (Hudson, 2003). However, the problem with risks is that they are mostly imperceptible, as most risks will cause harm not today but in the future. As a result, the general public is dependent on scientists and politicians, as they possess the knowledge about these risks (Beck, 1992). This emphasizes the important role of knowledge in society, and it puts the people who have the expert knowledge in the position of having to anticipate every risk. The expectation that experts can prevent any possible harm by using their knowledge to anticipate risks is of course impossible to be met, but its consequences are widespread.

One such consequence of the expectation that all risks are eliminated and that the state is responsible for removing fear and insecurities as well as actual threats is what Mitsilegas calls the 'individualization of security' (2012). According to Mitsilegas, there has been a growing tendency within governments to place the individual at the heart of security considerations, thus focusing policy and legislation around the security of one individual or group of individuals rather than the collective security of the state as a whole. This focus on individual security is supposed to ensure freedom from fear and decrease perceived insecurities. Because of this individualization of security the focus of the balance of power between the state and the individual transforms into a focus of the balance of power between the individual and other (more dangerous) individuals (Mitsilegas, 2012: 200). This leads to the notion that people no longer need to be protected from the state but instead need to be protected from other individuals who pose a threat to their personal security. There is thus a shift in the interpretation of the right to security.

A result of the individualization of security is that enhanced state powers are justified because they are in place to protect citizens from other dangerous individuals (Mitsilegas, 2012). What is so interesting about this reinterpretation of the right to security is that the state, which this right originally served to constrain in its interference with citizens, is now endowed with more legitimacy in meddling with its citizens' lives, all in the name of security. Moreover, when placing human security in the

heart of the security debate, preventive security becomes increasingly important. This leads to an increasing importance of risk assessments as a tool for the state, as it has to monitor and map the risks that some individuals pose in order to eliminate a possible security threat, as will be outlined below. As a consequence, an increasing restriction of fundamental rights takes place as the state constantly seeks to prevent security threats from occurring and to eliminate individual feelings of insecurity (Mitsilegas, 2012).

In line with the individualization of security and the effect that it has on fundamental human rights is the notion of pre-crime as theorized by Lucia Zedner (2007). In a society where pre-crime is the rule, just as with the individualization of security, the state seeks to eliminate every possible risk that could cause harm to its citizens. As was seen above, this focus on risks is a product of the modern society and citizens expect knowledge experts to eradicate all risks. In this pre-crime society, radical prevention plays a large role in security considerations (Zedner, 2007: 260). This notion is different from "normal" prevention in that it focuses on a remote threat whose occurrence is uncertain at best. As a result, civil liberties and human rights are often curtailed in an attempt to effectively prevent security threats. Since 9/11 and the Madrid and London bombings in 2004 and 2005 there has been a growing tendency by national governments to base their security considerations on the logic of pre-crime (Zedner, 2007: 260). This focus leads state and security agents to criminalize preparatory acts that could materialize into a threatening situation in the future but whose tangible effects are uncertain.

This evolution of societies with a pre-crime-based security regime has given rise to what is called the precautionary principle (PP) in criminal law (Lomell, 2012: 93). Originally developed in environmental studies, this principle holds that when there is a threat of serious and irreversible harm, the state has the responsibility to act upon this threat and try to prevent it, even when hard evidence about certainty of this event is lacking. The basic assumption of the PP is that human beings, society and nature are inherently vulnerable. As a result, insecurity has to be engaged in a proactive manner in order eliminate all the risks that threaten the vulnerabilities (Arnoldussen, 2009). In addition to an assumption of vulnerability, there is an assumption of uncertainty inherent to the PP. According to PP proponents, we have reached the limit of scientific knowledge. Therefore we have to find a way to accommodate this lack of scientific data so that human and natural vulnerabilities are still protected. Whereas science used to have all the answers and could come up with solid predictions of what was most likely to happen in the future, this role of science as arbiter has largely fallen away. The PP contains room for the prevention of risks that are not supported by scientific data and

are therefore unforeseen, suspected or feared. According to Lomell (2012), many counterterrorism measures fit this precautionary principle, as they are often intrusive and aim to prevent a threat that is uncertain but feared and based on unclear evidence (2012: 94)

The assumption of vulnerability that is inherent to all human life is also found in the paradigm of the vulnerability-led policy response (Furedi, 2008). According to Furedi (2008), most governments in the post 9/11 era base their security measures on a sense of vulnerability rather than resilience. This is mainly due to the enormous technological advances that have been developed over the last two decades or so. Instead of viewing the technological capabilities and networks of cooperation that exist nowadays as a source of strength, governments stress the vulnerability that it leads to, as any technological power can be used as a weapon against the state when in the wrong hands. Dangerous individuals, such as terrorists, are then viewed to become more and more powerful as the state's technological capabilities increase. As a result, counterterrorism measures are increasingly based on risk-aversion and the elimination of any vulnerability that exists within the state. This leads to an increased perception of fear and insecurity. Consequently, policy response is based on the elimination of this sense of vulnerability and revolves around worst-case scenarios as opposed to scenarios that are most likely to happen (Furedi, 2008).

What all the abovementioned paradigms and theories have in common is that a risk-based approach is nowadays most common in security considerations and that security measures are supposed to ensure freedom from fear and eliminate perceptions of insecurity rather than actual threats, resulting in mostly preventive measures. In addition, the state is seen to carry the main responsibility to protect individuals, and it is increasingly endowed with more and farther-reaching powers that are justified in the name of security. As a result of these stretching powers, and the restrictive effect they can have on civil liberties and human rights, the debate regarding security and human rights has increasingly been centered around the idea that security and justice exist in some kind of balance and that this balance can shift from one side to the other, depending on the needs of society.

When arguing in favor of rhetoric depicting the relation between justice and security as a balance that must be sought and maintained, it is important to first distinguish between first-tier rights, such as a the right to life, and second- and third-tier rights, such as the right to privacy. First-tier rights are those rights that are seen as absolutely fundamental for every human being and inalienable under any circumstance. On the other hand, second-tier and third-tier rights might be restricted if a strong case

can be made that restriction is absolutely necessary and proportional (Hudson, 2012: 17). According to this view, rights can be ranked and, according to their relative importance, suspended in times of exceptional need.

The question that arises then is what exactly constitutes an exceptional situation. According to Buzan et al. (1998), a security issue becomes exceptional when an authoritative person, usually a state official, uses the word "security", thereby invoking a situation of exceptional threat. When this happens, and this particular security issue gets prioritized on the public and political agenda, the state gets to take security measures that would not be acceptable in a "normal" situation. Buzan et al. call this process 'securitization' (1998). Securitization is thus a means for justifying extreme security measures. There is no objective measure as to what constitutes an exceptional security threat and what does not; only practice can tell which particular issue is securitized. A prime example of securitization is George W. Bush's rhetoric on the 'War on Terror': by invoking images of war, extreme measures that operated in the name of security were more or less justified. This theory is especially important in the debate whether justice and security constitute a balance, because the securitization of an issue would shift the balance in favor of security and away from the protection of human rights.

As a matter of fact, this debate takes place in a situation where rhetoric increasingly focuses on an exceptional situation (Bigo and Guild, 2007). According to Bigo and Guild (2007: 108), this tendency actually produces an insecurization of the world, as state leaders have an incentive to uphold a feeling of fear and vulnerability among the public and can so legitimately implement extreme security measures. So instead of going back to a "normal" situation after a state of emergency or exception, security rhetoric continues to conjure up perceptions of an exceptional threat, leading to greater feelings of insecurity and thus greater acceptance of invasive measures.

This focus on discourse and the interests of decision-makers in maintaining the picture of an exceptional threat is also highly relevant in the discussion of threat perceptions and their underlying causes. As many of the paradigms presented above focus on the elimination of fear and subjective feelings of threat, it is important to distinguish how threat perceptions arise and what their influence on threat responses can be. According to Gross Stein (2013) there are a number of variables that influence the concept of threat perception. Even though her categorization is focused on threat perceptions in international relations, some of the variables she presents are also relevant for the topic at hand.

The first variable revolves around the institutional interests of political actors. The political structure may be such that certain actors benefit from a high or low level of perceived threat by the public and who thus engage in rhetoric that suggests that this high or low threat level is indeed present. The second variable in this category is socio-cultural. It focuses on the domestic society and national identities that strongly influence a state's decision-makers' threat perceptions (Gross Stein, 2013: 7). This influence can be so strong that objective threat levels are entirely discarded and the threats that are perceived are in fact not present. This variable is mostly present in states that adhere to hypernationalism and militarism, and who consequently tend to think in terms of worst-case scenarios (Gross Stein, 2013: 7). The third factor is based on norm-breaking behavior of the threat sender. This means that if the actor or actors that pose the threat break some widely accepted norm, threat perceptions of those under threat increase (Gross Stein, 2013: 8).

However, threat perceptions are formed based on the attitudes of not only decision-makers but also of the public and of experts. In addition, the media play an important role in sketching and forming the general perception of threat by reporting on certain salient issues and neglecting others. These actors thus form an interplay that influences the level and nature of the threat that is perceived and consequently the response to this threat as well. If the public, for instance, does not perceive any threat whatsoever, the government is not likely to impose restrictive policies that are to counter a threat, and vice versa. The different perceptions of threat held by different groups of people, most notably the public, experts and political actors, determine for a large part the overall threat perception of a certain country due to the specific interaction between these groups.

