Master Thesis

Europol Policing the Web

Internet Content & Counter-Radicalization – An Interpretive Policy Analysis Approach

Author: Kilian Vieth

Otto-Suhr-Institut | FU Berlin
Dual degree program | Political Science & European Affairs

First supervisor: Prof. Dr. Ursula C. Schröder
Second supervisor: Dr. Ben Wagner

Submission date: 3.09.2016

Word count: 21,106

Table of Contents

For Wutz.

I. Introduction

1. Topic and Research Question

Europol's Internet Referral Unit (EU IRU) makes recommendations to internet industry players for take-down of online content. This body monitors online material, assesses it, and asks hosting platforms to remove content that Europol regards as inappropriate. Basically, the unit tries to draw attention to activities that may breach the commercial terms of service of social media platforms, not laws. The EU Internet Referral Unit was created in the context of European counter-terrorism policy and began operations in 2015.

The EU IRU is the main subject of this thesis, explored in the greater context of transnational law enforcement operations and the privatized governance of online media. Where is the connection between countering terrorism and filtering and removing of internet content? Is the unit's policy merely a symbolic one? This research project dismantles the discursive practices underlying the EU IRU – with the aim of understanding the (in)security dynamics of online (counter-)radicalization and assessing the related human rights issues – by addressing the following research question:

How does Europol frame radicalization and internet content?

This paper's theoretical and empirical discussion engages with the threat construction behind the EU IRU and examines why and how filtering internet content has become 'normal' practice in European counter-terrorism policy. I have located the EU IRU within the wider discourse on counter-radicalization and contend that we need to better understand the meaning of security and security-related concepts – such as radicalization – used by professionals working in the field.

What assumptions and what ideas underlie the transformation of European policing and police co-operation? Are these assumptions and ideas potentially damaging or politically dangerous? This master's thesis focuses on referral and take-down practices and only parenthetically touches upon other forms of law enforcement operations on the internet, such as open intelligence gathering and the investigation of criminal networks on social media.

This thesis follows an interpretive research design. It begins with a brief summary of the academic and political relevance of the topic. This is followed by a theoretical discussion of a

practice-oriented approach to security and counter-terrorism that addresses the starting point of my discussion of countering (online) radicalization. The central concept – radicalization – is explained and criticized. The critique of this term combines normative and human rights-based arguments with academic criticism. This discussion is linked to a consideration of the role of the internet in countering violent political extremism online. This theory part of the paper is followed by an integrated account of my interpretive research design, that outlines the methodology and methods applied in this study. The subsequent policy analysis proceeds in two parts. Firstly, the activities of the EU IRU and the political context are scrutinized in great detail. Secondly, this thesis delineates how Europol frames its internet referral operations by focusing on terrorism, radicalization, the role of technology, and references to Islam. This empirical analysis of the concepts underlying Europol policy also scrutinizes the broader significance and priorities of Europol's policy solutions. The main conclusion of this thesis is that the EU IRU is rooted in a flawed and ineffective understanding of radicalization. The concluding remarks concern the relationship between the symptoms and root causes in counter-terrorism policy and critically engage with the rising corporatocracy structures involved in the regulation of online content.

2. Political and Academic Relevance

In a 2008 interview, Facebook CEO Mark Zuckerberg said that social media can act as a means of fighting terrorism because it connects people with one another. Terror, he suggested, does not emerge "out of a deep hatred of anyone, it comes from a lack of connectedness, a lack of communication, a lack of empathy, and a lack of understanding" (Zuckerberg, quoted in Packer 2013). Zuckerberg portrayed the social exchanges that platforms like Facebook can provide as a force for social good that has the power to broaden perspectives and open up users' minds – hence making terror less likely. It is startling how out of place this idea seems today, as pundits currently argue precisely the opposite, highlighting the 'radicalizing function of the internet' and the 'abuse of social media' by terrorists.

This subject is of political interest because it entails a number of human rights concerns, ranging from freedom of speech to freedom of association and assembly. Jillian York, Director of Freedom of Expression at the Electronic Frontier Foundation, says that "social media companies have an abysmal track record when it comes to regulating any kind of speech" (York 2016). Over-blocking of content, failing to provide paths to recourse, and a

complete absence of due process are just a few of the problems that arise when social media companies act as arbiters of human rights[1]. The former UN Special Rapporteur on Freedom of Expression has also stressed the importance of official judicial intervention and transparent procedures in the regulation of internet content and emphasized that "there must be effective remedies for affected users, including the possibility of appeal" (la Rue 2011, 21).

Studies have also demonstrated the power of social media to influence human behavior in various ways (Bond et al. 2012; Kramer, Guillory, and Hancock 2014). Countering radicalization on the internet raises vast ethical concerns due to the enormous power leveraged by technology. The way in which law enforcement and social media platforms cooperate is therefore relevant to the general public. A better understanding of the reasoning behind the EU IRU is needed in order to address these human rights concerns.

Linking radicalization to digital communication is a relatively new development. In recent policy documents and media articles, internet content has been increasingly cited as key means of disseminating political propaganda and recruiting fighters. The terms radicalization, extremism, violent extremism and Islamism are often confused with one another and loaded with different meanings and functions in the context of these discussions. However, being radical or holding radical beliefs does not constitute a crime, nor is it necessarily negative or harmful. Nonetheless, law enforcement targets individuals and groups that demonstrate certain behaviors or make certain statements – which places serious restrictions on the right to free speech. We consequently have to analyze what 'radicalization on the internet' means and how this concept affects policy, as the current popular narrative is likely to dominate public discourse, research, and policy agendas for years to come.

The EU IRU represents one specific case in the broader discourse on (counter-)radicalization in security politics. This unit is concerned with the emerging constellation of public and private actors cooperating to regulate expression online in the name of counter-terrorism. As such, the unit's activities can be contextualized within the growing debate on countering violent extremism online[2], focusing on one approach out of a broad range of counter-radicalization measures.

Studying Europol brings together patterns from security studies, such as the privatization of security, the blurring of internal and external security spheres, and the merging of intelligence and policing practices. This practice-oriented interpretive study deals with knowledge

1 https://onlinecensorship.org/news-and-analysis (last retrieved 13 July 2016)
2 http://www.voxpol.eu/ (last retrieved 12 July 2016)

production and the policy framing of new governance mechanisms to regulate internet content. It ultimately tries to encourage searching for better concepts and understandings of (in)security.

The EU Internet Referral Unit is an interesting case to explore in the context of ongoing discussions on law enforcement operations combating propaganda as well as privatized regulation of speech. The public/private cooperation between the European Police Office and social media corporations is a relatively new phenomenon. Since recent developments have not yet been studied in greater detail, I would like to contribute to critical discussions on counter-terrorism policy in Europe by concentrating on the sense-making behind one specific policy that was implemented during 2015, namely the EU IRU.

II. Theoretical Approach

1. Performing (In)Security – Practices and Professionals

This first chapter outlines a few foundational concepts that inform my empirical frame analysis, case selection, and research design. The theoretical discussion below combines the relational and meaning-centered concepts that provide the backdrop for the empirical research I conducted.

1.1. The International Political Sociology of Policing 'Terror'

Over the past few decades, a large body of literature has discussed the blurring of divides that traditionally used to demarcate divisions within the field of international security studies. New theoretical conceptualizations of what security is and how it comes about have emerged (Bigo 2000; Bigo 1996; Daase 2010; Buzan, Wæver, and de Wilde 1998; C.A.S.E. Collective 2006). For instance, the de-differentiation of domestic and foreign security is one of those boundaries that has been vanishing. The blurring of the divide between the external and internal dimensions of security has fundamentally reshaped the way in which security is understood. Threat constructions converge towards global insecurities and security professionals develop global interconnected networks – two developments that significantly alter the notions of defense, war and policing (Bigo 2008). Security has become a de-territorialized and potentially unlimited concept, linked to a broad range of political struggles. The European Police Office (Europol) is one of the transnational security actors heavily involved in the changing field of security, both as a driver and a symbol of change. This agency represents the transformation of statehood and the increasing interconnectedness of European security production (Bigo et al. 2007). It is hard to define precisely *where* Europol is active in terms of territorial location. Some of the agency's departments, such as the European Cyber Crime Centre (EC3) and the EU IRU, claim to operate in 'cyberspace.' Beyond all the imprecise and misleading connotations that this term entails[3], this claim illustrates the fact that Europol's operations transcend not only the borders between EU Member States, but also the border between the EU and the rest of the world.

Ensuring the security *of* a certain group always implies the need for security *from* some outside threat. In the face of transforming security architectures, the promise of security

3 For an in-depth discussion of the 'cyberspace' metaphor see Graham (2012) and Hansen and Nissenbaum (2009).

necessarily entails the production of insecurity for the out-group – a dilemma inherent to the concept of security. Threats are socially constructed through "boundary-creating processes" that use symbols and social enemies to label deviant out-groups (Tsoukala 2008). Many eloquent metaphors have been used to describe the interplay between security and discrimination, ranging from David Lyon's famous "social sorting," to the separation of the "risky" from the "at risk" (Edkins and Pin-Fat 2004). These metaphors all try to capture the visible and invisible political violence that is inscribed in the many practices of (in)securitization.

I will therefore use (in)security as an inherently ambivalent term in order to avoid ontological security frames which employ 'objective' understandings of security. Security is often taken as a given – a 'natural' – concept linked for example to individual safety. From a analytical standpoint, such a definition security is of limited conceptual value, at least within a constructivist theoretical framework. The research design of my inquiry is based on a *relational* conception of (in)security, following Didier Bigo, whereby security and insecurity are produced simultaneously through discursive practices. This in turn assumes that in order to understand (in)security, we do not need new definitions of security, but rather a better understanding of (in)securitization processes.

The Paris School of critical security studies – similar to the "practice turn" in international relations (Pouliot 2008; Adler and Pouliot 2012) – conceptualizes (in)securitization processes based on transnational practices of (in)security. This approach, also known as 'international political sociology,' borrows Bourdieu's theoretical vocabulary – including concepts such as 'practice,' 'field,' and 'habitus' – to set forth a relational theory of (in)security (Bigo 2011, 234ff). The Paris School represents a shift away from the existential threat-based securitization model developed by the Copenhagen School (Buzan, Wæver, and de Wilde 1998) and emphasizes the importance of communities of (in)security professionals for (in)securitization processes. This school adopts a sociological perspective to study the professional everyday routines of (in)security production instead of a narrowly defined speech act theory that concentrates on the political appeal of existential threats (Bigo 2011; Bigo 2006; Balzacq et al. 2010). That said, this practice-based orientation does not oppose the study of language per se, but rather regards knowledge production as one of multiple practices. This approach goes beyond the mere examination of politicians' speech acts and emphasizes the role of working-level professionals for the production of discourse on (in)security. The practice-based theory of (in)security justifies why researching the

knowledge production of everyday (in)security practitioners might be more informative than studying the speech acts of political elites.

Bigo's adoption of Bourdieu's theoretical discussion inspired me to search for discourses, social practices, communities of professionals and routine processes of knowledge production in European (in)security. The fact that (in)securitization extends beyond speech acts does not, however, imply that everything can be securitized. Bigo et al. suppose that mobilizing security substantially concerns producing of truth and prioritizing threats by publishing threat models, crime statistics, risk assessments, strategic plans, and analytical reports, which only security professionals have the authority to do (Bigo 2000, 194). The mere linguistic power to proclaim a security threat is not sufficient to ensure securitization, Bigo argues; the social position of the professional making the statement is equally important. Professionals of security are able to frame the discourse about security due to their authority, which needs to be recognized by the other social actors in the field (ibid., 176). The process of (in)securitization cannot be considered to be independent of "a field of security constituted by groups and institutions that authorise themselves and that are authorised to state what security is" (ibid., 195). By assembling and categorizing data through 'technological routines,' (in)security professionals form "a 'field' of security in which they recognize themselves as mutually competent" (Bigo 2008, 8). Different groups have different stakes (e.g. following political and bureaucratic reasoning) in the power struggle over the definition of the term 'security':

> While politicians may seek to strengthen their position [...] by opposing themselves to the social enemies of the day, security professionals may associate their preventive and coercive policies with budget claims and/or the ongoing repositioning of their agencies in the security field (Tsoukala 2008, 141).

De-differentiation of security spheres does not equate to the homogenization of (in)security practices. Urban police, riot police, customs officials, and border control guards have different interests and experiences that do not add up to one holistic logic of security. My empirical analysis follows the Paris School approach by focusing on the work conducted by an (in)security agency consisting of police and intelligence professionals. Europol occupies a unique position in the field of European (in)security in that it seeks to advance its own competences and resources, yet relies upon cooperation with EU Member States' security agencies. Examining the knowledge that Europol contributes to the "regime of truth" (Bigo 2008, 9) around internet content and terrorism is helpful in theorizing of practice-oriented approaches to European (in)security.

1.2. The Logic of Preventing Risk and Countering Radicalization

Emanating from the Paris School approach of (in)security, a brief discussion of the logic of prevention in modern counter-terrorism policy provides the analytical starting point for Europol's sense-making processes regarding internet content and (counter-)terrorism. Radicalization is the key concept analyzed in the context of the EU IRU. Where does the idea of radicalization come from and what does it actually mean? The development of radicalization as a concept is linked to the future-oriented policing approach under the paradigm "prevention is better than cure" (Elshimi 2015, 111). Especially in counter-terrorism policy – but also in many other (in)security sectors – the logic of risk prevention has been one of the most persistent reasons behind the creation of anticipatory measures to reduce the likelihood of violent attacks. Martin-Mazé and Burgess write: "Preventing harm through threat anticipation is, indeed, the foremost rationale underpinning current counter-terrorist frameworks" (2015, 105). This prevention rationale makes it necessary to act upon forecasts, which entails creating suspicion instead of investigating suspicion. Modern preventive counter-terrorism policy trades instruments of repression against instruments of pro-activity (Bigo and Tsoukala 2008).

Marieke de Goede suggests calling this phenomenon "precautionary" or "anticipatory" rather than preventative, because prevention addresses risks that are statistically knowable, whereas irregular events that occur in small numbers – such as terrorist attacks – "are irregular, incalculable, and, in important ways, unpredictable" (de Goede 2011, 9). Policing is increasingly detached from concrete dangers and individual behavior, and is based instead on probabilistic evidence. Looking for specific suspicious persons has been replaced by looking for types of people, groups that are statistically calculated based on allegedly impartial criteria (Krasmann 2006, 240f). Risk technologies produce depersonalized themes that depoliticize (in)security by invoking quantified types of knowledge (Hagmann and Cavelty 2012, 81). Such typification has to be analyzed from a relational perspective, taking into account the performative function of knowledge production. Anticipatory (in)security practices govern preemptively, in the sense that they do not act upon, but change the subject matter (de Goede and Simon 2013). Amoore and de Goede have argued that modern risk management is in many ways "the banal face of the preemptive strike" (2008, 14). They build upon the work of Judith Butler to conceptualize the performativity of risk for (in)security, assuming that the concept of risk produces the very phenomenon that it names. Risk-driven (in)security policy tries to manage threats based on predictions about the future. That is why,

in the words of Richard Ericson and Aaron Doyle, “Terrorism strikes at the foundation of risk society because it is a stark reminder of the limits to risk assessment and management” (2004, 141). A fully knowable future remains an illusion that many risk technologies try to gloss over in the search for perfect (in)security, adopting illiberal policies in the process.