What can be derived from the above is the fact that threat perceptions are dynamic and not easily established in a uniform manner. In addition, discourse that is presented by one group of actors can greatly influence the threat perceptions of another group of actors. Meyer (2009) offers a constructivist framework that effectively captures those factors that are relevant in answering the research question of this thesis. According to Meyer (2009), the prime factor that influences the threat perception of a state is previous experience with terrorism. If a state has encountered large-scale terrorism in its past, it is likely to maintain higher threat perceptions in the future. On the other hand, if a state has never experienced any major acts of terrorism, it is likely to maintain a low threat perception. These latter states, however, are likely to displays a steep increase in threat perception when a terrorist attack takes place, whereas the former generally shows a more stable level of threat perceptions (Meyer, 2009).

In addition to previous experience with terrorism, another factor that might influence the threat perception of a state is its attachment or alliance with the U.S. This is especially relevant in the case of Islamist terrorism after 9/11. A strong attachment to the U.S. generally results in a higher threat perception (Meyer, 2009: 660). Attachment in this sense can mean military alliance, but also shared cultural characteristics. This factor is in line with the last factor that is expected to influence threat perceptions, namely the type of foreign policy that a country pursues. If a state pursues a proactive foreign policy in that it tends to intervene in conflicts and strongly engage in international relations, threat perceptions tend to be higher as well (Meyer, 2009: 664).

The above paradigms, ideas and theories point to a number of overarching characteristics of the relation between security and human rights. First, the right to security can be interpreted on different levels, ranging from the negative duty of the state not to interfere with its citizens to the positive duty to protect every individual from harm and fear. The level of interpretation that is assumed is of great importance in discussing the impact of counterterrorism measures on the right to privacy, as it establishes the duties of the state and thus how far the state may go in safeguarding security. If the notion that all citizens should be protected from harm and fear is assumed, then more far-reaching measures are justified in order to achieve this goal. Nowadays, this seems to be the generally accepted viewpoint (Buhelt, 2012).

Second, a key variable in the above paradigms and theories is that of threat perception. The authors discussed above all point to the importance of the perceived level of (in)security of the state and the government's reaction to this perception. It therefore seems that a driving factor behind policy-making in the sphere of security is threat perception. This means that a state's threat perception has to be taken into account when analyzing the nature of counterterrorism measures. Seeing as counterterrorism measures have become increasingly invasive of human rights since 9/11, it can be expected that high threat perceptions lead to invasive measures. This can be summed up in the following causal chain:

Level of threat perception → invasiveness of counterterrorism measures → degree of restriction on right to privacy

Based on this causal chain, a number of hypotheses as regards the results of this research can be formulated. First, regarding the establishment of threat perceptions, three hypotheses can be distinguished:

1. Previous experience with terrorism leads to high threat perceptions.
2. Strong attachments to the U.S. lead to high threat perceptions.
3. Proactive foreign policy leads to high threat perceptions.

As regards the consequences in terms of counterterrorism measures the following hypotheses can be formulated:

1. A high level of threat perception is likely to result in more invasive counterterrorism measures, whereas a low level of threat perception will result in less invasive measures.
2. Invasive counterterrorism measures are expected to restrict the right to privacy to a greater extent than less invasive counterterrorism measures.

The case studies will each outline the level of threat perception, followed by the counterterrorism measures that were implemented and their level of restrictiveness. This will allow for a close analysis as regards threat perceptions and their influence on the nature of counterterrorism measures. The next chapter will present a brief outline of the data and method used in this research.

3. Data and Methods

In order to investigate the abovementioned hypotheses, this thesis will rely on a number of different types of data. As was seen above, this thesis aims to investigate the influence of counterterrorism measures on the right to privacy in Denmark, Great Britain and the Netherlands as a result of each state's threat perceptions. The data that are used therefore need to reflect the level of threat perception, the specific counterterrorism policies and legislation that are present in these countries, and effects on the right to privacy. This thesis therefore bases its analysis on both primary and secondary data in order to paint as complete a picture as possible.

First, in order to gauge counterterrorism measures, this thesis will make us of the national counterterrorism strategies, which can be found through the websites of the states' governments. In addition, it will briefly sum up United Nations resolutions and European Union legislation, as well as these institutions' counterterrorism strategies. Since these documents have greatly influenced national policies and legislation it is important that they too are outlined. They can also be found through the websites of these institutions. As for national counterterrorism efforts, country-specific legislation is also sketched, as this gives a clear view of the powers and checks of the

national security and intelligence services in relation to the fight against terrorism. These documents are found through the websites of the legislative branch of the governments. In addition, this thesis makes use of country profiles that have been drawn up by the Committee of Experts on Terrorism (CODEXTER) and by the Institute for Strategic Dialogue (ISD). This thesis will also draw on research done by national and international human rights organizations, such as Liberty (2015) and Freedom House, regarding the right to privacy in these three states and how it has been influenced by counterterrorism measures.

Lastly, this thesis will rely on the work of independent committees that were appointed in each country to monitor the workings of the agencies that are responsible for countering terrorism. These committees publish reports that outline the execution of counterterrorism measures and the points of improvement that have been found. These documents are used to get a clearer picture of the different types of measures that each country has implemented, and consequently how these measures affect the right to privacy.

The method that will be used to investigate the effects of counterterrorism measures on the right to privacy is that of controlled comparison. This is done to attribute any differences in the effects on privacy rights to factors that are different between the three states. The research method of controlled comparison requires cases that are alike in many aspects but differ in one crucial factor. The next section will elaborate on the choice of the Netherlands, Denmark and Great Britain.

4. Case Selection

As was mentioned in the introduction, despite the high terrorist risk in the Netherlands, Great Britain and Denmark, these countries remain understudied when it comes to the effects of counterterrorism measures on the right to privacy. The cases of the Netherlands, Great Britain and Denmark were chosen for a number of reasons, mainly revolving around the variance that can be observed in the extent to which the countries have been exposed to terrorism and the measures that each country has taken to combat terrorism. However, there are a great number of similarities between the countries that make them suitable cases for a controlled comparison. These similarities strengthen the inferences found as other variables that could influence the findings are controlled for. As the main difference between the states, namely the extent to which they have encountered terrorism, has already been outlined in the introduction, this section will focus on the similarities between the three countries.

First of all, the cases are all Western European countries and are thus for the most part based on the same liberal norms and values. In addition, all three states have a legal system that has its foundations in the rule of law. Second, all three states are members of the European Union and the United Nations and are consequently obliged to implement a number of regulations regarding counterterrorism, although a certain degree of room for interpretation remains for each separate government. Third, Denmark, Great Britain and the Netherlands have multicultural societies with roughly the same percentage of Muslim inhabitants (Pew Research Center, 2011). Fourth, in all three countries the main terrorist threat stems from radical or extremist Islamism. Last, and most importantly, the terrorist threat in these countries is perceived to be high (Opstelten, 2014; PET, 2015; May, 2015).

It may have already come to attention that this study focuses specifically on Great Britain as opposed to the United Kingdom as a whole. The reason for this is twofold. First, the United Kingdom includes Northern Ireland, which has the authority to determine its own counterterrorism measures and legislation to a certain degree. There are thus small differences to be observed between the measures implemented in the island of Great Britain and Northern Ireland, although a substantive part of the measures coincide. Therefore, in order to avoid confusion this thesis will only focus on the measures implemented in Great Britain. The second reason for leaving out Northern Ireland is that a number of measures that were implemented in Great Britain were aimed at reducing terrorism rooted in Northern Ireland. The analysis would therefore paint a distorted picture if Northern Ireland were included, as a number of measures that were implemented in Great Britain targeted just that area.

Having explained the choice of cases and the data and method that will be used in the analysis, the next section will outline how exactly this thesis will go about measuring the variables 'threat perception', 'counterterrorism measures' and 'the right to privacy'.

5. Operationalization

5.1 Threat perception

As was outlined above, there are many factors that influence a state's threat perception. Threat perception is in turn expected to influence the responses of a state to the terrorist threat and thus affect the right to privacy of its citizens. For the purposes of this thesis it would be very interesting to investigate these separate factors, and how each state's threat perception is influenced in different ways. However, the scope of that study would simply be too large for the purposes of this thesis. For that reason, this

thesis will rely on previous research that monitored the threat perceptions of Great Britain, the Netherlands and Denmark (Meyer, 2009; Muller, 2003; Walker, 2003). This research presents data up until 2008. For threat perceptions after 2008, this thesis will formulate expectations that are based on three factors that influence threat perceptions of European states to a great extent. This combination will allow for the analysis to evaluate precisely whether varying threat perceptions resulted in different responses in terms of counterterrorism measures. The three factors were already mentioned in the theoretical chapter, and include previous experience with terrorism, attachment to the U.S. and proactive foreign policy.

5.2 Counterterrorism measures

Counterterrorism measures in the Netherlands, Great Britain and Denmark are based on the general guidelines presented by the European Union. The strategy as drawn up by the Council of the EU is based on four pillars: 'prevent', 'protect', 'pursue', and 'respond' (Council of the EU, 2005). The central aspect of these four pillars is the goal to impede terrorists in their acts and ambitions, both at the very early stage of radicalization and at the more developed stage where a radicalized individual poses an urgent threat to citizens and the state. Despite these guidelines, EU member states carry the primary responsibility to combat terrorism, and therefore have a degree of freedom in implementing their own laws and measures to achieve their goals most effectively. The indicators for counterterrorism measures are thus as follows, based on the strategy prepared by the Council of the European Union in 2005:

1. A measure that aims to prevent people from taking to terrorism.
2. A measure that aims to protect citizens and infrastructure and reduce vulnerability to attack.
3. A measure that aims to pursue and investigate terrorists across EU borders and globally.
4. A measure that aims to prepare the member state to manage and minimize the consequences of a terrorist attack.

In the analysis the country specific interpretation of these guidelines will be outlined, as it will present the different measures that each country has taken in order to combat terrorism. The focus will be on those measures that are expected to influence the right to privacy, although other measures will also be mentioned. Based on what will be found there it will be possible to conclude what the effects are of each country's measures on the right to privacy enjoyed by its citizens.