In the following section, the scholarship on radicalization’s origins, meanings, and discursive functions is presented as the most striking concept underlying preemptive counter-terrorism policy. The debate on risk prevention leads us to three critical questions that need to be addressed: Does counter-radicalization as a counter-terrorism measure depend on biased assumptions about race and vulnerability to extremism? What assumptions about causality and risk are made in this context? And is the policing of cognitive radicalization a legitimate strategy in liberal democratic regimes?

2. Analyzing Radicalization – Concept and Critique

Radicalization has become the primary narrative used to make sense of terrorism and design counter-terrorism policy. The present EU strategy on countering terrorism contains a subprogram on combating radicalization, violent extremism, and recruitment to terrorism (Council of the EU 2014). Arun Kundnani argues that, immediately after the 9/11 attacks, terrorism was mainly identified as the result of bare hatred and fanaticism. Numerous commentators regarded requests to investigate the root causes of the attacks as attempts to justify the mass murder of innocent human beings. The terrorists were framed as purely evil, incorrigible individuals whose actions had no political context. This led to the conclusion that “only overwhelming force would be successful against this new enemy,” which led to the war in Afghanistan and Iraq and the establishment of Guantánamo (Kundnani 2014, 14). This counter-terrorism policy founded on violent retaliation turned out to be deficient. The subsequent attacks in Madrid and London and the failing military campaign in Iraq helped to surface radicalization as a new way to guide counter-terrorism policy. Radicalization became the vehicle that made it possible to talk about the causes of terrorism, broadening counter-terrorism efforts beyond the “killing and capturing” approach, shifting priorities towards “winning hearts and minds” (Kundnani 2014, 15). However, radicalization emphasizes the individual and de-emphasizes the social and political circumstances, which often causes the radical to look like a rebel without a cause (Sedgwick 2010, 480f).

The upswing of radicalization was mirrored by an increase in academic research on

radicalization, as Kundnani demonstrates (2014, 18). Although radicalization is by no means a new concept, the increase in research on radicalization since around 2004 is remarkable. Over the last ten years, most of the literature on radicalization has been published in the fields of security and counter-terrorism studies. This concept "has burst onto our screens and political agendas [...] replacing decades of social movement research into the contextual and political factors which inform the turn towards clandestinity within groups and movements" (Heath-Kelly, Baker-Beall, and Jarvis 2014, 1). This older strand of social movement research is associated with scholars such as Crenshaw (1981) and della Porta (1992), who highlighted how terrorist groups can develop out of wider social movements by exploiting organizational dynamics. These researchers studied the relationships between terrorism, political opportunity structures, and contextual factors such as poverty, regime types and disenfranchisement.

Whether or not radicalization 'actually' exists is not a very relevant question in this context, because it is a socially constructed concept. Individuals may or may not undergo a process of radicalization, but media, state, and academia have decided to use this term to describe "what goes on before the bomb goes off" (Sedgwick 2010, 479; Neumann 2008, 4). In a way, radicalization exists because we collectively say it does. Hence, it appears to be more fruitful to develop a better understanding of what radicalization means in different situations, rather than asking whether it 'actually' exists.

How is radicalization understood today? Even terrorism studies literature acknowledges that there is no universally accepted definition of the term; nevertheless, there seems to be a general consensus that radicalization poses a threat (Heath-Kelly 2013, 398; Richards 2011, 143). Generally speaking, the concept of radicalization assumes that individuals can be radicalized and that this process may lead to violence:

> [T]he terms 'radicalisation', 'radicalise' and 'radical' are employed in a way that suggests they are self-evident concepts. Even worse, the terms are often used in a circular fashion: a radical is someone who has radical ideas or who has been radicalised (Nasser-Eddine et al. 2011, 13).

This in turn gives rise to criticism that radicalization is an "essentially contested concept" (Heath-Kelly, Baker-Beall, and Jarvis 2014, 6) because it is inherently political and incorporates ideological elements that make it impossible to define based on empirical evidence – no 'neutral' definition of radicalism is possible. Studying the framing of radicalization on the working level of Europol law enforcement is an insightful approach

because it allows to unwrap how the everyday meaning of radicalization is (re)shaped by (in)security practitioners. For example, the European Commission distinguishes between violent and non-violent radicalization in its strategy papers, while a high-level expert group at the European Commission frames radicalization as a socialization process (ENER 2008). It matters who uses the word – and under what circumstances – because different groups of professionals set different priorities.

In the current counter-terrorism discourse, the initial conception of radicalism has been replaced by the idea that radicalization involves a shift from moderation to extremism (Githens-Mazer 2012, 556). Addressing radicalization is generally presented as the wiser, more nuanced and thoughtful approach to counter-terrorism, and is readily embraced by policymakers and law enforcement officials. Governments are eager to find out what turns a person into a terrorist, and radicalization – stemming from the Latin word radix for root – appears to provide exactly the right framework for obtaining this information. Neumann distinguishes between two main types of radicalization, with different consequences for policy frames. He speaks of *cognitive radicalization*, which focuses on radical thinking, holding radical beliefs and following radical ideologies. He also identifies *behavioral radicalization* which considers engaging in violent action to be the relevant constitutive end-point that defines radicalism. As such, behavioral radicalization stipulates that actions, not thoughts, define the state of being radical (Neumann 2013, 874ff). This conceptual differentiation gives rise to two corresponding models of counter-radicalization. Neumann labels tackling behavioral radicalization as the "Anglo-Saxon approach," and categorizes targeting cognitive radicalization as the "European approach" to countering radicalization. Of course, the European approach does not ignore radical behavior to exclusively focus on cognitive radicalism; instead, it rather deals with both cognitive and behavioral radicalization. However, Neumann's distinction between the two approaches is based on the emphasis of radical beliefs inherent to the European approach to counter-radicalization.

The EU IRU fits the 'European approach' as defined by Neumann: Monitoring and censoring online content can only be justified by tackling cognitive radicalization. A consequentialist frame of expected consequences (Eroukhmanoff 2015) that draws a direct connection between radical speech and radical actions must be applied. After all, without assuming causality between radical thinking and radical actions, filtering and removing material from the internet does not make sense.

The biggest issue with tackling cognitive radicalization is the inherent chilling effect this

approach has on free speech (Eroukhmanoff 2016, 2). If radicalization starts with holding radical beliefs, this may place strong limits on the fundamental right to freedom of expression. Policing cognitive radicalism – that is, radical ideas – falls outside of the traditional realm of liberal legal frameworks that (mostly) criminalize actions, not ideas. Being radical is not a crime in liberal democracies – or, at least, it should not be, because it is vital to democracy (cf. Neumann 2013, 892). Radical thinking has often led to positive change, or, as Rik Coolsaet puts it: "Most democratic states would not exist but for some radicals who took it upon themselves to organise the revolt against a foreign yoke or an autocratic regime" (2011, 260). Radicalism is essentially a question of standpoint; many ideas are radical at some point in history, but become mainstream over time (and vice versa). Women's right to vote used to be a radical claim a century ago, but is uncontested today in Western society. The civil rights movement in the United States also fought for 'radical' demands, but is now celebrated for the positive social change it brought about. On the contrary, National Socialism was mainstream in Germany in the 1930s and 1940s, but is regarded as radical today. In many ways, descriptions of what is 'extreme' or 'radical' tell us more about the dominant mainstream of the society in which these descriptions are assigned than about the groups deemed radical. Being radical or extreme is always a relational term that entails narratives of identity. Following Said's theory of orientalism, constructing an identity depends on the depiction of a negative 'other' that serves as a mirror and antipode of the self (Said 2012). Radicalism is one of the frames that shapes counter-terrorism policy by, often implicitly, defining a certain social identity. Creating otherness traces the problem to an obscure socialization process that must have happened outside of 'mainstream' society, thereby conveniently absolving the hegemonic part of society of responsibility and taking Western nations out of the equation. The place in which a state searches for the cause of a problem often tells you much more about said state than it does about said problem. For example, after leading RAF member Ulrike Meinhof committed suicide in prison in 1976, investigators examined her brain to find physical clues as to her radicalization (Kundnani 2014, 14). An approach that tacitly frames the desire to engage in political violence as pathological, not political.

One crucial line of criticism of the concept of radicalization rests upon the unsatisfactory scientific foundation of the term. Although "[r]adicalization is one of the great buzzwords of our time" (Neumann and Kleinmann 2013, 360), the body of evidence substantiating popular claims made about radicalization is relatively meager. In their review of empirical research

on radicalization published between 1980 and 2010, Neumann and Kleinmann found that there are significant empirical and methodological shortcomings in the field of radicalization research (2013).

Arun Kundnani has voiced a corresponding criticism of research results, questioning their explanatory power, because they often take correlation for causality. Kundnani specifically criticizes several prominent studies that he considers to be the most influential benchmarks of recent radicalization research, namely those by Wiktorowicz (2005), Sageman (2008), and Gartenstein-Ross and Grossmann (2009). Firstly, he criticizes the scientific quality of the research designs, which are marred by errors such as biased case selection, missing control groups, and failure to consider important intervening variables. He questions whether some of the 'terrorists' that are part of the studies could also be seen as 'radical activists.' Secondly, he provides a powerful normative critique of these studies, arguing that they use ill-defined and misleading terminology and ignore the political consequences of their publication. Most importantly, Kundnani highlights the detrimental effects of the association of radicalization with Islam, saying that these poorly designed studies have been very influential among law enforcement agencies: "In the hands of the NYPD, Sageman and Wiktorowicz's radicalisation scholarship becomes a prospectus for mass surveillance of Muslim populations" (Kundnani 2014, 29). The typical problem with most mainstream radicalization research is that it uncritically takes individuals holding radical religious beliefs as a cause for violence. Githen-Mazer and Lambert agree with Kundnani that radicalization research is dominated by conventional wisdom and frequently grounded in assumptions and intuition (Githens-Mazer and Lambert 2010, 889). Gill and his colleagues present similar findings for inquiries into online radicalization, which reveal a "striking lack of data" and regularly make "unempirical" claims (2015, 5f). This is irresponsible, since it contributes to alienating the Muslim community and unduly extends the suspect community and the suspect space.

The association of radicalization with Islam has become an unavoidable truth in mainstream scholarship on radicalization. Explanations produced by radicalization researchers since 2000 often favor ideology and religion as prevailing elements of radicalism. Political circumstances such as structural injustice or even personal anger are regularly disregarded. Attributing vulnerability to othered communities puts the burden of constant suspicion on a constructed out-group of society, creating insecurity for said group. The decontextualization of radical thinking and action overrides scientific distance and tends to oversimplify the subject matter. The sociologist Olivier Roy recently stated that this phenomenon is "not, then,

the radicalization of Islam, but the Islamization of radicalism" (Roy 2016).

Conceptions of vulnerability (to be radicalized) pathologize dissent – specifically, Muslim dissent (Heath-Kelly 2013, 404; Richards 2011, 150f). Heath-Kelly and colleagues sharply criticize this:

> Counter-terrorism has invented a feedback loop between vulnerability and ideology to explain away the resurgence of violence in the supposed heartlands of liberty, democracy and equality (Heath-Kelly, Baker-Beall, and Jarvis 2014, 2).

Many radicalization researchers do not seem to consider the possible detrimental political consequences of the publication of their work. There are, of course, remarkable exceptions to this, such as the recent attempt to formulate a relational approach to radicalization (Alimi, Demetriou, and Bosi 2015). Nonetheless, the prevailing conventional wisdom on radicalization assumes causality where there might be none and ignores impractical and complicated factors like social exclusion, economic hardship, and foreign policy. Both radicalization research and counter-radicalization policy willfully act upon the idea that targeting suspect communities instead of individuals might make it possible to prevent future attacks. In doing so, they perpetuate the new orthodoxy for explaining and responding to political violence. Radicalization has become a powerful instrument that serves to divide and control Muslim communities in the name of counter-terrorism (Githens-Mazer and Lambert 2010, 901). Dismantling the toxic framework that produces guilt by association should be on the agenda for both researchers and policy-makers. This would also encourage the design of more effective measures to prevent further attacks that forgo making assumptions about entire religions and thereby produce counter-productive outcomes.

3. Countering Extremism Online – Censorship and Counter-Speech

How does the discussion on preventive (in)security production and radicalization relate to the EU IRU's activities to counter extremism on the internet? A policy based on the vague and flawed concept of radicalization will most likely be ineffective and, at worst, be harmful. Developing appropriate instruments to effectively tackle online radicalization seems unachievable if we do not know what online radicalization is. Nonetheless, Europol tries to act upon the notion of radicalization, and its sense-making underpinning this policy is relevant to understanding the dynamics of countering online extremism.

There is no doubt that terrorists use the internet, just like virtually everybody else in today's

society. Terrorists are highly integrated with the internet; they depend on it to the same extent that non-terrorist do. Conceptualizing the internet as a separate and, somehow distinct space is a flaw in counter-terrorism policy, the same as this would be a flawed presumption to make in the context of any other policy. The internet is a constructed technology that shapes human behavior and is shaped by human practices (Bijker et al. 2012; Brey 2005). From a critical security studies perspective, the role that technology plays in (in)security goes beyond the clash between the concept of artifacts conceived as purely being instruments for certain ends and the concept of technology as an autonomous driving factor (i.e. Amicelle, Aradau, and Jeandesboz 2015, 298). Objects – and certainly technologies such as the internet – are not objective or mere facts, they are much more heterogeneous and complex than that, and cannot be reduced to simple materiality (cf. Latour 2005, 26f).

What does this mean for the study of counter-radicalization efforts undertaken by law enforcement? We need to integrate practices, materiality and language in the study of counter-terrorism policy on the internet. New technologies play an important role in pushing counter-terrorism policy from investigation to anticipation. The narrative of big data implies that every piece of data available must be gathered and analyzed to help ‘connect the dots.’ Digital technology allegedly makes data collection and data mining much faster and cheaper, which raises hopes that more accurate predictions of threats can be developed. This particularly promotes “intelligence-led policing” (Martin-Mazé and Burgess 2015, 106), based upon mass surveillance measures that normalize omnipresent suspicion.

The imperative of technological progress demands the relentless adoption of digital means for (in)security purposes. Keeping up with technological development is framed as indispensable and pushes many legitimate concerns aside (Huysmans 2014, 149f). For example, the fact that the strive for greater efficiency in (in)security is driven by human actions and is in no way inevitable is often overlooked. The Paris School theory of (in)securitization highlights the role played by human practices in the construction of (in)security technology: Professionals such as law enforcement officers, intelligence agents, and government bureaucrats shape technology’s development to a large extent.