5.3 Right to privacy

The operationalization of the effects on the right to privacy finds its roots in international law. The right to privacy is defined the European Convention on Human Rights as "the right to respect for his private and family life, his home and his correspondence" (art. 8). In addition, the right to privacy has been codified in the constitutions of the Netherlands and Denmark. In the Netherlands, the right to privacy is formulated as "the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament" (Constitution of the Kingdom of the Netherlands, art. 10, 2008). In the constitution of Denmark, its definition is somewhat more extensive: "The dwelling shall be inviolable. House searching, seizure, and examination of letters and other papers as well as any breach of the secrecy to be observed in postal, telegraph, and telephone matters shall take place only under a judicial order unless particular exception is warranted by Statute" (The Constitutional Act of Denmark, section 72, 2013). Great Britain forms an exceptional case, as it does not have a written constitution. Instead, British legislation is based on common law, case law, historical documents, Acts of Parliament and European legislation (Morris, 2008). As for the right to privacy in Britain, the Human Rights Act of 1998, which is the leading document when it comes to fundamental human rights, has incorporated the definition as proposed by the ECHR.

The statement that the right to privacy is a fundamental right that is supposed to be protected by each country's government is evident. However, as was mentioned above, in a matter of national security governments have the option of limiting their constituents' privacy in accordance with the law. This makes the right to privacy a qualified right. However, this limitation has to be necessary and proportionate for it to be lawful (UN High Commissioner for Human Rights, 2013; ISC, 2015). This means that in order to investigate the effects on the right to privacy, including its curtailment, the necessity and proportionality of the measures have to be taken into account. Necessity in international human rights law is related to the objective of a measure. But a measure must not only be logically connected to the intended objective; it must also be expected or proven to be effective in and capable of achieving it (EFF, 2014). This means that a certain infringing measure must be expected to be so crucial that the intended goal cannot be reached otherwise (EFF, 2014). If multiple options are possible to achieve this aim, the option that is the least infringing must be adopted. As for proportionality, a restrictive measure must be implemented only insofar as it is proportionate to the results that are expected to be generated (EFF, 2014).

A very restrictive measure is thus one that limits citizens' privacy in a way that is unnecessary and disproportionate. That means that such a measure is not proven or expected to be crucial in achieving a certain goal, which is in this case enhanced security from terrorism. In addition, a very restrictive measure is one that is disproportionate in that it affects citizens' right to privacy more than strictly necessary: a lower degree of infringement would then not result in less security from terrorism. This means that a measure that does affect a citizen's privacy but is both necessary and proportionate does not violate his right to privacy, whereas a measure that touches upon privacy but is not necessary or proportionate does restrict the right to privacy. The distinction between the practical concept of 'privacy' and the legal concept of 'right to privacy' is thus very important in understanding how the effects on right to privacy will be measured. The practical manifestations of counterterrorism measures on privacy are not at the centre of analysis, but rather the legal implications of these measures on the right to privacy are key in this study. That is the reason for the strong emphasis on the legal concepts of 'necessity' and 'proportionality'.

For the purposes of this thesis it is useful to formulate three categories of measures: those that are not restrictive, those that are somewhat restrictive, and those that are very restrictive. The specific case studies can then apply these categories to the measures at hand and analyze which country has implemented which types of measures. The three categories are then as follows:

Non-restrictive

- A measure that does not affect an individual's privacy.

Somewhat restrictive

- A measure that does affect an individual's privacy and that could be implemented in an unnecessary and/or disproportionate manner.

Very restrictive

- A measure that does affect an individual's privacy and that is unnecessary and/or disproportionate.

The case studies will further outline these three types of measures and how they are manifested in practice. The next chapter will outline the strategy and legislation implemented by the European Union in order to combat terrorism.

6. European Union Legislation and Strategy

The three states analyzed in this thesis are all member states of the European Union and are therefore for a great deal bound by legislation drawn up by EU institutions. This section will consist of two parts. First, European legislation regarding the right to privacy will be outlined. Second, European counterterrorism strategies and legislation will be elaborated on.

As was mentioned before, the right to privacy is a fundamental human right that has been codified in many international declarations and treaties. In the European Convention on Human Rights (ECHR, art. 8), the right to privacy, titled the 'Right to respect for private and family life', is formulated as follows:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The list of exceptions that can provide a basis for a limitation of the right to privacy is, as can be seen above, quite extensive. Not only can respect for private and family life of citizens be limited when national security or public safety is at stake, but also when the rights and freedoms of others need to be protected. As was seen in the theoretical section, the notion that the fundamental rights of some might be limited in order to protect the rights and freedom of the many can have far-reaching consequences. If the right to privacy is interpreted as a positive duty of the state, and in many cases it is, then this provision can easily lead to a restriction of the right to privacy. If, however, "the rights and freedoms of others" is interpreted in the most basic sense, then a restriction is not accounted for.

In addition to the provision of privacy protection in the ECHR, the Charter of Fundamental Rights of the European Union (art. 7 and art. 8) provides a somewhat more detailed provision relating to privacy rights of EU citizens. Article 7 is similar to article 8.1 of the ECHR, but article 8 specifically focuses on the protection of personal data. It states that "Everyone has the right to the protection of personal data concerning him or her", and "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law".

This Charter possesses the same legal value as EU treaties, making it a binding agreement.

The European Commission has implemented a number of directives that relate to the protection of privacy of EU residents more specifically than the provisions mentioned above. The basis of privacy protection is provided by Directive 95/46/EC, which aims to protect individuals with regard to the processing of personal data and the free movement of such data. In addition, two directives were implemented in 1997 and 2002 that specifically address the protection of privacy in the sphere of telecommunications and electronic communications, respectively.

EU legislation is thus largely focused on privacy protection in the sphere of communications. However, directives are not immediately enforceable but have to be transposed into national law first. Additionally, directives are a type of EU legal acts that allow for room for interpretation, as only the specified goal is binding, but specific policies and legislation are left up to the separate member states. It can thus be expected that some variation will be found in national legislation and policies regarding privacy protection.

The leading document on counterterrorism on EU level is 'The European Union Counter-Terrorism Strategy", published in 2005. This is a non-binding document but it nonetheless provides an extensive security framework for EU member states. The strategy is based on four pillars: 'prevent', 'protect', 'pursue', and 'respond', which are supposed to reduce the terrorist threat and the states' vulnerability to attack. The overall aim of this strategy is to combat terrorism while respecting human rights, and to make the EU a safer area in which its citizens can enjoy freedom, justice and security (Council of the EU, 2005). It is made clear that member states carry the main responsibility in fighting terrorism, but the EU can provide aid by strengthening national capabilities, fostering European cooperation, developing collective capabilities and enhancing international partnerships (Council of the EU, 2005).

The preventive character of this strategy is focused on stopping people from turning to terrorism, thus aiming at prohibiting recruitment and radicalization into extremist terrorist groups and organizations. Key policies in this area include the early spotting of radicalized behavior, prohibiting incitement of terrorist ideas, and preventing the misuse of the Internet for recruitment and incitement purposes (Council of the EU, 2005: 9). As for protection, this strategy focuses on measures that reduce vulnerability to attack and to minimize the impact that an attack would have on key targets. The priorities in this field mainly involve infrastructural security, thereby focusing for instance on using biometric data in air travel and aligning standards for civil

aviation, port and maritime security (Council of the EU, 2005: 11). In order to pursue terrorists and impede terrorist activities this strategy aims to block terrorist funding, dismantle terrorist networks and obstruct terrorist planning. In order to achieve this effectively, policy recommendations mainly evolve around the use and sharing of data, the use of surveillance and intelligence and information exchange (Council of the EU, 2005: 14). Finally, the strategy's focal points for 'response' mainly include the mechanisms that are already in place to deal with catastrophes such as natural disasters (Council of the EU, 2005: 16).

In addition to this common strategy, the most important document relating to counterterrorism on EU level is the Council Framework Decision of June 13th 2002 (2002/475/JHA) and its amending act of 2008. A framework decision was similar to a directive in that it binds the member states to a certain goal to be achieved, but does not include the concrete measures and policies that should lead to this goal, leaving this up to the member states national jurisdictions. This framework decision is important for two reasons. First, it implements a common definition of terrorism and a list of offences that are deemed terrorist. Second, it provides a detailed list of terrorist offences and a rough guide to their corresponding penalties.

The definition of terrorism highlights two aspects: the aim with which a terrorist act is committed and the actual offences that are committed. There are three aims that are inherent to terrorism: seriously intimidating a population, compelling an government or organization to act or abstain from acting, and seriously destabilizing and destroying the political, constitutional, economic or social structure of a country or organization (Council of the EU, 2002: 2). As for terrorist offences, there are a number of different acts that constitute terrorism, such as attacks upon a person's life, kidnapping, and seizure of public means of transport. The amending act of 2008 added more offences, mainly enhancing the preventive character of counterterrorism policy. It is not the aim of this thesis to go into too much detail here regarding these documents, but suffice it to state that these framework decisions provide a clear basis for national counterterrorism policy with regard to what exactly constitutes terrorism and how to penalize it.

A controversial document in this area is the Data Retention Directive (DRD), which was established in 2006. This directive calls on EU member states to compel their telecommunication providers to retain communication data for a period between six months and two years (European Union, 2006: art. 6). These data include the source of communication, type of communication and time of communication, among other things, but does not include the communication's content. Several states had already

implemented measures on data retention in order to combat serious crime and terrorism, as the analysis of processed communication data had proven to be an effective tool in the past. This directive's aim was to unify the varying measures that were implemented in national legislations across the EU. It specifically points out the human rights concerns that are related to this measure, and specified that any measure that could infringe upon an individual's right tot privacy must be proportionate and necessary and in accordance with the law. However, in 2014 the Court of Justice of the European Union (CJEU) declared the DRD to be invalid. The reason for this was that "it entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary" (CJEU, 2014).