Research on the role of the internet in terrorism has yielded long lists of ways in which the internet may be used to support or enable terrorist activity (Weimann 2004; Cohen 2002; Conway 2006). In the context of the EU IRU, the use of the internet for propaganda and recruitment – and, to a lesser extent training and finance – are the most relevant functions. Spreading propaganda is the most prevalent concern in countering radicalization online,

because the internet gives terrorists unprecedented control over the means of delivering their messages: “It considerably extends their ability to shape how different target audiences perceive them and to manipulate not only their own image, but also the image of their enemies” (Conway 2006, 5). Unsurprisingly, all kinds of online media channels and media formats are used, from videos, and online magazines to popular websites and social media platforms. This is also done for recruitment and training purposes, which entails tactics such as mobilizing specific individuals online and spreading instructional materials to certain ends.

What is the specific relationship between radicalization and the internet? Related research typically concludes that digital technology is an incubator that accelerates the development of, but does not solely initiate radicalism. Would-be radicals seek out extremist internet content, not vice versa, and consuming propaganda on the internet does not necessarily turn anyone into a terrorist (Hussain and Saltman 2014; Bartlett and Fisher 2015; Howard 2015). Most scholars agree that while the internet may mediate and facilitate terrorism and extremism, it does not cause these (Brown and Cowls 2015, 60).

Online radicalization is used as an incredibly broad concept in large swathes of research published on the topic. Gill and his colleagues point out that “a wide range of virtual behaviours is subsumed into the category of online radicalisation” (Gill et al. 2015, 5). In their meta-study of studies on online radicalization, they criticize the lack of empirical foundation of most of the literature on this issue. They do cite studies that stand out for their empirical thoroughness such as those conducted by von Behr et al. (2013) and Gill and Corner (2015), which examined primary data found in interviews, trial records and computer registries. These studies found that the internet functions as a key source of information and means of communications (as it supposedly does for most people). Furthermore, opportunities to confirm existing beliefs are greater on the internet than in offline interaction. However, these studies also conclude that the internet does not necessarily speed up radicalization, and did not replace offline gatherings in the cases examined. Digital communication only supplements in-person meetings, but it does not substitute them. Since the internet pervades modern life, it makes no sense to frame it as a separate space in which radicalization occurs.

Broadly speaking, there are two political strategies to engage with terrorists’ use of the internet, which can be labeled censorship and counter-speech. The former tries to filter and remove unwanted internet content, while the latter attempts to fight extremist speech with specifically designed counter-messages and opposing communications campaigns. Saltman

and Russell frame the blocking and filtering of online content as “negative measures” and techniques such as developing contrasting narratives as “positive measures” of online counter-terrorism (Saltman and Russell 2014, 11).

In structural terms, ‘negative’ censorship measures have two essential flaws. Firstly, they are “beset by issues of control due to the open, fluid and constantly mutating nature of contemporary online media” (Nasser-Eddine et al. 2011, 50). The technological design of the internet undercuts the effectiveness of censorship approaches, since contents can be copied and reproduced at practically no cost and the decentralized design of the infrastructure frustrates centralized control. The nature of the internet makes total message control impossible and counter-productive, as users are driven to anonymous networks and the ‘dark web’ (cf. Seemann 2014). This holds less true for privately controlled platforms such as Facebook or Twitter, which run on a more centralized server infrastructure.

Secondly, ‘filter and remove’ strategies may unintentionally send a reaffirming message to alleged extremists, implying that said extremists are in the right. If arguments are not challenged with counter-arguments, but simply taken down, this potentially stabilizes the extremist’s worldview which is often based on conspiracy ideologies. Censoring speech from a position of power may reinforce the ideas held by extremists, who see themselves as ‘radical’ outsiders trapped by a conspiracy (Nouri and Whiting 2014, 184).

Governments have always tried to regulate speech (Wagner 2013). Bearing this in mind, the creation of internet referral units should not be treated as a totally unexpected, unique phenomenon. On the contrary, I perceive the EU IRU as just one new element in the long history of the regulation of media and the internet. Most debates about the control of internet content have focused on issues such as child abuse, pornography, and incitement of the general public. Political speech in particular typically enjoys a high degree of legal protection in most European countries because of its fundamental importance to the tenets of liberal democracy.

Now that these theoretical considerations about (in)security, radicalization, and the role of the internet have been presented, the next chapter will set forth the methodology and methods applied in the later empirical analysis.

III. Research Design

1. Interpretive Methodology

The methodology of this master's thesis is in keeping with interpretive research design. Unlike positivist research, interpretive approaches highlight the role of meaning and meaning-making in social lifeworlds and oppose the ideas that research is neutral and that its main task is to trace causal relationships. The interpretive researcher does not formulate and test hypotheses that try to capture causal relationships with variables. Instead, interpretive research aims to understand context-specific meaning by asking 'How?' rather than 'Why?' (Haverland and Yanow 2012; Yanow and Schwartz-Shea 2006). Approaching an empirical puzzle from a non-positivist point of view also means constructing research as an open process of "casing" (Ragin 1992, 217). This means scrutinizing what the subject matter actually is a case of, which avoids rushing to assort certain empirical settings into predefined categories. Theory provides informed expectations and important guidance for interpretive research, but it does not predetermine links between certain cases and pieces of empirical evidence and theoretical variables. I did not want to categorize what the issue under scrutiny is in advance, but rather carefully examine the ambiguities in meaning. In other words, my interpretive methodology favors understanding over explaining. It does not engage in classical deductively constructing hypotheses or inductively testing hypotheses. Instead, it pursues what interpretive researchers call 'abduction,' which means acknowledging the diversity of interpretations, rejecting claims of generalization, and constructing the research process in a way that makes it open-ended and adjustable (Schwartz-Shea and Yanow 2012, 28).

This approach stems from the epistemological assumption that one cannot make objective, independently truthful claims about empirical subject matter. As reality is socially and politically constructed, politics turns into a struggle over ideas. There is no reality 'as such,' because empirical evidence always requires interpretation. Knowledge is always linked to power, and the goal of this particular study is to reveal the political struggle behind the knowledge produced at Europol. As a researcher, I will engage in making sense of the relevant policy texts and their context, and I want to acknowledge that my "interpretation is likely to be incomplete and even possibly erroneous" (Yanow 2006, 16). Research is never value-free, as it inevitably reflects the personal norms and values – or implicit and explicit

biases – of the researcher(s). The implicit biases in this research are likely to be grounded in my political socialization and my social position as a white European male, which may, for example, lead me to highlight some aspects over others due to personal experience and preference.

Interpretive methodology assumes that there are no autonomous facts, but that there are instead many ways to produce knowledge that are linked to specific forms or rationality (Hawkesworth 2006, 38f). The post-positivist approach to research does not try to overcome normative bias but rather seeks to accept and embrace it by attempting to be transparent about its existence.

One important way to make ontological and epistemological assumptions explicit is by making methods explicit and transparent, which is what I am trying to do here. According to Münch, the interpretive turn in policy analysis can be broadly separated into two main strands of meaning-based research: interpretive-hermeneutic and post-structuralist (2016, 18). This research project is rooted in the hermeneutic tradition of interpretation, as it focuses on Europol as a political actor and tries to understand subject-specific sense-making. Assuming that actors come first and shape meaning subjectively according to their intentions, convictions, and routines allows us to study policy formulation at the working level in an interpretive manner. Therefore, for the purpose of this analysis, I do not regard subjects themselves as being constructed through discourse. The language adopted by Europol plays a performative role, for example, by generating consensus around certain positions and legitimizing certain counter-terrorism measures. I assume that humans have agency in their production and understanding of meaning and that the way in which they act is an expression of their values, feelings, and practices. Many positivist theories, most notably rational choice and behaviorist approaches, tend to ignore or sideline the role of ideas and values. This analysis focuses on the role of knowledge in policy-making and regards knowledge as the basis for action and the crucial capacity to act (Stehr 2001). Practitioners are overwhelmed with data and need to make sense of it. Therefore, knowledge production and action are not seen as two separate processes independent of one other, but as two sides of the same coin: in other words, knowledge constitutes action (Knoblauch 2005, 146).

2. Method

My tactical choice in analyzing the meaning-making that underlies the measures taken by

Europol to counter radicalization online is the *Critical Frame Analysis* (CFA) approach developed by Mieke Verloo and Emanuela Lombardo (2007).

2.1. Critical Frame Analysis

This method is designed for conducting an interpretive, micro-level policy analysis that aims to reveal the structuring principles and problem definitions involved in a certain policy debate. It was initially formulated and designed for the study of gender equality policies in Europe, but can be adapted – as I am attempting to demonstrate here – to the interpretive study of other policy fields, in my case online counter-radicalization policy.

I selected this method because it was explicitly created for the purpose of interpretive policy analysis. Compared to other approaches of interpretive policy analysis, critical frame analysis stuck out because of its clearly defined and delimited scope. Many qualitative methods (such as content analysis) emerged from positivist methodologies, which makes them rather ill-suited for interpretive research designs. There is also a wide range of interpretive policy methods, such as discourse-oriented approaches, that are more abstract and operate on a macro-level. These can offer insights into broader, long-term arrangements of meaning. But discourse analysis methods usually go well beyond the analysis of language and text and provide very extensive frameworks, which would greatly exceed the scope of this study.

The Critical Frame Analysis method fits the epistemological assumptions described above. CFA is rooted in the social movement strand of frame analysis approaches. The purpose of this method is to map how an issue is framed. This method defines a frame as

> an interpretation scheme that structures the meaning of reality, and a policy frame as an organizing principle that transforms fragmentary or incidental information into a structured and meaningful policy problem, in which a solution is implicitly or explicitly enclosed (Verloo and Maloutas 2005, 4).

The authors of CFA drew upon to Gadamer's concept of prejudices as the theoretical foundation for their method. This concept does not apply the normative meaning of bias to 'prejudice,' instead, this term is used to describe socially constructed "conditions for understanding" (Gadamer 1960, quoted in Verloo and Lombardo 2007, 32) that allow people to filter information. Understood in this sense, we all use frames to structure and prioritize knowledge. Frames are shaped by discursive and practical consciousness, as well as by rules and routines. Practices that are typical for certain contexts and situations, possibly without reflection on their use, shape practical consciousness. Van Hulst and Yanow supplement this definition by describing frames as "implicit theories of a situation: They model prior thought

and ensuing action, rendering that action sensible in terms of pre-existing thinking" (2016, 98).

Framing a policy means conceiving of, adapting, and negotiating the conditions for its understanding. The process of constructing frames (framing) is a dynamic, interactive, context-specific act of sense-making. A key part of the sense-making is naming and categorizing certain problems. "Sense-making is a situated process to which policy-relevant actors attend in circumstances that are ambiguous or about which there are uncertainties" (van Hulst and Yanow 2016, 97). Sense-making is a largely implicit process; it builds upon known, established ideas and practices.

Frames and framing are instrumental concepts for understanding public policy development. The CFA approach assumes that there are multiple possible interpretations of a policy issue and that the initial question that must be addressed to form an understanding of them is *"What's the problem represented to be?"* (Bacchi 2009). In order to determine 'what the problem is represented to be,' CFA distinguishes two key dimensions that structure the analysis of policy frames: diagnosis and prognosis. The former addresses the question 'What is represented as the problem?' while the latter accounts for possible solutions by asking 'How and by whom can the problem be solved?' The CFA method provides a number of detailed and practice-oriented guiding questions for analysis, including (cf. Verloo and Lombardo 2007, 34ff):

- Why is it seen as a problem?
- Who has a voice and who is acted upon?
- Whose problem is it represented to be?
- Where is the problem located (both in diagnosis and prognosis)?
- How is the problem (re)produced?
- Are the diagnosis and prognosis consistent?

These 'sensitizing questions' were used to analyze the policy documents by progressively assigning in-vivo codes to three CFA code categories (diagnosis, prognosis, roles) as well as three additional code categories (radicalization, facts, language). In-vivo coding is an interpretive practice that picks up on the language used in the policy documents (Kuckartz 2010, 68). Coding was done using the free and open source RQDA software[4]. This program allows users to group codes according to categories, organize files, and assign attributes for

4 'free' as in freedom, based on the R statistics software, cf. http://rqda.r-forge.r-project.org/

in-depth analysis. The ‘facts’ code category covered information and numbers found in the documents, while ‘radicalization’ captured all kinds of different references of the term. The methods presented in Laura Shepherd’s work on critical approaches to security were of great use in specifying the ‘language’ coding category (Shepherd 2013). The contribution on predication, presupposition, and subject-positioning (Åhäll and Borg 2013) were particularly instrumental in defining and fine-tuning the language-based codes. A table with an overview of the coding system and the respective coding rules can be found in the appendix (VI.1.).

The coding system was adjusted and refined iteratively by re-reading documents multiple times. The inventors of CFA already proposed this in their outline of the method, suggesting that re-coding material might be necessary to include new insights in the coding system. After a first round of coding, pre-defined and in-vivo codes were grouped according to the code categories mentioned above. In a second round of coding, more detailed codes were assigned within each code category. During the coding process, memos were written for each code category and multiple codes, documenting spontaneous associations, impressions, and ideas. Memo writing proved to be an excellent research technique that allowed for findings to be continuously mapped across different sources (cf. Soss 2006).

The CFA approach has been criticized for being unable to explain why certain policy frames are used in certain ways, since this method neglects to thorough study context (Münch 2016, 84). On the one hand, this is a valid criticism, but on the other hand, this is also a reason why I chose this method for this specific analysis. It seemed more suitable to use a narrowly designed method instead of picking out elements of broader analytical frameworks in order to make them fit this research project. Focusing on the ordering principles of a certain policy debate makes it easier to identify the details and nuances in the frames used and may still allow to generate insights about the larger discursive arrangement in the policy field. The potential lies in being able to challenge generalizations, and not necessarily in creating new ones. The use of sensitizing questions enables the researcher to find unexpected or inconsistent elements of frames, because “it does not close possibilities of coding ahead of the analysis; thus it grants more freedom and flexibility for interpreting the specific variations of a text” (Verloo and Lombardo 2007, 38).

2.2. Empirical Data – Policy Documents and Interviews

The empirical data gathered for this analysis was two-fold: EU policy documents, and insights gathered through interviews with public officials and experts in the field of European

counter-terrorism policy. The body of policy documents comprises the mandate of Europol's work, the published strategies of EU counter-radicalization policy, as well as the threat assessments, work programs, PR publications, press releases, and annual reports published by Europol. To delimit the body of texts adequate for analysis, only texts that directly relate to the EU IRU and Europol's counter-radicalization policy were selected for the coding process: for example, if they included references to the EU IRU or online counter-radicalization strategies. If these documents were 50 pages or more in length, only the relevant sections or chapters were selected for thorough frame analysis. The bulk of the primary documents were published after the attacks in Paris on January 7, 2015, but some of these documents predate these attacks. The last document taken into account was published in July 2016; later publications were not analyzed. A full list of coded files can be found in the appendix (VI.2.). Directly quoted documents are listed in the bibliography.