To sum up, the European Union has provided a clear framework in which member states can develop their own counterterrorism measures. It focuses primarily on the prevention of radicalization, the tracking down of individuals who pose a terrorist threat, and reducing the vulnerability of member states. In addition, the EU has implemented a number of straightforward policies that are to protect the right to privacy of EU citizens. As will be seen below, the three cases in this study have all largely based their national counterterrorism measures on this EU strategy. The next section will outline the global UN strategy as this document has also provided a great foundation for counterterrorism efforts for the three states of this study.

7. United Nations Resolutions and Strategy

In addition to EU legislation and strategic objectives, the United Nations has also implemented a number of influential resolutions and strategy points that aim to fight terrorism. This section will therefore go over the three UN resolutions that have contributed most to national policy-making. These resolutions are for the most part focused on making preparation and incitement of terrorism a criminal offence, strengthening cooperation between states and relevant international organizations and ensuring compliance with international human rights law.

The first resolution that was adopted in relation to terrorism was Resolution 1373 (2001). This resolution was the answer of the United Nations Security Council (UNSC) to the 9/11 attacks on the US and was adopted unanimously. Its content consists of two main branches of declaration. First, it calls on states to prevent terrorism and to impede terrorists in their actions and plans. This should be done by, for instance, freezing finance of people who commit or who are planning to commit a terrorist crime, and by denying safe havens to those who are planning to commit a terrorist attack.

Second, it calls for a greater degree of information sharing between states. This should lead to enhancement of operational information that states possess and that they can use to combat terrorism, and it should ease the judicial processes related to terrorist crimes in separate states. In order to strengthen these decisions the Counter-Terrorism Committee (CTC) of the UNSC was established with this resolution. The main goal of this body is to assist states in implementing the decisions taken in Resolution 1373 and to assess whether states do this in the most effective manner (CTC, 2015). However, this body does not have any powers to sanction states that do not comply.

The next resolution that had great influence on national legislation and policies was Resolution 1624 of 2005. In this resolution, the UNSC reaffirms its determination to combat terrorism and calls on all states to do the same. A number of characteristics stand out in this resolution. First, it goes further than Resolution 1373 in that it extends the criminal offence of terrorism to incitement in addition to the actual planning and executing of a terrorist attack (UNSC, 2005). States should prevent incitement and also deny access to individuals who are reasonably suspected of having incited others to commit acts of terrorism. The second characteristic of this resolution that deserves attention is the fact that it greatly focuses on human rights and the fact that every counterterrorism measure should be taken in compliance with international human rights law (UNSC, 2005). For instance, it states that

"Reaffirming also the imperative to combat terrorism in all its forms and manifestations by all means, in accordance with the Charter of the United Nations, and also stressing that States must ensure that any measures taken to combat terrorism comply with all their obligations under international law, and should adopt such measures in accordance with international law […]"

This goes further than the decisions in Resolution 1373, in which human rights were barely mentioned. It thus seems that states needed to pay greater attention to human rights in their counterterrorism efforts as more far-reaching decisions were made.

In 2006 the UN General Assembly adopted a resolution that implemented a globally unified strategy to combat terrorism. This strategy is also based on four pillars. The first of these consists of measures that "address the conditions conducive to the spread of terrorism" (UN, 2006). This includes measures to strengthen UN capabilities to peacefully resolve conflicts through mediation, negotiation, conflict prevention and peace building, as this would help the global fight against terrorism. In addition, the focus in this pillar is on promoting social cohesion and reducing youth unemployment,

promoting a culture of peace, human development and justice, and encouraging dialogue and understanding among civilizations and peoples in order to enhance mutual respect. These measures are thus aimed at tackling the underlying motives for taking to terrorism and at promoting peaceful means of voicing grievances.

The second pillar consists of measures that are to prevent and combat terrorism (UN, 2006). This pillar contains 18 points and is thus by far the most extensive pillar in this strategy. First and foremost, the measures in this pillar encourage states to impede the planning, financing, inciting, supporting, participating, organizing and tolerating of terrorism in any circumstance. It calls on states to intensify cooperation and coordination in relation to combating serious crimes that can precede terrorism and to exchange information that is important for the prevention and combat of terrorism in a timely manner. This includes the set up of regional and international border controls. It also urges states to build capabilities that are to protect specific objects, persons and infrastructure that would suffer most from a terrorist attack, and to ensure that an appropriate response can be made when a terrorist attack occurs (UN, 2006).

The third pillar is mainly focused on improving states' capabilities to combat and prevent terrorism and on enhancing the role of the United Nations in this process. It includes measures that call for the active participation in fighting terrorism of a number of relevant organizations, such as the International Monetary Fund, the World Bank and the World Health Organization. It calls on these organizations to provide assistance and information to states in their specific field of knowledge, for instance by asking the International Atomic Energy Agency to help build state capacity to prevent terrorists from accessing the state's nuclear materials. It also reaffirms the importance of information sharing and for that means establishes the Counter-Terrorism Implementation Task Force (CTITF), which is charged with the overall coordination of coherence among UN member states' counterterrorism efforts.

The last pillar revolves around the respect for human rights and the rule of law as a basis for all counterterrorism measures across the globe (UN, 2006). It affirms that effective counterterrorism measures and human rights and the rule of law are not mutually exclusive but in fact reinforce each other. Measures in this pillar aim to strengthen the role of the High Commissioner for Human Rights and the Special Rapporteur on the Protection and Promotion of Human Rights and Fundamental Freedoms While Countering Terrorism. However, both these institutions do not have the power to sanction states but can merely offer advice and assistance and address human rights allegations. It also reaffirms that national criminal justice systems must be founded on the rule of law and must therefore provide for the prevention and

prosecution of terrorist crimes in accordance with human rights and fundamental freedoms (UN, 2006).

To sum up, the resolutions and strategy that were adopted by the United Nations Security Council and General Assembly in the first decade of the 21st century expand the scope of crimes that constitute terrorism in order to more effectively prevent terrorist attacks from occurring. In addition, they call for enhanced cooperation between states, especially in the field of information exchange about possible threats, and between states and international organizations and institutions that can aid states in preventing terrorism and diminishing terrorist threats. Lastly, the last two resolutions place great focus on the respect for human rights and fundamental freedoms in combating terrorism, and call for legal systems that ensure that terrorists and victims of terrorism are dealt with in a way that is in accordance with international law. As was mentioned before, these resolutions have influenced national decision-making, but as with the EU counterterrorism strategy, states are left to their own devices in formulating the specific details regarding counterterrorism measures. The next chapters will present how the three states in this study have dealt with the terrorist threat and how threat perceptions have influenced the right to privacy.

8. Case Study of Great Britain

8.1 Threat Perception

The current threat level that Great Britain faces is 'severe'. This is the second highest level, and it means that a terrorist attack is very likely to happen. The greatest threat stems from Islamist terrorism, especially from Syria and Iraq, as many British nationals have travelled there and probably received terrorist training (May, 2015: 7). Despite this high threat level, Great Britain is no stranger to severe terrorist threats. Already in colonial times did Great Britain experience acts of terrorism in their overseas territories (Walker, 2003: 13). In addition, the struggles in Northern Ireland caused many terrorist acts related to nationalist sentiments up until 1997 (Walker, 2003: 13). After the ceasefire between the Provisional Irish Republican Army and the British police was reasserted, threat perceptions decreased, despite a threat assessment of 'moderate' in relation to Northern Irish terrorism (MI5, 2015).

However, after the attacks of 9/11 on the US threat level somewhat increased again, albeit to a lesser extent than most European countries. This is probably due to the fact that Great Britain already had extensive experience with terrorism and was not easily intimidated (Meyer, 2009: 657). Since then, the British threat perception has been relatively high, mainly due to Britain's active participation in the so-called US led

'Coalition of the Willing' that invaded Iraq in 2003, and the large-scale terrorist attacks that hit London on July 7th 2005 (Meyer, 2009). The threat perception of Great Britain has at the same time been relatively stable since it increased after 9/11, with an average of 25 per cent of the population regarding terrorism as one of the two most important issues between 2003 and 2008 (Meyer, 2009: 658).

Due to the threat perception that has been higher than most in European countries since 2003 it can be expected that Great Britain has implemented fairly restrictive measures since then in order to prevent an attack from actually happening.

8.2 Counterterrorism Measures and the Right to Privacy

Great Britain's counterterrorism framework is extensive and developed quite randomly over the past decade and a half (ISC, 2015). The first set of counterterrorism legislation and policies was presented already in 2000 in the Terrorism Act (CODEXTER, 2007: 1). This took place before the terrorist attacks on the U.S. happened, and is thus in line with the notion that the relatively high threat perceptions of Great Britain have inspired new counterterrorism measures at times when there was no particular cause in the form of a grave terrorist attack. After this Act, many Acts have followed, all focusing on different aspects of the counterterrorism regime. As a result, the British counterterrorism framework is complicated and lacks transparency (ISC, 2015: 2).