These documents and reports were retrieved from the official websites of Europol, the Council of the European Union, the European Commission and the civil rights organization Statewatch. News reports were mostly obtained via Google News as well as Twitter searches.

Going beyond the study of written text, I conducted five semi-structured interviews. Two of these interviews were held with 'inside' officials, one working at Europol, and another working at the Council of the EU. These were most insightful, as they provided informal 'spoken frames.' Both interviewees agreed to these interviews on the condition of anonymity. Therefore, the content of the interviews is not quoted literally, but informed both the textual and the contextual analysis of the EU IRU. Three conversations conducted with 'outside' experts in the policy field were used as "helicopter interviews" (Hajer 2008, 221) to gain contextual information beyond the study of secondary literature. The experts were selected based on their proven, long-standing experience in researching Europol's policy.

These interviews were meant to provide an understanding of the context of the EU IRU's formation, as well as additional facts. The authors of the CFA also claim that "interviews with key actors involved in the formulation and adoption of official documents [...] would be useful to complement the analysis" (Verloo and Lombardo 2007, 40). Indeed, the interviews provided a great opportunity to gather more details, gain different perspectives on the issue, and check assumptions. The interviews were conducted with semi-structured guidelines, either in person or on the phone, and were fully recorded and transcribed. A list of all conducted interviews is attached in the appendix (VI.3.).

IV. Empirical Analysis

1. The EU Internet Referral Unit and Its Political Context

This first part of this analysis examines what exactly Europol does towards countering terrorism and violent extremism on the internet. The following chapter delineates the institutional evolution of the EU IRU and demonstrates how this fits into the context of broader political developments.

1.1. Development of the EU Internet Referral Unit

The EU IRU is a working unit at Europol that officially began operations on July 1, 2015 under the purview of the European Police Office in The Hague, Netherlands. The creation of the EU IRU was requested by the Justice and Home Affairs (JHA) Council on March 12, 2015, roughly two months after the attacks in Paris in January 2015, which targeted the staff of the satirical magazine Charlie Hebdo and customers of the Jewish supermarket Hypercacher. The creation of the EU IRU was portrayed as a direct reaction to those attacks in several of the interviews I conducted, as well as in the preparatory policy documents I analyzed.

After its establishment, the new unit operated in a pilot phase for six months, then proceeded to what Europol describes as ‘initial operational capability’ until June 2016, and has been running at full operational capability since July 2016 (Europol 2015f). In November 2015, the EU IRU’s staff was consisted of nine employees; in April 2016 the total number of staff had increased to 17, and it is projected to rise to 21 by end of 2016 (Europol 2016h, 4). Several interviewees confirmed these figures and timelines.

The EU IRU builds upon a prior Europol project called Check the Web (CTW), which was established in 2007 following a Member State initiative led by Germany. The goal of the CTW project was to collect and analyze terrorist propaganda material on the internet. The project team was composed of counter-terrorism experts and linguists who searched for relevant material and stored it in a database accessible to all Member States. Europol says that this database contains about 10,000 electronic documents and individuals (Europol 2015d, 3). The Check the Web project merely focused on monitoring and analysis; referral and take-down initiatives were not included. A second project already in place on the European level, CleanIT, consisted of a dialog process held between the public and the

private sector that drafted ‘general principles’ and ‘best practices’ for how to fight terrorism online[5]. These initiatives were criticized for their overly broad understanding of what constitutes terrorism and undesirable online content, exceeding the definitions stipulated by law (Bigo et al. 2014, 21; EDRi 2012).

The United Kingdom was the first EU Member State to implement law enforcement strategies targeting radicalization on the web, most prominently the ‘PREVENT’ strand of its counter-terrorism approach, which was put forward in 2006. Documents suggest that the main model for the EU IRU was the so-called ‘Counter-Terrorism Internet Referral Unit’ (CTIRU) in the United Kingdom, which has been in operation since February 2010 (EU Counter-Terrorism Coordinator 2015a, 3). This special unit is in charge of flagging and, if necessary, removing material from the internet. As was confirmed during several of my interviews, the UK’s CTIRU works together with Europol and actively supports the development of the EU IRU. As the UK is the Member State with the most in-depth experience with an internet referral unit, police officers from the UK also make up a large part of the EU IRU’s staff. The second Member State leading the European effort on policing internet content to combat terrorism, is the Netherlands. The Dutch government led the CleanIT project and started to develop informal social media policies and engage in a dialog with the internet industry relatively early on (EU Counter-Terrorism Coordinator 2015a, 2). Furthermore, a Dutch police officer, Wil van Gemert, is Europol’s Deputy Director and the head of its operations department. The Director of Europol, Rob Wainwright, used to be a British law enforcement and intelligence officer. The nationalities of these two top-level staff members serve as further indication of the leading roles of the UK and the Netherlands in the development of the EU IRU.

The most outspoken supporter of the EU IRU on the European level has been the EU Counter-Terrorism Coordinator, Gilles de Kerchove. He spearheaded a push for internet referral capabilities at Europol shortly after the attacks in Paris in January 2015. The Riga Joint Statement of the Council on January 30, 2015 mentioned that

> [t]he internet plays a significant role in radicalization. [...] we must strengthen our efforts to cooperate closely with the industry and to encourage them to remove terrorist and extremist content from their platforms (European Council 2015, 5).

After the subsequent attacks in Paris in November 2015, the European Counter-Terrorism Center (ECTC) was established within Europol, also following a decision made by the JHA

5 http://www.cleanitproject.eu/ (last retrieved 11 July 2016)

Council of Ministers. My interviewees confirmed that the creation of the ECTC was an ad-hoc political move to demonstrate action after the attacks. The ECTC basically consolidated the existing counter-terrorism units into one center at Europol. The EU IRU therefore became part of the ECTC, but remains a relatively independent working unit within Europol. This is also due to the double mandate of the EU IRU, which covers counter-terrorism as well as "fighting traffickers" (European Council 2015, 2). The dual strategic focus of the EU IRU encompasses working on 'illegal immigration,' which became a paramount topic in 2015 and resulted in the creation of a European Migrant Smuggling Center:

> Europol will establish and develop in early 2016 the European Migrant Smuggling Centre (EMSC) which will provide increased operational support to MS in their fight against organised people smuggling networks. [...] The expertise of the EU Internet Referral Unit will also be used to identify and refer online content relating to the provision of illegal migration services (Europol 2015g, 9).

The following analysis of the EU IRU's working mandate will illuminate this dual function of countering both 'terrorism' and 'illegal immigration.'

1.2. Casing the EU Internet Referral Unit

Identifying and taking down online material is the core mission of the EU IRU: The unit aims to reduce the amount of 'terrorist material' on the internet. According to official documents, the unit's mandate comprises the following tasks (cf. Europol 2015d):

> - To coordinate and share the identification tasks (flagging) of terrorist and violent extremist online content with relevant partners,
> - To carry out and support referrals quickly, efficiently and effectively, in close cooperation with the industry,
> - To support competent authorities, by providing strategic analysis and operational analysis,
> - To act as a European Centre of Excellence for the above tasks.

This means that the staff of the EU IRU searches the internet for what it deems to be 'terrorist and violent extremist online content.' Identifying relevant content essentially means carrying out web surveillance and storing the identified content in a central IRU database. The online content is then analyzed by counter-terrorism experts and, if it is assessed to be relevant, sent to the private company where it is hosted. Given its limited resources and relatively small team, the EU IRU currently only targets large platforms and key points of dissemination of online content. Most requests for taking down content originate from the EU IRU's own surveillance activity (Europol 2015f, 11; Europol 2016a). Unlike the UK's CTIRU, the EU

IRU does not receive information about relevant content from the public, as its legal basis does not allow for this (Jones 2016, 2). Another way to identify content is through so-called 'support referrals.' These involve Member States sharing a piece of content that they have detected with Europol; the EU IRU then organizes the referral to the hosting company. This coordination and support role is Europol's basic mission and provided as a service to Member States who do not have national internet referral units.

Referrals, Europol claims, to not entail privileged access to hosting platforms. As far as is known at the time of writing, the EU IRU does not have the status of a 'super-flagger' with special access to certain online platforms.

The online content targeted by the EU IRU could be anything, such as text, image, or video material. It also comprises entire social media accounts or profiles. In order to work most effectively, the EU IRU tries to focus on social media accounts, especially Twitter accounts, that have a large outreach, provide translations into EU languages, serve as dissemination hubs, and function as high-profile influencers (Europol 2015f, 11). This prioritization was also emphasized in the interview I conducted with a senior Europol official. Which platforms are mainly targeted? Europol states that the "EU IRU refers internet content across the following social media platforms, in ascending order of volume: Facebook, SendVid, Vimeo, Google Drive, Youtube, Archive.org and Twitter" (Europol 2015f, 12).

Details regarding the kind of content that is monitored, assessed, and referred are scarce and rudimentary. What is publicly known is the double mandate of the EU IRU: addressing 'terrorist and violent extremist' content as well as content related to 'illegal immigration.' Although the decision to establish the EU IRU was triggered in the context of counter-terrorism, shortly after the Charlie Hebdo attacks, the scope of its mandate was extended in April 2015 by the European Council. The accompanying statement mentioned that Europol should also target "internet content used by traffickers to attract migrants and refugees, in accordance with national constitutions" (European Council 2015, 3). This expansion of the mandate occurred before the EU IRU officially began operating on July 1, 2015. In the words of the EU Counter-Terrorism Coordinator, this means that the EU IRU "is also tackling the facilitation of illegal immigration, with a continuous analysis of social media-related information on a 7/7 basis" (2015b, 5).

Figures on how many pieces of online content are assessed, referred, and deleted vary. In April 2016, the European Commission published a report saying the EU IRU

> has assessed over 4,700 pieces of material across 45 platforms and made over 3,200 referrals for internet companies to remove content, with an effective removal rate of 91% (European Commission 2016a, 7).

The numbers cited in a more recent document, published in May 2016, are significantly higher:

> 7,364 pieces of online content were assessed by the IRU, triggering 6,399 referral requests (with a success rate of 95% concerning subsequent removal). In 2016, 629 new terrorist media files were uploaded to the Check-the-Web (CTW) portal (Europol 2016e, 7; Monroy 2016).

Even more recent numbers released in July 2016, refer to "11,000 messages across some 31 online platforms in 8 languages" that have been assessed and referred (Europol 2016i; Europol 2016h). 91.4 percent of those referrals were removed by the respective hosting platform.

As there is no possibility to compare or fact-check these figures, one thing becomes quite clear: The interesting piece of information is the small percentage of referrals that were *not* removed by the platforms. The key question is not necessarily how many pieces of content are assessed and deleted, but the criteria by which they are assessed and deleted.

How does this process work? Online content is assessed at two different points by two different organizations, respectively. The first assessment is conducted by the EU IRU, which classifies some content as 'terrorist' or 'violent extremist' propaganda. After the referral has been made, a second assessment is conducted by the private company hosting the content in question. The nature of this second assessment is left fully to the company's discretion and is based on its corporate terms of service. At this stage of the process, Europol denies having any formal or informal influence on the company's categorization of the referred content (e.g. EuroparlTV 2016, min 3:30; also confirmed in several of my interviews). Europol has to leave the decision to the private hosting provider because of Europol's legal basis. Since Europol does not authorize any executive powers, it can only flag content on the platform, but is unable to enforce the take-down.

Both assessment processes are obscure and completely inscrutable. The take-down quota of 95 percent indicates that the IRU and the private companies must use different criteria to assess the content, at least to some extent. Since there is no judicial oversight of the process, there is no right to formal objection or disclosure foreseen for this process. Europol's referral activities are non-binding requests, legally equivalent to the flagging of posts done by

ordinary users; “thus the decision and related implementation of the referral is taken under full responsibility and accountability of the concerned service provider” (Council of the EU 2015b, 3).

It is important to highlight the fact that neither of the two distinct assessment processes is based on existing legal rules, but rather on the ‘community guidelines’ or ‘terms and conditions’ of the platform in question. The relevant criteria for referring content to internet companies is whether “Europol assesses it to have breached their terms and conditions. This is a voluntary arrangement in order to alert the companies when their sites are being abused by terrorist organisations” (European Commission 2015). This arrangement is not accidental, but part of the reasoning that lead to the introduction of the EU IRU. This is evident in statements made by EU Counter-Terrorism Coordinator Gilles de Kerchove, who advocated the creation of the EU IRU, because this would allow for more online content to be deleted by private actors, than is legal under European and national legislations:

> Consideration should be given to a role for Europol in either flagging or facilitating the flagging of content which breaches the platforms’ own terms and conditions. These often go further than national legislation and can therefore help to reduce the amount of radicalising material available online (EU Counter-Terrorism Coordinator 2015a, 3).

Clear examples of materials that are not protected by the right to free expression can only be constructed within a given set of rules. Conditions for what kind of content is permissible differ significantly from country to country, and even more so from one social media platform to another. Defining the limits of free speech in a democratic society is usually not a technocratic practice, but rather a deeply political choice. For example, certain symbols or statements denying or trivializing the Holocaust constitute criminal offenses in Germany and many other European countries, and are liable to prosecution. In other countries, the same symbols or speech might be legally permissible. The interpretation of the boundaries of free speech certainly cannot be generalized and detached from the respective social and political context in which it is made. How does Europol make this complex decision? In the interviews I conducted, I only received a rather vague and general answer, along similar lines to this explanation:

> An expert evaluation of the content is performed in accordance with the principles set up in Council Framework Decision 2008/919/JHA on combating terrorism. The Council Framework Decision 2008/919/JHA on combating terrorism (amending the Council Framework Decision 2002/475/JHA) sets out a definition on what is to be considered as ‘public provocation to commit a terrorist

offence' (Europol official, quoted in Jones 2016, 2).

Resorting to quoting legal norms does not necessarily clarify the categories employed here, as legal definitions are often formulated in rather vague terms, too. Whether or not the laws cited here provide a transparent basis for the assessment of online content will be analyzed in Section 2.1.1.

1.3. Political Context

Every text has a context. This paper investigates the formation of the EU Internet Referral Unit from roughly January 2015 to June 2016, during which period most of the policy documents analyzed in this study were published. Taking into account the political conditions under which policy-making takes place is crucial for any policy analysis. The Critical Frame Analysis method primarily focuses on the content and language of policy text. In order to complement the CFA, a quick overview of the political context and developments surrounding the establishment of the EU IRU ought to be given, but without aiming to cover all of the details of the institutional and legislative developments in EU counter-terrorism policy.