Non-restrictive measures

As is the case in many other European countries, Great Britain has implemented a number of programs that aim to reduce the risk of radicalization among mainly young people, and with that reduce religious extremism. Seeing is this is a key source of terrorism, these policies are supposed to increase security from terrorism by focusing on its root causes. This body of policies is found in Britain's counterterrorism strategy's (CONTEST) 'prevent' pillar. This pillar includes measures that aim to prevent individuals from taking to terrorism and to respond to the ideology of terrorism and those who promote it. This is also in response to the increased threat posed by foreign fighters, and these measures therefore aim to reduce the impact that terrorist propaganda can have on individuals. Online propaganda is tackled by the Counter-Terrorism Internet Referral Unit (CTIRU), whose job it is to find and remove content that breaches UK terrorism legislation. Also offline propaganda is inhibited as propagandists can be excluded from the country and as platforms that offer a stage to propagandists, such as educational institutions, are removed (May, 2015: 15). In addition, measures in the 'prevent' pillar aim to stop people from radicalising by offering counselling and mentoring, and by

distributing leaflets containing information about the dangers of travelling to Syria and Iraq (May, 2015: 16). There is also an increased focus on community-led initiatives to stop radicalisation, and a new provision in the Counter-Terrorism and Security Act of 2014 that compels certain bodies such as universities and local authorities to actively map the risk of terrorism and, if a risk is revealed, to draw up a plan to counter it.

Somewhat restrictive measures

Measures that affect the right to privacy and that might not be fully necessary or proportionate constitute a considerable part of Great Britain's security policy. First of these is targeted interception, which is a tool that is used to monitor the content of a communication and to have someone other than the sender or the receiver analyze it (ISC, 2015: 17). This type of interception is only useful when there is already significant evidence that the person whose communications will be intercepted may pose a threat to Britain's security. In order for a targeted interception to take place, the security agent needs a warrant signed by a Secretary of State. In his application for the warrant, it has to be clearly stated how this specific interception is necessary and proportionate (ISC, 2015: 19). Comparable to targeted interception is the analysis of communications data. This differs from interception in that communications data reveal the 'who, when and where' of a communication, but not its content (ISC, 2015: 47). This type of security measure is used to focus on specific individuals who may pose a threat so that a targeted interception can be made in a later stage. Communications data thus reveal whether a person might require further investigation or not.

This type of security measure has been a source of controversy. The reason for this is that technological advances have made it possible to derive much more than just the 'who, when and where' from a communication. This means that the initial legislation on communications data has been stretched and that nowadays many more details about an individual, such as habits, preferences or lifestyle, can be analyzed through the use of communications data, even without reading the actual content (ISC, 2015: 53). This means that this type of security measure has developed further than its original mandate, resulting in counterterrorism powers that are not governed in a complete manner. As a consequence, the use of communications data could lead to disproportionate and unnecessary privacy infringements if its not supervised very carefully (ISC, 2015: 53). So even though the use of communications data is less intrusive than analyzing a communication's content, these two types of security tools are in the same category.

Very restrictive measures

There has been much debate about Britain's counterterrorism measures that affect citizens' privacy but that are not necessary or proportionate. These measures became an issue especially after whistleblower Edward Snowden revealed the existence of large-scale interception capabilities of the Government Communications Headquarters (GCHQ). These capabilities are used to determine in the first place which individuals might pose a threat to the security of Great Britain by generating new intelligence leads (ISC, 2015: 25). This was done through the use of a program named Tempora, which made use of a large number of interceptors on fiber optic cables through which as many as 600 million communications could be monitored every day (Omzigt, 2015: 6). This type of surveillance is indiscriminate and unnecessary, as the vast majority of the data that are collected are not used and most data are about citizens against whom there is no suspicion at all that they might pose a threat to Britain's security (Bigo et al., 2013: 16).

In addition to the mass interception of communications, Britain has recently passed a bill that allows for security agencies to force telecommunications providers to retain communications data for one year, called the Data Retention and Investigatory Powers Act (DRIPA) (May, 2015: 11). Data retention was already implemented as a counterterrorism measure in the Anti-Terrorism, Crime and Security Act of 2001 (CODEXTER, 2007: 3). DRIPA was passed shortly after the European Court for Human Rights declared the EU Directive on data retention to be unlawful, as it allowed for too great a restriction on the right to privacy of EU citizens. However, in Britain's counterterrorism strategy this type of measure was stated to be a vital tool for security and intelligence agencies (May, 2015: 11). This means that telecom providers must intercept and retain either certain types of data or all data and disclose these when lawfully requested (May, 2015: 11).

9. Case Study of Denmark

9.1 Threat Perception

The threat level in Denmark is 'significant', meaning that a terrorist attack is likely but not imminent. In its latest report of March 2015 on the threat level in Denmark, the Centre for Terror Analysis specifically mentions that the risk of falling victim to a terrorist attack in Denmark is very limited, despite the general threat to the country being significant (CTA, 2015: 1). The terrorist threat in Denmark mainly stems from Islamist extremism, both from domestic sources and from abroad. This means that not only international terrorism poses a threat, but also foreign fighters who return from

Syria or Iraq to Denmark and who adhere to extremist Islamism. As for preceding years, Denmark's threat perception has fluctuated to a great extent. After the 9/11 attacks in 2001 it increased more than average, and it settled again to average levels in 2003. This is due to the fact that Denmark is a small country with relatively little experience with terrorism, so the 9/11 terrorist attacks had a great impact on the country (Meyer, 2009: 657). Threat perceptions increased sharply again after the cartoon controversy in 2005, remaining high until October 2006. This implies that the cartoon controversy had a large impact on threat perceptions in Denmark. After 2006 it declined again to lower levels (Meyer, 2009: 658).

After the cartoon controversy Denmark has not experienced any significant terrorist attacks, apart from the Copenhagen shootings that took place in February 2015. However, as was already mentioned, as these events took place so recently, it will be very difficult to already discern meaningful responses in terms of counterterrorism measures. One factor that has been present to a certain extent is an active foreign policy with regard to states that harbor or are believed to harbor terrorists and terrorist networks, as Denmark decided to participate in the fight against ISIS in Iraq in September 2014 (Worland, 2014). This decision resulted in the assessment that the terrorist threat is now 'significant'.

Based on the above it can be expected that the number of counterterrorism measures increased after 2001 and after 2005, due to the increased threat perceptions that were observed in Denmark. Overall, however, threat perceptions in Denmark have been relatively low, so the level of restrictiveness of counterterrorism measures is also expected to be limited.

9.2 Counterterrorism Measures and the Right to Privacy

The counterterrorism measures that are present in Denmark right now were presented in two main "Anti-terrorism Packages", one in 2002 and one in 2006. This is perfectly in line with the increased threat perceptions in 2001 and 2005/2006. The measures that were presented in Package I mainly focused on expanding the scope of terrorist offences and on giving the Danish Security and Intelligence Service (PET) increasing powers to detect dangerous individuals. Package II built on the first by further increasing the powers and capabilities of PET and enhanced cooperation between several security and police services in Denmark. A large part of Danish counterterrorism measures is focused on preventing radicalization, especially among young people, in addition to the prevention of terrorist attacks.

Non-restrictive measures

Denmark has implemented a vast number of measures that are to counter radicalization and extremism, and which are thus not restrictive of the right to privacy. Two main programs stand out in this category, called "Back on Track" and "Targeted Intervention" (Søvndal, 2012). Both programs are aimed at reducing the risk of individuals radicalizing into Islamist extremism, but their focus groups are different. The "Back on Track" program is aimed at former inmates charged with terrorist crimes who are perceived to be the most vulnerable to Islamist propaganda. The "Targeted Intervention" program offers mentor schemes to those who are perceived to be most likely to radicalize, and it offers a way out for people who find themselves in milieus in which extremist ideas are the norm and who wish to get out (Søvndal, 2012: 5-6). In addition, there is a great focus on actively engaging local workers such as police, teachers and social workers in identifying individuals who might be at risk of radicalizing and in helping them to prevent this.

Somewhat restrictive measures

As is the case in many other states, including those under scrutiny here, targeted interception is an important tool for the Danish Security and Intelligence Service to identify individuals who might pose a threat to the security of Denmark, including potential terrorists. The use of targeted interception requires a court warrant that states the name of the individual whose communications are to be intercepted. This can only take place if the communication in question is expected to be sent or received by the suspect, if the communication's content are expected to be of decisive importance, and if the crime that is suspected is punishable with at least six years imprisonment (CODEXTER, 2007: 4). As for surveillance, there are a number of measures that make it easier for the PET to monitor certain places and individuals. More specifically, the surveillance of individuals using a controlled or automatic device can take place if the offence that is suspected is punishable with more than one year and six months imprisonment. In addition, for surveillance in a private home or premise a court warrant is needed that specifically states the necessity and proportionality of the action (CODEXTER, 2007: 4).

An aspect of Denmark's counterterrorism efforts, one that is unlikely to be found anywhere else, is the use of the Danish Personal Register (DPR). This is an online database that contains a large number of details and information about each Danish citizen. With the implementation of the second Anti-Terrorism Package of 2006, the PET obtained the power to make use of the personal information contained in the DPR. The

agency needs the approval of the particular authority that is in charge of the information that is acquired. However, there is no judicial oversight over this procedure, so the possibility exists that the powers are used in a manner that is not necessary and proportionate (Lindekilde and Sedgwick, 2012: 21).

Very restrictive measures

As is the case in Great Britain, Denmark implemented a law on the retention of communications data by telecommunications and Internet providers in 2001. This happened before the EU Data Retention Directive was implemented. The Danish law on data retention obliges telecom and Internet providers to log communications data for at least one year (Lindekilde and Sedgwick, 2012: 20). This concerns the details about the communication only, as opposed to the content of, for instance, an email. The PET requires a court warrant to access these data, but the all data about individual data traffic have to be retained nonetheless. In addition, Denmark has implemented so-called sniffer programs (CODEXTER, 2007: 3). These programs allow for repeated covert searches under the same warrant, meaning that communications can be intercepted without a specific court order. Despite the fact that an initial court order is needed to implement the interception, and that thus necessity and proportionality are an important factor in deciding whether or not the interception will take place, the repetitive nature of this measure is not dependent on necessity or proportionality.