Many scholars agree that European counter-terrorism policy has been developing mostly ad-hoc and does not necessarily follow a coherent strategic approach. Although the European approach to counter-terrorism has become more comprehensive over time, it has evolved in "a primarily incremental and external shocks-driven process" (Schröder 2013, 85). As security policy is traditionally regarded as a core part of national sovereignty, EU Member States have been reluctant and slow to cooperate on security matters or even confer security-related competences to the EU level. The broader narrative of EU counter-terrorism policy follows pivotal events – first and foremost the attacks on September 11 in 2001, on March 11, 2004 in Madrid, and on July 7, 2005 in London – as the critical junctures that opened windows of opportunity for counter-terrorism policy-making. At the same time, it also urges policy makers to act in an ad-hoc manner, without conducting thorough analysis of what ought to be done. Pressure to demonstrate decisiveness and authority has led to the rather hasty adoption of pre-existing policy proposals, which are usually not tailor-made and sometimes merely symbolic solutions to specific situations (Bossong 2008; Hayes and Jones 2015). As explored above, the development of the EU IRU also follows this pattern of EU counter-terrorism policy-making: An established infrastructure (the CleanIT and Check the Web initiatives) was extended based on existing models in some Member States (the UK and

the Netherlands).

The time frame investigated in this paper coincides with the negotiation phase for the new Europol regulation, which was adopted by the European Parliament in May 2016. It will provide a new legal basis for Europol, and is going to enter into force on May 1, 2017 (Europol 2016f). The regulation appears relevant for the context of the EU IRU because some of the provisions included therein were drafted to allow the exchange of information with private parties (Rudl 2016). This happened late in the legislative process, after there had been some public criticism that the EU IRU still lacks an appropriate legal basis (Monroy 2015). A Council document acknowledges that the new Europol regulation was subsequently amended during the trilogue negotiations in order to insert a sound legal basis for the EU IRU:

> In order to provide explicit legal basis in the draft Europol Regulation for the functioning of IRU while ensuring the necessary guarantees for the protection of personal data, the Presidency has developed [...] proposals to amend the draft Europol Regulation (Council of the EU 2015b, 5).

The initial draft of the Europol regulation prohibited the transfer of personal data to private parties. It therefore seems that a high-level political decision to create a new police unit at Europol was only later authorized by the adoption of the amended regulation.

At present, Europol's legal foundation consist of the Council Framework Decisions 2002/475/JHA and 2008/919/JHA. These will remain the working basis of Europol until the new regulation will enter into force on May 1, 2017. In the mean time, the two Council Decisions authorize Europol to only retrieve and process data only from publicly available sources, but not to share it with private parties. One document shows that the Council is aware that the current Framework Decision "has no express provisions regulating the transfer of personal data (for example, the URL link)" (Council of the EU 2015b, 4). Accordingly, the development of the EU IRU can be conceptualized as a process of mission creep (cf. Hayes and Jones 2015, 17), whereby competences and mandates are introduced and expanded informally, and later incorporated into the formal legal structures of the organization.

Parallel to the establishment of the EU IRU, two closely related initiatives were advanced on the European level. Counter-speech initiatives were created, aiming to provide alternative perspectives and facts to counter propaganda efforts. Notably, one counter-speech project – called EU East StratCom Task Force – operates in the context of the conflict in Ukraine and is run by the European Union External Action service. It collects 'pro-Kremlin

disinformation' and regularly publishes a 'Disinformation Digest.'[6] According to media reports, the project team, which is led by the High Representative of Foreign Affairs, works rather obscurely, and has failed to disclose the scope of its mission (Bonse 2015). Recently, the task force made headlines with a humorous video it distributed on social media that openly mocked 'pro-Kremlin media' for its disinformation strategies[7].

The second counter-speech initiative is the Syria Strategic Communications Advisory Team (SSCAT), which serves as a specialized advisory team that provides expertise on countering "terrorism communication campaigns" and "works as a network where best practices on countering violent extremism and counter terrorism communications between the Member States is shared" (Council of the EU 2015a, 9). It consists of a team of experts seconded by Member States that work under the Belgian Ministry of Home Affairs. SSCAT consults national governments across the EU on how to improve their counter-speech operations.

Cooperation with the internet industry, most prominently companies such as Google, Facebook, Microsoft, Twitter, but also others, has also been promoted. The 'EU Internet Forum' initiative was launched in December 2015, so that partnerships could be established a partnership with relevant stakeholders "to restrict the accessibility of terrorist material online and increase the volume of effective counter-narratives" (European Commission 2016a, 7). Leading social media companies published a code of conduct that was prepared together with the European Commission. The agreement requires the platforms to "review the majority of valid notifications for removal of hate speech in less than 24 hours and remove or disable access to such content" and moreover calls to "educate and raise awareness" about the companies' guidelines (European Commission 2016b). The agreement was met with refusal by NGOs such as European Digital Rights and Access Now, who dropped out of the EU Internet Forum talks and criticized the public/private cooperation which constitutes a "privatization of censorship" (Dachwitz 2016; EDRi 2016). Other observers say the agreement is designed to produce chilling effects on users and encourage over-blocking of legal content. Although having been severely criticized for human rights violations, the cooperation between internet corporations and governments on regulating speech online seems to be on the rise, with similar advances evolving in several EU Member States and many countries around the world (e.g. Nakashima 2016).

6 http://eeas.europa.eu/euvsdisinfo/ (last retrieved 12 March 2016)
7 https://twitter.com/EUvsDisinfo/status/753648355247394817 (last retrieved 14 July 2016)

2. Europol's Framing of the EU IRU

We have seen why the EU IRU is a highly suitable case for studying the policy framing of developing governance mechanisms to regulate online content, emerging at the interface of private actors and law enforcement. The following section analyzes the frames employed to describe, structure, and make sense of Europol's Internet Referral Unit. Policy documents produced by Europol will be examined, building on the conception of frames as conditions for understanding and of framing as an implicit act of sense-making.

2.1. Diagnosis – What Is the Problem Represented to Be?

The following empirical analysis is structured along the two main categories of the critical frame analysis method. Starting with the diagnosis that asks what the problem is constructed to be, this section presents key frames in Europol's practitioners' sense-making and problem definition.

2.1.1. Terrorism – A Presupposed Threat to Security

According to Didier Bigo, 'terrorism' is a term with no conceptual value for social sciences – but it undoubtedly has a powerful political function (Bigo 2005). It is important to scrutinize where and how the word 'terrorism' is used and what it stands for. The discursive (in)securitization of political issues through the mobilization of existential threats has become a common theme in critical security studies debates. It almost goes without saying that – in the context of Europol's counter-terrorism policy – explicit and acute threat construction is absolutely prevalent. To give only one of many possible examples, the Head of Europol recently stated, when asked about terrorist attacks, that "[t]he threat is alive and current. Another attempted attack is almost certain" (Wainwright 2016). Alarming language is even used in some policy documents, for example, "special forces style attacks" (Europol 2016a) are mentioned.

What does Europol talk about when it talks about terrorism? Understanding what terrorism means for Europol starts with the legal basis of EU counter-terrorism policies. My interviewees tended to refuse to provide their own, orally formulated definition of terrorism, instead referring to the Council Framework Decisions 2002/475 and 2008/919 as the encompassing legal basis for their work. But it seems fair to say these two laws provide only vague or extremely broad categories of what constitutes terrorism, covering all "intentional acts" that "may seriously damage a country or an international organisation" with the aim of (inter alia, only an excerpt):

- seriously intimidating a population, or

- unduly compelling a Government or international organisation to perform or abstain from performing any act, or

- seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation (Council of the EU 2002 Article 1).

This provision is followed by a list of offenses that are relevant in the context of terrorism, including attacks on human beings, kidnapping, destruction of all kinds of infrastructures, seizure of vehicles, the creation, proliferation, and use of weapons, and many more. The list also includes "threatening to commit any of the acts listed." Generally speaking, this legal basis does not provide clear instruction for law enforcement, as it only sketches a broad spectrum of offenses that may potentially be covered or investigated. For example, it may well be the case that politicians' statements "seriously intimidate a population," but they are never labeled as terrorism. Going further, the second Council Framework Decision of 2008 amended the scope of what may constitute terrorism, specifying how the offenses of public provocation, recruitment, and training for terrorism ought to be understood (Council of the EU 2008 Article 3). Article 4 of the Framework Decision also criminalizes "aiding or abetting, inciting and attempting" as offenses linked to terrorism.

Looking at the legal definitions of terrorism with which practitioners have to work makes it clear what political margin of discretion practitioners have in interpreting these definitions. Europol, a relatively small agency with about 950 employees, has to formulate relevant priorities. The European Commission clarifies that the Framework Decision "aims to reduce the dissemination of messages and material that may incite people to commit terrorist attacks" and explicitly mentions the internet as a means to do so (2014b, 3f). Merely based on the legal text, terrorism becomes more of a container term than a clear assignment. Without prioritization on the practice level, no implementation of counter-terrorism measures would be possible.

How Europol breaks down this overtly broad categorization of terrorism is best illustrated by the agency's annually published Terrorism Situation and Trend Report (TE-SAT). In the methodology chapter, the report first refers to the nature and context of terrorism as formulated by the aforementioned legal basis. Europol acknowledges that "it can be difficult to assess whether a criminal event should be regarded as an act of 'terrorism' or as an act of 'extremism'" (Europol 2015a, 46). In the report, terrorism (a very broad and loose category) is classified into different types based on their source of motivation (cf. Europol 2015a, 3ff):

- ‘Religiously inspired Terrorism’
- ‘Ethno-Nationalist and Separatist Terrorism’
- ‘Left-Wing and Anarchist Terrorism’
- ‘Right-Wing Terrorism’
- ‘Single Issue Terrorism.’

This approach poses some difficulties, because these categories are not mutually exclusive. Europol concedes that “many [terrorist] groups have a mixture of motivating ideologies, although usually one ideology or motivation dominates” (Europol 2015a, 47). For example, religion is invoked as a motivating factor for both religiously inspired terrorist groups as well as for ethno-nationalist terrorism. Furthermore, the separation between ethno-nationalism and right-wing terrorism often appears to be blurry. Europol also lists ‘unspecified’ terrorist attacks in its statistics, making the problems inherent to the classification of types of terrorism based on motivation even more apparent. This might be due in part to different Member States reporting different statistics to Europol, but it also shows that Europol has struggled to define sound and distinct categories for what terrorism actually is. The level of sophistication of an attack is clearly not regarded as a criterion for terrorism, as both very sophisticated and unsophisticated attacks are listed in the TE-SAT reports.

Type of Terrorism	**Number of reported ‘failed, foiled and completed attacks’ per year and category in EU Member States**								
Religiously inspired (“Islamist”)	1	4	0	1	3	0	6	0	2
Ethno-Nationalist and Separatist	424	532	397	237	160	110	167	84	67
Left-Wing and Anarchist	30	21	28	40	45	37	18	24	13
Right-Wing	1	1	0	4	0	1	2	0	0
Single Issue	0	1	5	2	1	0	0	0	1
	2006	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**

Table 1: ‘Failed, foiled and completed attacks’ according to data in TE-SAT 2007-2015

Table 1 presents the figures on attacks reported in the TE-SAT since 2007. There was a striking discrepancy in the figures and the way in which the data was presented. Numbers on attacks attributed to single issue and right-wing terrorism are only mentioned in the appendix of the report, while the attacks listed under the other terrorism categories are presented with graphs early on in the text. The chapter on religiously inspired terrorism prominently illustrates the figures on “suspects arrested for religiously inspired terrorism 2010 to 2014,” *without* mentioning the total number of ‘failed, foiled or completed attacks,’ which is significantly lower. The numbers on ‘failed, foiled or completed attacks’ presented in Table 1 can only be retrieved in the appendices of the TE-SAT reports. While the number of

religiously inspired terrorist attacks was relatively low (cf. Table 1), the number of arrests for religiously inspired terrorism constituted the largest proportion of total arrests in the EU. The chapters on left-wing and ethno-nationalist terrorism include statistics for both 'suspect arrests' as well as 'failed, foiled, and completed attacks' in a single graph. The chapter on religiously inspired terrorism is the only one in which only the number of arrests, but not the number of attacks is illustrated. This raises questions about a biased presentation of facts in the TE-SAT, which treats figures on 'religiously inspired terrorism' differently than all other types of terrorism. Why are the same statistics for the categories presented in different ways?

Researchers have already pointed out problems with the TE-SAT reports, criticizing that they compile incomparable national data and gloss over national differences in trying to present a harmonized European threat assessment. De Goede writes that Europol performs 'cultural work' with the TE-SAT reports and – consciously or not – follows "the first lesson of identity theory – which is that in order to develop a common identity and a common space for action, one requires a common enemy, or at the very least, a shared threat perception" (de Goede 2011, 7).

Even without going through all the categories used, a clear priority in the TE-SAT is tangible. 'Religiously inspired terrorism' has been the first and by far largest section of the reports issued over the past few years. Interestingly, the category was renamed in 2012 from 'Islamist terrorism' to 'religiously inspired terrorism,' although the chapter still exclusively covers the actions of violent jihadi groups. This suggests that the shift from 'Islamist' to 'religiously inspired' was mere semantics. In striving to harmonize European-wide threat perceptions, Islamism is still the presumed underlying ideological motivation behind this categorization, thereby (re)affirming the association of the terrorist threat with 'Islam.' This brings us to the notions of radicalization and extremism, which are regularly invoked in this context of the fight against terrorism.

2.1.2. Radicalization and (Violent) Extremism

How is radicalization framed by Europol? Notably, I was unable to find any description of the term in any Europol publication over the course of my investigation. Europol does not explicitly define radicalization in its policy discourse. There are only indirect references to it in several documents and statements. Two different conceptions of radicalization can be derived from the way in which Europol uses the term. One is *radicalization as a process*, which draws upon formulations such as "efforts to radicalize and recruit" or "on the path of radicalization." Radicalization is described like a conscious action that some humans perform

on others, whereby the active party is the recruiter or demagogue who radicalizes an individual who adopts a rather passive role. The second conception is *radicalism as a condition*. This understanding of the term envisions radicalism to be an end product, a state of mind of persons who 'have been radicalized' or are described as 'radicalized attackers.' This suggests that radicalization stops at the point at which an individual has 'become radicalized' or 'a radical.' Radicalization is generally referred to as a very complex phenomenon, but no (public) effort is made to unpack this concept. Especially 'online radicalization' is often used interchangeably with the terms (online) propaganda and (online) recruitment.

Europol only occasionally uses metaphors to discuss radicalization – this occurs far more frequently in European Commission texts. Metaphors make it easier to grasp complex circumstances in policy texts and envision abstract concepts. For example, in order to describe the function of the internet for foreign fighters, the TE-SAT mentions that "social media continues to have a galvanising effect on potential travelers" (Europol 2015a, 22). Metaphors may occasionally only serve an illustrative function, but they also structure the way in which we think about problems in policy-making. The phrase 'playing whack-a-mole' is associated with a very particular mental image. What does a 'fertile environment for radicalization' look like? How about a 'breeding ground for radicalization?' What is 'homegrown' terrorism? The occasional use of such metaphors for radicalization makes it easy to talk about radicalization as a process that – quite naturally – resembles a tiny seed sprouting into a large tree.

The TE-SAT frequently mentions radicalization, but makes no attempt to define it. The report does, however, briefly elaborate on *extremism* as a phenomenon separate from terrorism. Stating that extremism and terrorism show similar 'behavioural patterns,' the report points out that "contrary to terrorism, not all forms of extremism sanction the use of violence" (Europol 2015a, 46). But since the focus of the TE-SAT is terrorism, Europol does not expand upon its idea of extremism any further. Some sections mention terms like 'extremist media,' 'extremist offences' or 'extreme jihadist views' without detailing what constitutes their extremist nature. In some parts of the reports, the unclear definition of extremism seemed to be apparent to the authors; for example, when they noted that "religious extremism seems to have played a role" (Europol 2015a, 8). Generally, extremism is mainly described in negative terms, as the opposite or complement of terrorism, with terrorism adopting different methodologies and tactics to extremism (Europol 2015a, 35).

One *predication* that comes up in both political and more technical policy texts is 'violent

extremism.' Attaching a certain property to a noun, in this case 'violent,' endows the term with a particular capacity (cf. Åhäll and Borg 2013). No doubt is left about the quality of the extremism in question, the attribution tells us everything about the extremism that we need to know. All European institutions use variations of this expression, such as 'violent extremist activities' or 'violent extremist views.' Violence becomes inscribed in the term 'extremism,' making the term 'violent extremism' virtually redundant. Similar alliances between noun and adjective include 'extremist propaganda' and 'extremist ideology,' that still carry the predicated violence with them.

What is the EU IRU is actually tackling, then, when it speaks of 'terrorist and violent extremist content?' Judging by my analysis of Europol's policy documents, it predominantly targets online *propaganda*. The concept note sees the EU IRU as part of

> a coherent and coordinated European prevention strategy to counter terrorist propaganda and ensure that the Internet remains a public good, free of terrorist and violent extremist propaganda while respecting fundamental principles such as the freedom of speech (Europol 2015d, 2).

This suggests that radicalization is also seen as communication, or at least as the dissemination of terrorist propaganda. The EU IRU is, in this regard, an attempt to (re)gain control over the flow of information on the internet and keep a check on the usage of social media platforms "for radicalisation purposes, through terrorist and violent extremist propaganda" (Europol 2016e, 5).

In an interview, the Director of Europol said that "groups like IS are very good in their use of social media – IS alone is active on more than 20 platforms, including Twitter where it has, we are told, 5,000 accounts" (Wainwright, quoted in Banks 2016). Terrorists becoming social media savvy seems to be a considerable concern for law enforcement. Wainwright frames the scale of terrorists' social media operations as a threat and simultaneously worries about the propaganda being aimed at Western audiences.

> With the rise of social networking, hate propagators have evolved their techniques. […] they present themselves in a friendly and appealing way to attract young followers. Humour and satire are used to disguise hate speech (Europol 2015a, 13).

Statements such as this one assume a direct link between radicalization and propaganda that promotes and accelerates radicalization as a process. All it takes, according to Europol, is a certain susceptibility among members of the public for propaganda to resonate:

> It can be a matter of weeks, in some cases, for vulnerable young men or young women to have their minds turned by this ugly propaganda and to turn themselves into people capable of going to Syria or Iraq and engaging in conflict there, and in some cases carrying out terrorism (Wainwright 2016).

The 'mind-turning' effect of propaganda is a recurring frame in the context of the EU IRU. Although humans are exposed to media content almost everywhere all the time, terrorist propaganda is credited with having a particularly strong resonance. What kind of content is considered relevant online propaganda? Europol gave some clues as to this in a press release, naming "e.g. terrorist propaganda videos, pictures of beheadings, bomb-making instructions and speeches calling for racial or religious violence" (Europol 2016c).

Religious radicalization is a central interpretation scheme in many text segments. As mentioned before, references to Islam have been frequent in the TE-SAT reports, although references to 'religious inspiration' are now favored. Large shares of Europol's analyses remain preoccupied with "violent jihadist terrorists," and especially the "Islamic State" is the prime example given of a religiously inspired terrorist group (cf. Europol 2015c, 3ff). In many contexts, religious beliefs and motives are cited as causes of radicalization. The frame of religion (read: Islam) as the main driver behind radicalization to terrorism is part of Europol's knowledge production. Europol indicates that, when speaking of

> this shift away from the religious component in the radicalisation of, especially, young recruits, it may be more accurate to speak of a 'violent extremist social trend' rather than using the term 'radicalisation' (Europol 2015c, 6).

Europol's analysts see radicalization is so obviously linked to religion that they suggest using a different term if religion is *not* part of the equation. Interestingly, religious beliefs are downgraded to being a driver of radicalization, with an emphasis on "group structures" and "social bonds (common background, ethnic and geographical commonalities and language)" (ibid.).

Another frame that accompanies the notion of radicalization is that of *vulnerability*. In order for radicalization to resonate, targeted individuals need to be vulnerable (i.e. Europol 2015d, 4). A "certain vulnerability" is framed as an essential feature of potential terrorists, which is "picked-up by recruiters to be used as such" (Europol 2015c, 6). This vulnerability is especially attributed to young people, which usually means "individuals aged below 25" (cf. Europol 2015a, 41f). The vulnerability frame undermines the agency of these individuals and questions their judgment. Analysts are certain that age plays a role here because younger people are held to be more susceptible and radicalize quicker. The tropes of vulnerability and

religious radicalization are intertwined when Europol asserted that

> less than half of all persons arrested for joining IS or expressing/displaying any intention to do so have relevant knowledge about their religion and are thus vulnerable to interpretations of the Koran that fit IS logic (Europol 2015c, 6).

This frames terrorists as intellectually dependent persons who lack their own powers of reasoning to become terrorists. It also neglects social circumstances and political motives. Europol employs a consequentialist frame based on the model of cognitive radicalization. The IRU approach appears inevitable for those who aim to counter behavior based on expected consequences of radical ideas.

Whenever statements only make sense to readers if certain background knowledge is taken for granted, a *presupposition* applies. The idea that "patterns of radicalization have evolved and broadened" is a presupposition underpinning the policy debate of the EU IRU. It is also presupposed that "terrorism finds its inspiration in ideologies" and that "vulnerability" is a prerequisite for becoming radical. Often, these constructions take a certain context as given and make assumptions about causality and preferences. For example, the statement that "security is naturally one of citizens' greatest concerns" (European Commission 2016a, 17) takes a certain understanding of security for granted, one that is closely linked to European nation states' representation of reality. The prevalence of radicalization and the primacy of security is taken to be true by the formulation of Europol's European counter-terrorism policy.

2.1.3. Technology as the Problem

What role does technology play in the framing of the problem? Europol's publications on the EU IRU alternate between referring to terrorists' *use* and the *abuse* of the Internet. In this specific context, internet and social media are sometimes used interchangeably. Ambiguous references to the internet therein are a sign of practitioners' inner conflict when it comes to technology: Although it provides new opportunities and methods for law enforcement, it equally does so for criminals. Technology is constructed as a problem as soon as enemies are seen to be gaining an advantage from technical knowledge and means. This argumentation is also deployed in debates on encryption and 'cyber crime.' In the context of 'online radicalization' and 'propaganda,' these advances are more recent:

> Terrorists' use of the internet and social media has increased significantly in the recent years. [...] They have launched well-organised, concerted social media campaigns to recruit followers and to promote or glorify acts of terrorism or

violent extremism (Europol 2015e).

Dealing with propaganda and recruitment campaigns is not necessarily the task of police officers. The above statement exemplifies why terrorists' and extremists' progress in digital innovation is seen as a problem for law enforcement, although this field traditionally lies outside the remit of policing. To accommodate this, Europol's sense-making has to strike a balance between describing social media activities as 'terrorism' (read: high priority) and labeling them as 'criminal acts' (read: policing duty). They are therefore often named together; for example, when concerns are voiced that "the Internet has become a principal instrument for facilitating organized crime and terrorism" (Wainwright in Adamson 2016).

Threat construction is promoted by referring to the scale and speed associated with technology. Policy documents explain that "[t]he nature of terrorist communication on the Internet is constantly changing as a result of new technologies" and emphasize how terrorist groups "adapt their approaches to communication, exploiting new methods for interaction and networking on the Internet" (Europol 2015a, 12). In one public statement, Europol Director Rob Wainwright said that "technology is not always a friend of society and is, in fact, part of the security challenge we face today" (Wainwright in Banks 2016). This framing of social networks – and digital technology in general – as a threat to security occurs frequently and mostly focuses on the role of social networks in disseminating propaganda and facilitating recruitment.

Similar claims about technology as a security threat are made in the European Commission's communications, which stress the scope, velocity, and effectiveness of social media propaganda:

> Terrorist groups and extremists are capitalising on advances in technology to find new ways of engaging with disaffected youth, taking advantage of social networking sites, online video channels and radical chat rooms. They are spreading their propaganda more widely, more rapidly, and more effectively (European Commission 2014a, 2).

European policy-makers associate a loss of control with technology that they seek to tackle. They acknowledge that law enforcement struggles to regulate access to certain material, which is attributed to the nature of digital technologies (European Commission 2014a, 9; Council of the EU 2015a, 10).

Framing technology as facilitating terrorism rests upon a linear and simplistic understanding of radicalization; mere exposure to certain content is constructed as a problem. Sometimes

this direct causal relationship between internet content and terrorism is even explicitly stated, for example, in a report given by the EU Counter-Terrorism Coordinator, which mentions that a person attempting an attack on a Thalys train "looked at preaching on the internet prior to the act" (EU Counter-Terrorism Coordinator 2015b, 2).

2.1.4. Free Movement as a Security Threat

Another frame that I was able to identify during the coding process was the link between terrorism, extremism, and migration. The phenomenon of so-called *foreign fighters*, people traveling to war zones (mostly Iraq and Syria) to participate in combat training and join terrorist groups, is brought up frequently. Although the idea of people choosing to engage in violent struggles outside one's home country is in no way a new phenomenon, the number of people deciding to become foreign fighters is 'unprecedented,' according to Europol. Why is this relevant for European law enforcement? Mostly, because "the increasing number of travelers and returnees represents a significant threat to security in the EU" (Europol 2015a, 18). Europol Director Wainwright recently publicly cited the figure of 5,000 Europeans who returned to Europe after having been "radicalized by IS" and "could be plotting terrorist atrocities like those seen in Paris and Brussels" (Wainwright, quoted in Banks 2016).

This frame is not limited to foreign fighters returning home from battles, but potentially includes all *Muslim refugees* associated with the current war zones:

> A real and imminent danger, however, is the possibility of elements of the (Sunni Muslim) Syrian refugee diaspora becoming vulnerable to radicalisation once in Europe and being specifically targeted by Islamic extremist recruiters (Europol 2015c, 3).

Europol's policy documents draw an explicit connection between terrorism and migration. This frame extends well beyond the realm of regulating internet content, and fits the broader issue of (in)securitization of migration. This includes the increased criminalization of *migrant smuggling* (Europol 2016b). Interestingly, Europol declares that

> although a systematic link between migrant smuggling and terrorism is not proven, there is an increased risk that foreign terrorist fighters may use migratory flows to (re)enter the EU (Europol 2016g).

Despite the absence of proof of a link between 'illegal immigration' and terrorism, migrant smuggling has become a top priority in European (in)security politics. Wainwright says that human traffickers "range from taxi drivers to international smuggling syndicates" (in Banks 2016). There is insufficient space to discuss the development and challenges of European

migration policy in-depth within the scope of this thesis. However, I would like to note that the reinforced connection to law enforcement practices is evident in Europol's policy frames. This includes, as explained above, the mission of the EU IRU, which is also in charge of monitoring and referring online content posted by traffickers who facilitate 'illegal immigration.'

2.1.5. Location of the Problem and Attribution of Roles

The Critical Frame Analysis method provides a structure for incorporating the location and roles of the problem in the analysis of policy texts. Although it proved difficult to discursively locate the problem of 'radicalization to terrorism,' the texts provide a number of hints as to where the problem allegedly originates from.

Terrorist activity is always constructed as being enacted by an out-group that is clearly distinct from the norm-group or in-group. Over the last 15 years, most terrorist activity was attributed to jihadi groups based outside of Europe. The emergence of 'homegrown' jihadi terrorism complicated this clear 'in vs. out' distinction, since 'violent extremists' are also found in many EU Member States. Nonetheless, jihadi extremists are still regarded as an extreme out-group of society that is excluded from mainstream society.

As one interviewee confirmed, the problem holders are still held to be Muslims, and right-wing extremist activity or right-wing terrorism is only framed as a reaction to Islamist extremism. Structural racism is neglected as a cause for growing nationalist and far-right movements. "Acts of violence by Islamic State have the potential to increase the number and intensity of extreme-right wing activities, both legal (e.g. demonstrations) and illegal (e.g. violent acts), in EU Member States" (Europol 2015a, 7). This logic of extremism (the Islamist one) inciting backlash extremism (by the far right) leads policy-makers to make the assumption that they can kill two birds with one stone if they successfully tackle Islamist radicalization. The established out-group (Muslims) remains the most dangerous out-group. It also appears more politically opportune to place the consequences of alienating (in)security practices solely on the Muslim community.

From what has been presented thus far, two observations about the locations of radicalization can be made. Firstly, radicalization and violent extremism are attributed to Islamist ideologies. The presumed link between holding strong beliefs and acting in a radical way demonstrates this. Secondly, radicalization is increasingly located on the internet. One interviewee told me that 'part of the radicalization process' is assumed to 'happen online,'

which is still constructed as a separate sphere of life.

Framing the problem as located on the internet highlights the transnational character of the threat. As the European Commission puts it in a strategy paper:

> Radicalisation crosses national boundaries in many ways. For example, the use of chat rooms, social media, and other online tools often has an international dimension. The type of threats Member States face are often similar, so it can be effective to take action at the EU level (European Commission 2014a, 3).

Online radicalization becomes, by definition, a European issue, to be tackled by European policies. As Europol is at the heart of European (in)security architecture, growing this agency's competences and capacities appears compelling.

Who is active and who is passive in Europol's problem framing? To some extent, a distinction between perpetrators and victims of radicalization is recognizable. As pointed out above, radicalization is connected to 'vulnerable' groups of victimized individuals who become radicalized by "Islamic extremist recruiters" (Europol 2015c), "radicalizers," and "radical preachers" (European Commission 2014a). Thereby, responsibility is shifted onto ideologues acting behind the scenes, leaving little room for autonomy of potential terrorists.