10. Case Study of the Netherlands

10.1 Threat Perception

As is the case with Denmark, the Netherlands has relatively little experience with terrorism. In its history, terrorist attacks have been very infrequent and small in scope. After the attacks of 9/11 on the U.S. the threat perception of the Dutch increased steeply as a result of this limited experience, with Dutch citizens considering international terrorism as the number one threat (Muller, 2003: 159). Dutch threat perceptions decreased a little until 2003, when the Netherlands started participating in the invasion in Iraq led by the United States and threat perceptions rose accordingly. In 2005 threat perceptions were the highest, with 40 per cent of the Dutch population considering terrorism as one of the two most important threats that the Netherlands faced (Meyer, 2009: 658). A clear reason for this is the assassination of Theo van Gogh in November 2004: after this terrorist act, threat perceptions started rising steeply (Meyer, 2009: 658). After this event threat perceptions decreased again, as no other acts of terrorism

took place. The Dutch participation in the fight against the Islamic State (IS) has presumably increased threat perceptions again from late 2014 on.

These fluctuations in threat perceptions in the Netherlands are reflected by the threat level as assessed by the Dutch National Coordinator for Counterterrorism and Security (NCTV). The first ever threat level that was assessed in 2005 was 'substantial', reflecting the threat perception described above. It remained at this level until March 2007, when it was lowered to 'limited' for a period of one year. For a period of three years the threat level was assessed at 'limited', until the current level of 'substantial' was put in place in March 2013 (NCTV, 2015). As is the case with Denmark and Great Britain, the biggest terrorist threat to the Netherlands stems from Islamist extremism and jihadism, with approximately 190 Dutch citizens having travelled to Syria and Iraq to support the cause of IS (NCTV, 2015).

Based on the above outline of Dutch threat perceptions, it can be expected that the Netherlands has implemented most restrictive measures in 2005. Apart from that, due to the relatively low threat perception and lack of experience with large-scale terrorism, it can be expected that Dutch counterterrorism measures are relatively non-restrictive.

10.2 Counterterrorism Measures and the Right to Privacy

As was mentioned earlier, the Netherlands barely had any experience with terrorism prior to the 9/11 on the U.S. Consequently, the Dutch counterterrorism policy was for the most part established after these attacks. Since then, counterterrorism efforts in the Netherlands are characterized by a clear balance between repressive measures and preventive measures (Muller, 2003: 152). This balance forms the basis of the counterterrorism policies that are in place nowadays and was dubbed the 'comprehensive approach (NCTV, 2011: 8). The counterterrorism framework that is currently in place was presented in a five-year strategy, lasting from 2011 until 2015.

Non-restrictive measures

An important aspect of the Dutch comprehensive approach is the prevention of radicalization and extremism. Other than in Great Britain and Denmark, the Dutch security policy does not view radicalization into extremism as a threat per se, as only violent extremism poses a threat. There is a great focus on the chain of events that leads individuals to become terrorists, and the overall assumption is that early intervention in this process can diminish the chance of a terrorist attack occurring in the future (CODEXTER, 2008: 1). In order to identify which influences enhance the risk of

radicalization, a great deal of research is done. Other policies that govern this area of counterterrorism aim at intervening in an early stage and reducing the risk of radicalization into violent extremism. In order to achieve this, it is necessary to reduce the breeding ground for radicalization by countering extremist narrative and investing in de-radicalization (NCTV, 2011: 10). This part of the comprehensive approach has led to a steady decrease of the threat posed by Dutch nationals since it was first implemented in 2003 (NCTV, 2011: 20).

Somewhat restrictive measures

As is the case in many other states, the use of targeted interception is an important tool for Dutch security and intelligence agencies. What sets apart the Dutch approach to interception from other approaches is that as opposed to 'reasonable suspicion', merely 'indications' of terrorism are enough to order a warrant for interception. This change was implemented with the Act to Broaden the Scope for Investigating and Prosecuting Terrorist Crimes of 2006 (Eijkman, 2012: 58). This relatively low threshold can lead to the use of interception in cases in which interception is not per se necessary to obtain crucial intelligence. However, a warrant signed by the relevant Minister is needed for each interception, so the indiscriminate use of interception as a security tool is unlikely to take place.

Very restrictive measures

There is no evidence that the Netherlands has implemented measures that are very restrictive of the right to privacy. This means, among other things, that there is no evidence of indiscriminate "mass" interception or surveillance done by Dutch security and intelligence agencies. While this is good news, there is currently a lively debate going on after the Dutch government requested a reassessment of the Intelligence and Security Services Act of 2002. This act makes it illegal to tap cable-bound communications under any circumstance (Bigo et al., 2013: 75). However, it was argued that since the bulk of communications nowadays takes place via cables, the Act is no longer up-to-date and requires new legislation (Rjiksoverheid, 2013). If this proposition would indeed be passed, bulk interception of communications would be added to the capabilities of the Dutch security and intelligence agencies.

In addition, the Data Retention Directive was implemented when proposed by the European Council, but was declared invalid by the Dutch judiciary after the Court of Justice of the European Union ruled that it violated the right to privacy of Dutch citizens (Zenger, 2015). Immediately following this decision, many telecom providers

announced that they would stop executing this law and thus cease to retain data (Zenger, 2015).

11. Analysis and Discussion

11.1 Threat Perception

After 9/11 the fear of terrorism was highest in Great Britain, with the levels in Denmark and the Netherlands being very similar and somewhat lower (Meyer, 2009: 657). In general, the Dutch threat perception was the lowest of the three between 2003 and 2008, only outweighing that of Denmark and Great Britain in November 2005 (Meyer, 2009: 658). In 2008 the three states converged to almost the same level of threat perception (Meyer, 2009: 658). After 2008, none of the three cases of this study experienced any significant terrorist attacks. This would lead to the conclusion that threat perceptions after 2008 were relatively low. However, all three states participated in the U.S.-led coalition against the Islamic State, mainly in Iraq, with varying intensity. Whereas Denmark and the Netherlands only sent aircrafts and tools such as helmets and bulletproof vests, Great Britain also sent troops and conducted air strikes against targets in Iraq (Drennan, 2014). This would generate the expectation that threat perceptions in Great Britain have been somewhat higher since its participation in the fight against IS. This decision was in line with previous foreign policy decisions made by Great Britain, as the country is known as a loyal ally of the United States (Watt, 2012). This fact in itself already constitutes a reason for a higher threat perception, as links and attachments to the U.S. have been proven to be a source of high threat perceptions (Meyer, 2009: 660).

Based on this, it can be concluded that threat perceptions have generally been highest in Great Britain. This is despite the fact that British threat perceptions did not increase as much as other states' in the aftermath of 9/11. This high threat perception is due to the extensive experience with terrorism that Britain has, stemming from the struggles in Northern Ireland and the related acts of terrorism, and from the London bombings of 2005. In addition, Great Britain is a close ally of the United States, which is itself an important target of international Islamist terrorism. As a result, Britain has actively participated in the invasion of Iraq in 2003 and in the coalition against IS in 2014. This thus confirms the hypotheses regarding the causes of a high threat perception. Denmark and the Netherlands, on the other hand, have not experienced any large-scale terrorism in their history, leaving out the recent shooting in Copenhagen. They are also not as close in alliance with the United States. So despite both countries' engagement in the fight against IS in 2014, their threat perceptions have been and still

are somewhat lower. Denmark and the Netherlands therefore also confirm the three hypotheses concerning threat perception. These findings are reflected in the threat levels as assessed by the countries' security agencies: Great Britain's threat level is 'severe', whereas the Dutch and Danish threat levels are assessed lower at 'substantial'.

These findings generate some expectations as regards the severity of their counterterrorism efforts. As was seen in the theoretical section, many states have turned into "risk societies", focusing on eliminating every possible risk (Beck, 1992). This is the job of the governing elite, as they are responsible for the population's general well-being, including their freedom from fear. As a result, security policies are completely centered on the elimination of risks, calling for measures that are increasingly preventive and intrusive of certain rights and liberties. The higher the risks that are perceived, the more preventive the measures become. This means that threat perception is an important factor in predicting the severity and intrusiveness of counterterrorism measures. As Britain has had the highest threat perception of the cases studied here, it is expected to have implemented the most restrictive measures as well. Denmark and the Netherlands, on the other hand, have both experienced relatively low threat perceptions, and are therefore expected to have implemented less invasive measures. The following section will analyze the differences between each country's counterterrorism policies, followed by a discussion regarding the results.

11.2 Counterterrorism Measures and the Right to Privacy

A striking finding that can be observed in the counterterrorism frameworks of the three countries of this study is that both Great Britain and Denmark have implemented most measures that are very restrictive of the right to privacy. This is contrary to the expectations that were formulated in the hypothesis regarding the influence of threat perceptions on the restrictiveness of counterterrorism measures, as that would have predicted lower levels of restrictiveness in Danish measures as a result of a lower level of threat perception. The counterterrorism measures implemented by Great Britain have a very repressive nature, and are less focused on removing breeding grounds for terrorism, tackling extremist propaganda and overall intervening early in the process of radicalization. On the contrary, most of the British counterterrorism framework revolves around intrusive capabilities used by the security and intelligence services, such as wiretapping, surveillance and interception. As a matter of fact, the British capabilities for interception are by far the most expansive of the three countries studied here (Bigo et al., 2013: 50). Most restrictive of these is the use of bulk interception capabilities, which can indiscriminately collect the data of hundreds of millions

communications per day. Even though the content of these data is not collected and can only be collected with a warrant signed by a Secretary of State, the analysis of communications data can disclose a lot of personal information about an individual. In addition to the bulk interception of communications, the new Data Retention and Investigatory Powers Act (DRIPA) obliges telecom and Internet providers to retain data for up to one year.