The depoliticization of terrorist motivations is a common theme; terms such as 'disengagement' and 'rehabilitation' are employed that portray terrorists' behavior as socially or psychologically abnormal. As mentioned above, Europol has increasingly established a connection between terrorism and crime. From this point of view, the desperate and confused logic of vulnerable individuals can be applied to the problem group of petty criminals:

> The link between terrorism and crime is much more prevalent now than at any other time in the past. The recruits we are seeing now are more and more from a criminal background, a criminal lifestyle (Wainwright 2016).

There are empirical clues that suggest a link between crime and terrorism: Six out of the ten attackers in Paris last year had a 'criminal background' and all of the Brussels attackers were known to the Belgian police for their criminal backgrounds. However, it still remains unclear if there is a direct relationship between committing petty crimes and planning and executing a terrorist attack. Even though the same individual might undertake both activities, they may do so for entirely different reasons.

Incidentally, considerations of gender roles are largely absent from discussions about Europol's conceptions of radicalization and violent extremism. Feminist security studies have long criticized that women's and gendered perspectives are overlooked and marginalized,

despite their powerful explanatory potential. The TE-SAT mentions that

> The number of young women and minors traveling out to Syria and Iraq has been reported as increasing from some EU Member States in 2014 [...]. Some women have followed their husbands to the conflict zones (some with children have also traveled), and some single women have since married fighters (Europol 2015a, 23).

This captures the typical representation of women* in security policy analyses: Lumping together 'young women and minors' as if they were one entity, displaying them to be fully passive and dependent upon men.

2.2. Prognosis – How Can the Problem Be Solved?

The second part of the text analysis is called prognosis, leaning on, again, the Critical Frame Analysis terminology. The sensitizing question – 'How can the problem be solved?' – informs this section.

2.2.1. Ever Closer Police Cooperation

Increasing cooperation among European police and intelligence agencies is Europol's number one demand for improving (in)security in Europe. The corner stone of this claim is the improvement of information sharing within Europe, with Europol acting as the central hub. The "fight against terrorism in the EU" is emphasized as the motivation behind this ambition, but other policy areas are, as has been shown, likely to follow suit. The creation of the European Counter-Terrorism Centre (ECTC) is one example that shows how the aim to provide 'coordinated reaction' to terrorism became more institutionalized. One of my interviewees called the creation of the ECTC a mere ad-hoc "marketing activity," whereas Europol officially says that the ECTC "will lie at the heart of a stronger EU standing up to the threat of terrorism" (Europol 2016a).

Recently, Europol said that "information sharing in the area of counter terrorism advances in quantity and quality, requiring continuous commitment by all stakeholders to keep pace with the terrorist threat" which calls for "unprecedented levels" of information to be shared (Europol 2016e, 9). The new Europol regulation is also framed as enhancing Europol's "role as the central hub for information exchange" (Europol 2016d). The main obstacle to sharing information is seen as a cultural issue instead of a legal or political one, since some Member States have "different views, different cultural attitudes, towards sharing." Europol Director Wainwright says

> there is still a cultural journey that the whole community is on, to open up a little bit more the posture of sharing, given the traditional mindset of intelligence officers needing to hold on to information, to protect sources (Wainwright 2016).

As my interviewees confirmed, recent attacks provided momentum to overcome said 'cultural' barriers and push for an increased exchange of information. With national security considered the essential component of national sovereignty, many Member States have long been reluctant to open up to sharing what is seen as sensitive information on a Europe-wide level. 'Trust' had to be built up to present Europol as a 'reliable partner.' In early 2016, Wainwright publicly declared that "I have been talking with people like me for 10 years about improving information sharing [...] but this is the first time where I can remember it becoming a mainstream issue" (Wainwright in Paravicini 2016).

Apart from event-driven calls for closer cooperation, the 'added value' of European information sharing is also frequently emphasized in Europol's documents. Arguing for greater 'effectiveness' frames Europol as a service provider for the Member States, a self-understanding that was confirmed during my interview with a Europol official. Member States' counter-terrorism agencies are seen as the leading actors, "supported by a pro-active EU central information hub at Europol" (Europol 2015f, 5). The same efficiency argument is also applied to other policing areas, such as organized crime or cybercrime (i.e. Europol 2015b, 14). The EU IRU capabilities are also based on close cooperation with Member States and described as a community effort:

> The full impact of the IRU, however, will be delivered by leveraging the combined resources of social media partners and national expert contact points [...] working as a concerted community through the EU IRU at Europol (Europol 2015e).

The framing of cooperation as increasing surveillance and take-down efficiency is prevalent in the debate about the EU IRU. Another argument is made about open intelligence on social media. There are cases in which law enforcement or intelligence services investigate certain websites or accounts to gain intelligence about suspect groups or suspect individuals, and in which taking down content would undermine surveillance of a site or account. For example, Twitter accounts may provide GPS coordinates or information about local events, which can be relevant for intelligence services. Cooperation through the EU IRU is supposed to "act as a European deconfliction structure." This means that information is also shared about contents that are meant to stay online for the purpose of gathering intelligence (Europol 2015d, 5).

Closer cooperation with Member States also entails enhancing capacities on the European level. Unsurprisingly, Europol emphasizes its own expertise and competences as often as it can. When justifying the creation of the EU IRU, Europol's special knowledge on the topic is repeatedly emphasized. Accordingly, Europol is portrayed as being best positioned to handle the removal of illegal content on the internet due to the comprehensive expert assessment of propaganda that it can provide. Europol officials see themselves as ahead of some Member States in the area of unwanted internet content and want to support the competent national authorities with strategic and operational analysis (Europol 2015d, 5).

2.2.2. Partnership with Private Actors

> With the support of the European Commission, social media companies are continuously approached to ensure, in particular, awareness concerning the political objectives of the prevention of radicalisation and the importance of a swift implementation of referred internet content. It has also been noticed that social media companies are starting to intensify own monitoring activities to remove propaganda material and extremist material (Europol 2015f, 12).

The novelty of the IRU approach is its lack of coercion in cooperating with private companies. There have been prior forms of voluntary cooperation between European law enforcement and the industry, most importantly in the field of cyber security (i.e. Europol 2015b, 12). But the "increased partnership" that aims to "promote 'self-regulation' activities" (Europol 2016e, 7) on a non-contractual basis can be considered a new form of public/private cooperation at Europol. In some way, it is the soft-power approach to policing the web.

Cooperation with the internet industry is closely intertwined with the 'EU Internet Forum' set up by the European Commission to deepen 'engagement' and 'dialogue' with internet companies. The official aim of the forum meetings is "to secure industry's commitments to a common public-private approach and to jointly define rules and procedures for carrying out and supporting referrals" (Europol 2015d, 5). Europol does not entirely deny the need to legally "compel private industry with law enforcement" but sees "greater benefit in establishing and building working relationships in order to stimulate the voluntary and proactive engagement of the private sector" (Europol 2015b, 10). Several of my interviewees confirmed that Europol has a "good relationship" with private internet companies. The quality of the public private partnership is underlined, the EU Counter-Terrorism Coordinator has even suggested that "joint trainings" for members of law enforcement, industry, and civil society would be a good way to promote cooperation and mutual understanding (2015a, 3). As described above, little is known about the substance of cooperation within the Internet

Forum; NGOs heavily criticize it, while social media companies remain completely silent concerning cooperation with Europol. Europol's Director calls cooperation with private partners "constructive" (Europol 2015e) and "effective" (Adamson 2016).

Why is loose, non-contractual partnership presented as the 'best way' to reduce the spread of terrorist material online? The 'voluntary' nature of the cooperation draws upon the terms and conditions of the platforms as reference points for what is permissible and what is not. The EU IRU refers contents to the industry "to remove it on the basis that it breaches *individual companies' user policies*" (Europol 2015d, 2, own emphasis). Europol frames the activities of the IRU as something "any citizen could do," and consistently highlights the non-enforcing nature of the cooperation. Therefore, academic observers, such as American scholar J.M. Berger consider the dominance of privatized rules in regulating speech on social media as a "corporatocracy"[8].

2.2.3. 'Playing Whack-a-Mole' – Technology and Preventing the Unpredictable

The political goal of reducing 'terrorist and extremist material online' is repeatedly broken down and described by Europol in technocratic terms. Speaking of 'identifying, assessing, and referring' propaganda and violent extremist content frames the process as an expert-driven, high profile operation. Emphasizing that the related measures are fully based on the opaquely formulated terms of service of private companies, and, for instance, also including content posted by 'migrant smugglers' would turn these operations into a much more mundane practice.

In one document, the practice of the EU IRU is described as akin to playing "whack-a-mole" with terrorists (Europol 2015d, 4), referring to the popular redemption game, in which hitting one mole on the head with a mallet just makes another one pop up somewhere else. Similarly to a cat-and-mouse game, the 'mole-fighting' efforts ultimately remain reactive and limited in scope. Correspondingly, resilience to take-down measures seems to evolve and adapt quickly.

Industry representatives with long-standing experience in taking measures against spam bots on their platforms privately confirm that playing whack-a-mole is an accurate description of the effectiveness of take-down practices on the internet. Colloquially referred to as the "Streisand effect,"[9] the infamous counter-effectiveness of removing online material is broadly known to both law enforcement and industry.

8 https://twitter.com/vox_pol/status/746299342449942528 (last retrieved 24 June 2016)
9https://en.wikipedia.org/wiki/Streisand_effect (last retrieved 12 June 2016)

The fact that Europol is calling for more resources to beef up its IRU operations is understandable from an institutionalist perspective, but this neglects the structural set-up of the internet. In an attempt to gain full control of the internet, having larger capacities does not hurt. But in principle it seems likely that IRU operations will still merely continue to play whack-a-mole, even with faster computers and more staff. To address the political imperative to "prevent every terrorist attack" (Wainwright 2016), technological solutionism offers a trajectory for law enforcement to demonstrate action to at least "mitigate the consequences of technology being turned against us" (Wainwright in Adamson 2016). The European Commission acknowledges that the 'filter and remove' approach is an uphill battle:

> Whilst it is perhaps impossible to rid the internet of all terrorist material, we must do more to reduce the immense volume of material that is online and so easily accessible to our citizens (European Commission 2015).

"The gap [...] between law enforcement's ability to track criminal activity online and our adversaries' ability to abuse technological advances" (Wainwright in Adamson 2016) drives Europol's wishes to obtain more resources and competences. One attempt to make the filtering and removing of online content more effective is the introduction of so-called upload filters, which help prevent blocked material from being republished. This works based on digital fingerprints of content, such as a picture or video, that allow platforms to recognize material even if it has been adjusted or altered. If someone tries to upload a file listed in the filter database, the upload is blocked.

Regardless of the technical means available, the policy framing of the IRU is clearly loaded with a striking imbalance between terrorist activities being unpredictable and an ever-stronger urge to prevent all attacks from occurring. When talking about "foreign fighters", Wainwright said that "we suspect that about one-third of them have come back: That is our best guess. We don't know for sure" (Wainwright 2016). Wanting to know when and where terrorist attacks will happen in advance may be an understandable desire on the part of law enforcement, but it also seems completely hopeless. Europol acknowledges this, stating that "the threat is persistent and terrorist attacks are *unpredictable*. Terrorism can strike anywhere at any time. It is therefore crucial that we work together to do what we can to pre-empt this threat" (Europol 2015d, 4, own emphasis). Lacking the ability to effectively exercise coercion makes the focus of law enforcement shift from prevention to preemption. In the context of radicalization on the internet, the IRU approach is framed as a key instrument in that it "combines both preventive – flagging and suspension – and pro-active measures; in

particular dynamic intelligence gathering to inform the flagging process" (Europol 2015d, 5).

Europol's self-perception as a leading center of expertise on this issue guides its approach to establish preemptive capabilities at the EU IRU:

> Ultimately, the EU IRU should be in a position to anticipate and pre-empt terrorist abuse of social media and play a pro-active advisory role vis-à-vis Member States and the private sector. It will act as an EU centre of excellence with a dedicated research and analysis team, formed of practitioners from law enforcement, the academia and the private sector which will underpin this work, helping to maintain current knowledge and a dynamic online research capability (Europol 2015d, 6).

This vision for the EU IRU seems still a long way down the road, but given the recent frequency of attacks, further growth in resources and institutional capacity seems likely. Though the imbalance between the measures taken and the conceptual foundation of the measures is striking, more research and analysis is needed. The central presupposition for the EU IRU remains that preventing radicalization serves to preempt terrorism in Europe, although this causal relationship is not scientifically proven, and may be impossible to prove. However, it continues to inform counter-terrorism policy-making on the European level because it is a presupposed frame. Breaking down the logic of preempting radicalization might be the only way to develop more effective approaches to tackling violent assaults, both on- and offline.

V. Conclusion

1. Summary of Analysis – The Main Frames

I used Critical Frame Analysis to examine what was selected as the policy problem and how this was labeled by Europol. My practice of naming and categorizing different aspects of the security threat revealed the ambiguous and vague use of related terms, even at the working level. Terrorism is ‘naturally’ taken as a high priority threat, yet no in-depth engagement with the term could be found. The misleading presentation of facts and statistics in the TE-SAT suggests a biased framing of counter-terrorism as the leading policy priority in European security.

Radicalization is framed as an insightful concept, one that is taken for granted despite the unclear and shaky scientific evidence behind it. This is reflected in the ambivalent use of the term to describe both a process and a condition. Radicalization is equated with online communication and the dissemination of propaganda. Reconfirming the critical theoretical debates on (counter-)radicalization, a strong link between radicalization and Islam was also prevalent. Religious radicalization is exclusively read as Islamic radicalization, adding to the dominant boundary drawing threat construction in Western counter-terrorism policy. Bundled with vulnerability as a precondition for effective radicalization, the group of problem holders is framed as young Muslim men – a common storyline, as presented in the theory section. Unlike radicalization, extremism features only marginally in the analyzed policy text. Most striking was the entanglement of extremism with violence, which contributes to the (in)securitization of radical ideas.

Europol frames technology as a security problem that is associated with a loss of control and a new dimension of threats – a gateway for terrorism and radicalization. The internet is not seen as the cause or source of terrorism, but framed as a facilitating means that therefore poses a risk. Following the radicalization frame, the mere exposure to certain content is constructed as a problem for law enforcement.

The direct link between migration and terrorism also frames free movement as a security threat, that is also strongly associated with Muslim refugees and foreign fighters. In all texts, the problem is located within Islamic ideologies that not only produce Islamist terrorism but also subsequently provoke far-right extremism as a counter-reaction.

Responses to what the problem is represented to be are both relatively banal and surprising. Promoting closer police cooperation in Europe and increasing information sharing appear to be straight-forward steps towards enhancing efficiency and effectiveness in European (in)security production. Terrorists are exploiting weak European security cooperation and Europol is framed as the right agency to tackle this issue. Pushes for closer partnership with private actors implicitly concede that law enforcement indeed lacks of control over digital communication and is struggling to resolve this on its own. Law enforcement's ceding of any direct claim to be an enforcing party is reflected in the lack of coercion or legal compulsion in its cooperation with private companies. This approach makes perfect sense for Europol, since it does not have any executive authority in the first place. It will be crucial to closely observe the developments in cooperation between police and private platforms in the regulation of speech on the national level.