Denmark does not have the capabilities to conduct mass interception, but does still enforce its own version of the unlawful Data Retention Directive of 2006. This means that Denmark too forces its telecom and Internet providers to retain data for a certain period and to disclose these to the intelligence and security service when so requested. As was already mentioned above, data retention is completely indiscriminate and thus allows for the storage of details about personal communications of individuals of whom there is no suspicion whatsoever. This was therefore categorized above as a very restrictive measure because it is neither necessary, in that it is expected to contain information that is crucial in an investigation, nor proportionate, in that it does not infringe the right to privacy more than absolutely necessary.

The Netherlands, in turn, shows a greater emphasis on the early prevention of radicalization in its counterterrorism efforts. This is part of the Dutch comprehensive approach, which clearly states the difference between preventive measures and repressive measures. This does not mean that no use of intelligence capabilities is made, but rather that allowing for intrusion of privacy is done more reluctantly than in Great Britain and Denmark. This is reflected in the fact that the capabilities and powers of intelligence and security services in the Netherlands are generally more limited than in the other two states. However, the Dutch government is currently looking to expand the existing legislation on interception and surveillance, so that also Dutch security and intelligence services could get more extensive powers in identifying, profiling and inhibiting possible threats.

11.3 Discussion

The first important result that can be observed is the fact that in each case a high threat perception led to renewed counterterrorism measures and tighter policies. In the Netherlands, threat perceptions peaked in 2005. In 2006, the Act to Broaden the Scope for Investigating and Prosecuting Terrorist Crimes was implemented, giving intelligence and security services extended powers and lowering the threshold from 'reasonable suspicion' to 'indications' of terrorist crimes. In Denmark, threat perceptions were highest after the 9/11 attacks in 2001 and after the cartoon controversy in 2005,

resulting in new anti-terrorism packages in 2002 and 2006. In Great Britain, threat perceptions were generally higher, but showed a slight peak after 9/11 and after the London bombings of 2005. Accordingly, the Anti-Terrorism, Crime and Security Act was passed in 2001 and in 2006 the new Terrorism Act was passed. However, as was seen above, British threat perceptions were on average high, but stable. As a result, counterterrorism measures were implemented on a more random basis than in the Netherlands and Denmark (CODEXTER, 2007; May, 2015). It can thus be concluded that high threat perceptions lead to new policies and measures that aim to counter the perceived threat.

However, the fact that high threat perceptions lead to new measures does not automatically imply that these measures are very restrictive. This leads to the second result, and that is that the hypothesis regarding the influence of threat perceptions on the level of restrictiveness of counterterrorism measures does not hold true: Denmark has, like Great Britain, also implemented relatively restrictive measures. This is remarkable as the level of threat perception in Denmark was similar to that of the Netherlands. This means that other factors besides threat perception must play a role in determining the level of restrictiveness of counterterrorism measures.

One reason for this has been proposed by Meyer (2009). He argues that the fact that a society has had to deal with a terrorist attack might not be fully responsible for the state's threat perception. What can also influence future threat perceptions is the way in which this terrorist act was resolved and consequently how it is remembered in society's collective memory. For instance, if a terrorist attack was not large in scale but was not resolved successfully, meaning that the authorities did not respond unilaterally and with confidence, the effects of this small-scale act of terrorism might be far-reaching. This means that if the terrorist attack is remembered as a traumatic experience, future threat perceptions might still be high. The question then becomes not how "big" the act of terrorism was, but whether it has "hit home" (Meyer, 2009: 659). In the case of Denmark, this means that the Mohammed cartoons controversy might have impacted the collective memory more intensely than is expected at a first glance. If this is the case, and the cartoon controversy is indeed remembered as a traumatic experience, the restrictiveness of Denmark's counterterrorism measures might be explained.

Great Britain, on the other hand, has implemented restrictive measures in accordance with the relatively high threat perception that was observed in the past 14 years. It is probable that this is due to the extensive experience that Britain has with terrorism, especially with the Provisional Irish Republican Army and the London

bombings of 2005. After these episodes of large-scale terrorism, the question of whether or not the terrorist attacks have hit home is not per se relevant, as the extent to which the British population and governing elite have been exposed to terror is enough in itself to cause high threat perceptions. It is thus likely that, in the case of Great Britain, the vast experience with terrorism in addition to the close alliance with the U.S. and proactive foreign policy have contributed to the relatively high restrictions of the right to privacy as an effect of counterterrorism measures.

On the contrary, the Netherlands has, as was expected, not implemented any measures that are very restrictive of the right to privacy. Like Denmark, the country experienced a small-scale terrorist attack when filmmaker Theo van Gogh was assassinated, and as a consequence threat perceptions increased after this event. However, threat perceptions decreased fairly quickly again, and the effects on the restrictiveness of counterterrorism measures were very limited. It therefore seems that this act of terrorism did not have a very strong effect on the Dutch collective memory and was resolved in a manner that allowed the Dutch society to come out stronger.

Despite the fact that some differences were expected, the degree to which the restrictiveness of counterterrorism per country varies is quite high. Where Denmark and Great Britain have implemented a number of very restrictive measures, the Netherlands has implemented none. In addition, Denmark and Great Britain implemented more measures that are somewhat restrictive, whereas the Netherlands had a clear focus on preventive measures as opposed to repressive measures. This large gap is significant, because the three cases are similar in many ways. For instance, all three states are EU and UN members, and their counterterrorism framework is therefore for a large part based on the exact same overarching frameworks provided by these international institutions.

In order to explain this large variation, it is important to take into account other factors that might influence threat perceptions and their responses. For instance, the level of securitization that is present in the three countries could constitute an explaining factor. If political and institutional actors have an interest in securitizing the terrorist threat, meaning that political discourse revolves around the existential threat that terrorism poses, more restrictive measures could be justified and thus further the cause of these actors. Different levels of securitization can then explain the variation between the three states. Future research should point out whether this is in fact the case, or whether other factors that are so far unstudied influence different levels of threat perception and responses in the form of counterterrorism measures.

Conclusion

The results of this thesis partly point at a relationship between a state's threat perception and the restrictiveness of the counterterrorism measures that it implements. However, one obvious difficulty stands out in this type of research, and that is the high degree of sensitivity of the data that are used to observe restrictiveness in counterterrorism efforts. As is the case with many security issues, agencies that are responsible for the protection and well being of a state generally do not disclose any important information to the public. The same goes for controversial information: agencies are very reluctant to disclose any information that might cause uproar. Unfortunately, it is this type of information that is of interest for this thesis specifically and for human rights research in general. No state would want to be seen as a violator of fundamental human rights, but then again, no state would want to be responsible for a grave security breach either.

One example of the controversial nature of this topic is the ongoing debate between Britain's Government Communications Headquarters (GCHQ) and British and international human rights institutions, such as Liberty and Privacy International. In addition, UN and EU human rights commissions have expressed their concern regarding security practices (Omzigt, 2014; UN High Commissioner for Human Rights, 2013) These institutions have repeatedly accused the GCHQ of bulk interception and mass surveillance, which are both unlawful. These allegations were mostly based on Edward Snowden's revelations. GCHQ, on the other hand, has constantly denied such practices (IPT, 2014). This highlights the problematic nature of research on human rights and security concerns, as different institutions have entirely opposing interests. It also highlights the necessity for security and intelligence agencies around the globe to be as transparent as possible as regards their practices, so as to avoid misunderstandings and encourage counterterrorism frameworks that enhance both accountability and efficacy.

Literature

Arnoldussen, Tobias. 2009. "Deus sive Natura: Investigating the Axioms of Precautionary Logic", in eds. M. Hildebrandt, A. Makinwa and A. Oehmichen, *Controlling Security in a Culture of Fear*, The Hague: Boom Legal Publishers.

Baumann, Zygmunt. 2006. *Liquid Fear*, Cambridge: Polity Press.

Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*, London: Sage Publications.

Bigo, Didier and Elspeth Guild. 2007. "The Worst-Case Scenario and the Man on the Clapham Omnibus", in eds. Benjamin J. Goold and Liona Lazarus, *Security and Human Rights*, Portland: Hart Publishing.

Buhelt, Anders Folmer. 2012. "Policing the Law of Fear?", in eds. Barbara Hudson and Synnøve Ugelvik, *Justice and Security in the 21st Century: Rights, Risks and the Rule of Law*, New York: Routledge.

Buzan, Barry, Ole Waever and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*, London: Lynne Rienner.

Fredman, Sarah. 2007. "The Positive Right to Security", in eds. Benjamin J. Goold and Liona Lazarus, *Security and Human Rights*, Portland: Hart Publishing.

Furedi, Frank. 2008. "Fear and Security: A Vulnerability-Led Policy Response", *Social Policy and Administration*, 42(6): 645-661.

Gibson, James L. 1998. "A Sober Second Thought: An Experiment in Persuading Russians to Tolerate", *American Journal of Political Science*, 42(3): 819-850.

Goold, Benjamin J. and Liona Lazarus. 2007. *Security and Human Rights*, Portland: Hart Publishing.

Hudson, Barbara. 2003. *Justice in the Risk Society*, London: Sage Publications.

Hudson, Barbara and Synnøve Ugelvik. *Justice and Security in the 21st Century: Risks, Rights and the Rule of Law*, New York: Routledge.

Ilardi, Gaetano Joe. 2009. "Irish Republican Arm Counterintelligence", *International Journal of Intelligence and Counterintelligence*, 23(1): 1 – 26.

Lazarus, Liona. 2007. "Mapping the Right to Security", in eds. Benjamin J. Goold and Liona Lazarus, *Security and Human Rights,* Portland: Hart Publishing.

Locke, John. 1960. *Two Treatises of Government*, ed. Peter Laslett. Cambridge: University Press.

Lomell, Heidi Mork. 2012. "Punishing the Uncommitted Crime: Prevention, Pre-Emption, Precaution and the Transformation of Criminal Law", in eds. Barbara Hudson and Synnøve Ugelvik, *Justice and Security in the 21st Century: Risks, Rights and the Rule of Law*, New York: Routledge.

Meyer, Christoph O. 2009. "International Terrorism as a Force of Homogenization? A Constructivist Approach to Understanding Cross-National Threat Perceptions and Responses", *Cambridge Review of International Affairs*, 22(4): 647-666.

Mitsilegas, Valsamis. 2012. "Security vs Justice: the Individualisation of Security and the Erosion of Citizenship and Fundamental Rights", in eds. Barbara Hudson and Synnøve Ugelvik, *Justice and Security in the 21st Century: Risks, Rights and the Rule of Law*, New York: Routledge.

Muller, Erwin. 2003. "The Netherlands: Structuring the Management of Terrorist Incidents", in ed. Marianne van Leeuwen, *Confronting Terrorism: European Experiences, Threat Perceptions and Policies*, Den Haag: Kluwer Law International.

Murphy, Cian C. 2012. *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law*, Oxford: Hart Publishing.

Stein, Janice Gross. 2013. "Threat Perception in International Relations", in eds. Leonie Huddy, David O. Sears and Jack S. Levy, *The Oxford Handbook of Political Psychology*, 2nd ed. Oxford: Oxford University Press.

Van Leeuwen, Marianne. 2003. *Confronting Terrorism: European Experiences, Threat Perceptions and Policies*, Den Haag: Kluwer Law International.

Walker, Clive. 2003. "Policy Options and Priorities: British Perspectives", in ed. Marianne van Leeuwen, *Confronting Terrorism: European Experiences, Threat Perceptions and Policies*, Den Haag: Kluwer Law International.

Zedner, Lucia. 2012. "Seeking Security by Eroding Rights: the Side-Stepping of Due Process", in eds. Benjamin J. Goold and Liona Lazarus, *Security and Human Rights*, Portland: Hart Publishing.

Online Sources

Bigo, Didier et al. 2013. "National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law", *Policy Department for Citizens Right and Constitutional Affairs*, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf

Centre for Terror Analysis (CTA), 2015. "Threat assessment", https://www.pet.dk/English/CenterforTerrorAnalysisCTA/Threat%20assessment.aspx

Committee of Experts on Terrorism (CODEXTER). 2007. "Denmark", *Profiles on Counterterrorist Capacity*,

http://www.coe.int/t/dlapil/codexter/Source/country_profiles/CODEXTER%20Profiles%20(2007)%20Denmark%20E.pdf

Committee of Experts on Terrorism (CODEXTER). 2007. "United Kingdom", *Profiles on Counterterrorist Capacity*, http://www.coe.int/t/dlapil/codexter/4_theme_files/Country_Profiles/CODEXTER%20Profiles%20(2007)%20UK%20E.pdf

Committee of Experts on Terrorism (CODEXTER). 2008. "The Netherlands", *Profiles on Counterterrorist Capacity*, http://www.coe.int/t/dlapil/codexter/4_theme_files/Country_Profiles/CODEXTER%20Profile%20(2008)%20NETHERLANDS.pdf

Council of the European Union, 2002. Council Framework Decision 2002/475/JHA, *Office Journal of the European Union*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Council of the European Union. 2005. *The European Union Counter-Terrorism Strategy*, http://www.statewatch.org/news/2005/nov/eu-counter-terr-strategy-nov-05.pdf

Counter-Terrorism Committee. 2015. "Our Mandate", http://www.un.org/en/sc/ctc/

Court of Justice of the European Union (CJEU). 2014. "The Court of Justice Declares the Data Retention Directive to be Invalid", *Press Release No 54/14*, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Drennan, Justine. 12-11-2014. "Who Has Contributed What in the Coalition Against the Islamic State?", *Foreign Policy*, http://foreignpolicy.com/2014/11/12/who-has-contributed-what-in-the-coalition-against-the-islamic-state/

Eijkman, Quirine, Doutje Lettinga and Gijs Verbossen. 2012. "Impact of Counter-Terrorism on Communities: Netherlands Background Report", *Institute for Strategic Dialogue*, http://www.strategicdialogue.org/Netherlands_FINAL.pdf

Electronic Frontier Foundation (EFF), 2014. "Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance", via *Office of the High Commissioner for Human Rights*, http://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf

European Court of Human Rights (ECHR). 2010. *European Convention on Human Rights*, http://www.echr.coe.int/Documents/Convention_ENG.pdf

European Union. 1995. "Directive 95/46/EC", *Office Journal of the European Union,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

European Union. 2006. "Directive 2006/24/EC", *Office Journal of the European Union*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

Folketinget, 2013. *The Constitutional Act of Denmark*, http://www.thedanishparliament.dk/Publications/~/media/Pdf_materiale/Pdf_publikationer/English/The_constitutional_act_of_denmark_2013.pdf.ashx.

Intelligence and Security Committee of Parliament (ISC), 2015. "Privacy and Security: a Modern and Transparent Framework", http://isc.independent.gov.uk/news-archive/12march2015

Investigatory Powers Tribunal, 05-12-2014. "IPT Rejects Assertions of Mass Surveillance", http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/IPT-rejects-assertions-of-mass-surveillance.aspx

Liberty, 2015. "State Surveillance", *Human Rights*, https://www.liberty-human-rights.org.uk/human-rights/privacy/state-surveillance

Lindekilde, Lasse and Mark Sedgwick. 2012. "Impact of Counter-Terrorism on Communities: Denmark Background Report", *Institute for Strategic Dialogue*, http://www.strategicdialogue.org/Country_report_Denmark_AD_FW.pdf

May, Theresa. 2015. "CONTEST: The United Kingdom's Strategy for Countering Terrorism: Annual Report for 2014", *Presented to Parliament by the Secretary of State of the Home Department*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415708/contest_annual_report_for_2014.pdf

Ministry of the Interior and Kingdom Relations. 2008. *The Constitution of the Kingdom of the Netherlands*, http://www.government.nl/documents-and-publications/regulations/2012/10/18/the-constitution-of-the-kingdom-of-the-netherlands-2008.html

Morris, Nigel. 14-02-2008. "The Big Question: Why Does the UK Not Have a Written Constitution, and Does it Matter?", *The Independent Online*, http://www.independent.co.uk/news/uk/politics/the-big-question-why-doesnt-the-uk-have-a-written-constitution-and-does-it-matter-781975.html.

National Coordinator Counterterrorism and Security (NCTV). 2011. "National Counterterrorism Strategy",

https://www.counterextremism.org/resources/details/id/584/national-counter-terrorism-strategy-2011-2015

National Coordinator for Counterterrorism and Security (NCTV), 2015. "Current Threat Level", https://english.nctv.nl/themes_en/Counterterrorism/terrorist_threat_assessment_netherlands/current_threat_level/

Opstelten, Ivo. 12-11-2014. "Dreigingsbeeld Terrorisme Nederland 37 en Beleidsbevindingen", *Nationaal Coordinator voor Terrorismebestrijding en Veiligheid*, https://www.nctv.nl/onderwerpen-a-z/dtn.aspx

Pew Research Center. 2011. *Muslim Population by Country*, http://www.pewforum.org/2011/01/27/table-muslim-population-by-country/.

Rijksoverheid. 02-12-2013. "Dessens Committee: Intelligence and Security Services Act has to be adjusted", *News*, http://www.rijksoverheid.nl/nieuws/2013/12/02/commissie-dessens-wet-op-de-inlichtingen-en-veiligheidsdiensten-moet-worden-aangepast.html.

Security Council Counter-Terrorism Committee (CTC). 2015. "Our Mandate", http://www.un.org/en/sc/ctc/

Security Service (MI5), 2015. "Threat Levels", https://www.mi5.gov.uk/home/about-us/what-we-do/the-threats/terrorism/threat-levels.html

Søvndal, Villy. 2012. "Government Report on Counter-Terrorism Efforts", *The Danish Government*, http://usa.um.dk/en/~/media/USA/Simon%20PDK%20praktikant%20E14/Terrorredegoerelse%202012%20ENGashx.pdf

United Nations General Assembly. 1948. "Universal Declaration of Human Rights", http://www.un.org/en/documents/udhr/

United Nations General Assembly. 2006. "United Nations General Assembly Adopts Global Counter-Terrorism Strategy", *United Nations Actions to Counter Terrorism*, http://www.un.org/en/terrorism/strategy-counter-terrorism.shtml

United Nations High Commissioner for Human Rights. 2013. "The Right to Privacy in the Digital Age", *Human Rights Council*, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

United Nations Security Council. 2001. "Resolution 1373", http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1373(2001).

United Nations Security Council. 2005. "Resolution 1624", http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1624(2005).

Watt, Nicholas. 14-03-2012. “Barack Obama: US-UK Alliance One of the Greatest Ever Known”, *The Guardian Online*, http://www.theguardian.com/world/2012/mar/14/barack-obama-uk-us-alliance

Worland, Justin. 26-09-2014. “3 More Countries Join Coalition Against ISIS”, *Time Magazine Online*, http://time.com/3433346/isil-isis-uk-belgium-denmark/

Zenger, Rejo. 2015. “Data Retention Law Struck Down – For Now”, *Bits of Freedom*, https://www.bof.nl/2015/03/11/data-retention-law-struck-down-for-now/