Comparing the diagnosis and prognosis reveals how Europol's approach is both balanced and unbalanced: If one understands radicalization in the way that Europol understands it, the presented solutions make sense. However, Europol's concessions to the fact that the IRU approach is strikingly ineffective make the agency's approach appear inconsistent. That Europol admits the IRU is playing whack-a-mole on the internet, can be interpreted in two ways: The measure is either a symbolic reaction to the previous attacks that created political opportunity structures, or it is to be understood as a preparatory measure that will increase in effectiveness as technology advances in the future. In any case, its existence allows Europol to praise its own expertise and increase its financial resources, which follows rationalist bureaucratic logic.

Interpretive approaches can help overcome presuppositions and biased perspectives. I hope to have demonstrated one way in which it might be possible to combine critical interpretation and empirical analysis in research.

2. Reflection on Research Results – Root Causes and Corporatocracy

Policy and research engaging radicalization remain limited to addressing radicalization's symptoms. Asking if and how certain material resonates instead of obstinately blocking and filtering content regardless of the individual situation would move the debate forward. Failing to take context into account and focusing on mere exposure to certain material undermines empirical radicalization research and the development of counter-radicalization

policy. The case of the EU IRU also strongly advises us not to overestimate the role of internet content and ideology in radicalization.

Although academia knows that take-down measures only treat symptoms, and civil society organizations know this too, and law enforcement also acknowledges this, the presented frames appear to be stable and durable. Other, more creative ways of perceiving and conceptualizing online radicalization and online extremism are necessary – and they must be grounded in relational concepts. Technology alone does not cause and will not solve radicalization. At the time of writing, the capacity of the EU IRU is still limited, but the erroneous reasoning behind it is a problem that continues to clamp down on freedom of speech. In other parts of the world – such as war zones or areas under authoritarian regimes – IRU-type approaches are far more advanced and harmful to society (e.g. Pizzi 2014). More effective approaches to violent and hateful internet content are needed, but they have to uphold human rights and transcend the delusive logic of online radicalization.

It must also be ensured that there are no double standards when it comes to freedom of expression. At the EU IRU, the restrictions point unilaterally towards Islam. In other crisis situations, for example, in Ukraine or in right-wing terrorism, the take-down of content is discussed and applied to a much lesser extent. At the same time, the IRU's targeting of 'illegal migration' shows that reasons for surveillance and taking down speech could potentially extend far beyond the traditional security realm. This could easily be extrapolated to a familiar pattern of incrementally impinging on civil liberties, introducing measures for seemingly uncontroversial cases (like videos of beheadings), putting infrastructure in place, and slowly but surely expanding the scope of the policy.

The EU IRU is not the determining driver of the privatization of regulation of speech on social media platforms. The fact that the ownership and control over most large social media outlets and the internet infrastructure lies in the hand of private actors is a broader, global development. Nevertheless, the EU IRU is clearly not a symbolic policy; it does have substantial impact on the changing interface between the public and private enforcement of law. The strategic use of cooperation with private firms is growing in other fields as well, for example, in fighting ransomware (Europol 2016j). The black-box-like character of companies such as Facebook or Google is strategically used to secretly leverage filtering practices. When private companies become enforcing actors, we move from questions of 'is a piece of content legal?' to 'is it politically and commercially eligible?' Of course, all private media platforms have curative freedom in designing their services and outlets. That being said, if an

instrument similar to the IRU were to be implemented in a non-digital medium, such as a large daily newspaper, it would probably be called ‘state censorship’ or ‘political exercise of influence,’ and the public outcry would most likely be immense.

It should be the task of digital social work, not police repression, to combat hateful material on the internet. In a report, a representative of the internet industry is quoted as saying “Governments think ISIS is amazing at social media, but in reality governments just suck at it. ISIS is just operating in the same way as teens and digital natives” (Brown and Cowls 2015, 89f). It might be worthwhile to consider capacity building in political education and media literacy on a Europe-wide level. Holistic approaches need to be developed, ones that embrace online and offline communication as one inseparable sphere in order to overcome technological solutionism and political biases.

In order to accomplish this, we need to employ security concepts that are effective, in line with fundamental rights, and which adhere to democratic principles of accountability. Criticizing and dismantling modern radicalization policy is a pivotal point for re-conceptualizing (in)security in a relational, non-essentialist, non-racist, non-discriminatory way.

VI. Appendix

1. Coding System

My coding system combines theoretical and methodological code categories. The code categories are ordered according to analytical steps. The order of codes within each code category does not imply a hierarchy, they are listed in alphabetical order.

Code Category	Code	Exemplar
Facts Coding rule: Dates, numbers, official descriptions, definitions and other "raw" information about the EU IRU.	ECTC facts	"The ECTC operates within Europol's existing (regulatory) framework and organisational structure, as well as already available resources"
	evolution of IRU	"The EU and its Member States have developed several initiatives related to countering radicalisation and terrorism on the internet"
	identify	"based on our knowledge we make a triage based on what is interesting and what is not"
	internet content	"more than 46.000 Twitter accounts were used by supporters of the Islamic State"
	IRU facts	"The specific objective of this Unit is reducing the level and impact of terrorist and violent extremist propaganda on the internet"
	legal basis	"new offences of public provocation, recruitment and training for terrorism were introduced by Framework Decision 2008/919/JHA"
	referral	"we give information back to the plattform that [...] this content is promoting terrorism or violent extremism"
	UK CTIRU	"The UK CTIRU had previously launched a national appeal for internet users to report harmful extremist and terrorist material"
Code Category	**Code**	**Exemplar**
Diagnosis Coding rule:	crime & terrorism	"In many cases they were perpetrated by radicalised, known individuals, often with a history in organised crime"

In-vivo codes that answer the sensitizing questions: – What is represented as the problem? – Why is it seen as a problem?	foreign fighters	“The significant number of EU citizens engaged as suspected ‘foreign terrorist fighters’ in Syria and Iraq”
	migration	“While a systematic link between migrant smuggling and terrorism is not proven, there is an increased risk”
	prevention	“prevention strategies such as suspending social media accounts or removing terrorist and violent extremist content”
	prioritization	“we are aiming for the content that is having the most impact on the radicalization”
	propaganda	“reduce the abuse of the Internet by terrorists for propaganda purposes”
	terrorism	“Sophisticated attacks are violent terrorist attacks that are carefully planned, directed against specific targets and professionally executed by focused, well trained and fully prepared operatives”
	threat description	“Clear international dimension in the planning and coordinating of attacks, involving a network”
	vulnerability	“vulnerable individuals”
	women/gender	“The number of young women and minors travelling out to Syria and Iraq has been reported as increasing”
	youth	“engaging with disaffected youth”
Code Category	**Code**	**Exemplar**
Prognosis <u>Coding rule:</u> In-vivo codes that answer the sensitizing questions: – How can the presented problem be solved? – What is the priority in goals? – What are means and mechanisms to achieve goals?	closer cooperation	“achieve results in the fight against terrorism and cross-border crime only if all actors concerned do more to work better together”
	cooperation with Member States	“engender trust and raise awareness among national counter terrorism authorities about existing cooperation instruments at EU level”
	cooperation with private actors	“increase partnerships (with the support of the European Commission) towards online service companies (to promote ‘self-regulation’ activities)”
	counter-speech	“Member States and EU institutions are encouraged to develop strategic communications and counter-narrative

		policies”
	Europol expertise	“ increase the visibility of Europol’s related services and tools”
	ideology	“terrorism in Europe now finds its inspiration in a variety of ideologies”
	information sharing	“Unprecedented levels of information are shared through Europol, requiring continued operational support”
	migrant smuggling	“carry out internet referral activities in relation to facilitated illegal immigration, by detecting internet content used by traffickers to attract migrants and refugees”
Code Category	**Code**	**Exemplar**
Radicalization <u>Coding rule:</u> In-vivo codes that focus on the different connotations radicalization in the texts.	extremism	“English-language extremist media produced by terrorist groups have continued to encourage western nationals”
	radicalism as a condition	“after he got radicalised”
	radicalization as a process	“the speed of radicalization is often startling”
	reference to Islam	“Jihadist groups in particular have shown a sophisticated understanding of how social networks operate”
	religiously inspired	“attacks were classified as religiously inspired”
Code Category	**Code**	**Exemplar**
Roles <u>Coding rule:</u> Codes that follow the CFA method, answering the sensitizing questions: – Who is seen to have made the problem? – Whose problem is it seen to be? – Who is attributed active and passive roles?	active roles	“Islamic extremist recruiters”
	passive roles	“protect the refugee population from radicalisation”
	role of technology	“ensure that Internet remains a public good”
	roles in diagnosis	“They have established networks of influential accounts across multiple social media platforms”
	roles in prognosis	“We are coordinating operations against some of the most dangerous criminal and terrorist groups operating in Europe”
	subject positioning	“Europeans need to feel confident that wherever they move within Europe their freedom and their security are well protected”

Code Category	Code	Exemplar
Language Coding rule: Pre-defined codes for different expressions and rhetorical tropes.	causality mechanism	"Acts of violence by Islamic State have the potential to increase the number and intensity of extreme-right wing activities"
	metaphor	"Terrorism in Europe feeds on extremist ideologies"
	normative terms	"exploit the internet to radicalise"
	othering	"core European values have been attacked"
	predication	"violent extremist"
	presupposition	"abuse of social media by terrorist organisations is a dynamic phenomenon"

Table 2: Overview of code categories and codes.

2. List of Coded Material

From Europol:

- Europol. 2015. "Changes in Modus Operandi of Islamic State Terrorist Attacks." Public Information. https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks.
- Europol. 2015. "The Internet Organised Crime Threat Assessment (IOCTA)." Threat Assessment. https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.
- Europol. 2007-2015. "Terrorism Situation and Trend Report (TE-SAT)." Threat Assessment. https://www.europol.europa.eu/latest_publications/37.
- Europol. 2015. "EU Internet Referral Unit at Europol - Concept Note." Report. http://www.statewatch.org/news/2015/may/eu-council-internet-referral-unit-7266-15.pdf.
- Europol. 2015. "Enhancing Counter Terrorism Capabilities at EU Level: European Counter Terrorism Centre (ECTC) at Europol and Counter Terrorism Related Information Sharing." Report. http://www.statewatch.org/news/2015/nov/eu-council-europol-ECTC-14244-15.pdf.
- Europol. 2015. "Europol's Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda." Press Release. https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda.
- Europol. 2016. "Europol's European Counter Terrorism Centre Strengthens the EU's Response to Terror." Press Release. https://www.europol.europa.eu/content/ectc.
- Europol. 2016. "Migrant Smuggling in the EU." Public Information. https://www.europol.europa.eu/sites/default/files/publications/migrant_smuggling__europol_report_2016.pdf.
- Europol. 2016. "Europol Joins UK Appeal to Report Extremist and Terrorist Material Online Using red 'STOP' button." Press Release. https://www.europol.europa.eu/newsletter/europol-joins-uk-appeal-report-extremist-and-terrorist-material-online-using-red-stop-but.

- Europol. 2016. “Europol launches the European Migrant Smuggling Centre.” Press Release. https://www.europol.europa.eu/content/EMSC_launch.
- Europol. 2016. “Europol and Interpol issue Comprehensive Review of Migrant Smuggling Networks.” Press Release. https://www.europol.europa.eu/newsletter/europol-and-interpol-issue-comprehensive-review-migrant-smuggling-networks.
- Europol. 2016. “New Regulation Boosts the Roles of EDPS and Europol.” Press Release. https://www.europol.europa.eu/newsletter/new-regulation-boosts-roles-edps-and-europol.
- Europol. 2016. “European Parliament Adopts New Regulation for Europol.” Press Release. https://www.europol.europa.eu/content/european-parliament-adopts-new-regulation-europol.
- Europol. 2016. “Enhancing Counter Terrorism Capabilities at EU Level: European Counter Terrorism Centre (ECTC) at Europol.” Report.
- Wainwright, Rob. 2016. “Online Terrorist Propaganda Being Done on a Scale Not Seen Before, Says EU Police Chief.” Interview. https://www.theparliamentmagazine.eu/articles/news/online-terrorist-propaganda-being-done-scale-not-seen-says-eu-police-chief.
- Wainwright, Rob. 2016. “Security, Terrorism, Technology ... and Brexit.” Interview. http://esharp.eu/conversations.
- Wainwright, Rob. 2016. “Paris Attacks Prompt EU to Share Secrets.” Interview. http://www.politico.eu/article/paris-attacks-prompt-share-secrets-eu-security-forces-eurodac-schengen-information-system-terrorism-isis-isil-islamic-state-bataclan/.
- Wainwright, Rob. 2016. “Europe’s Top Cop Warns More Attempted Attacks ‘Almost Certain.’” Interview. http://time.com/4336919/europol-terrorist-paris-brussels-rob-wainwright/.

From the European Commission:

- European Commission. 2014. “On the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.“ Report. http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/crisis-and-terrorism/general/docs/report_on_the_implementation_of_cfd_2008-919-jha_and_cfd_2002-475-jha_on_combating_terrorism_en.pdf
- European Commission. 2014. “Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU’s Response.” Report. http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/crisis-and-terrorism/radicalisation/docs/communication_on_preventing_radicalisation_and_violence_promoting_extremism_201301_en.pdf.
- European Commission. 2015. “European Agenda on Security - State of Play.” Fact Sheet. http://europa.eu/rapid/press-release_MEMO-15-6115_de.htm.
- European Commission. 2016. “Delivering on the European Agenda on Security to Fight against Terrorism and Pave the Way towards an Effective and Genuine Security Union.” Report. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents/docs/20160420/communication_eas_progress_since_april_2015_en.pdf.

From the EU Counter-Terrorism Coordinator and the Council of the EU:

- Council of the EU. 2014. “Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism.” Strategy Paper. http://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf.
- Council of the EU. 2015. “Riga Joint Statement.” http://data.consilium.europa.eu/doc/document/ST-5855-2015-INIT/en/pdf.
- Council of the EU. 2015. “Fight against Terrorism: Follow-up to the Council (Justice and Home Affairs) of 12-13 March 2015 - Implementation of Counter-Terrorism Measures.” Meeting Document. http://www.statewatch.org/news/2015/jul/eu-cosi-ct-9418-15.pdf.
- Council of the EU. 2015. “The Functioning of the Internet Referral Unit (EU IRU) on the Basis of the Future Europol Regulation.” Meeting Document. https://netzpolitik.org//wp-upload/council1497-15.pdf.
- EU Counter-Terrorism Coordinator. 2015. “EU CTC Input for the Preparation of the Informal Meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015.” Report. http://www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf.
- EU Counter-Terrorism Coordinator. 2015. “Follow-up to the Statement of the Members of the European Council of 12 February 2015 on Counter-Terrorism: State of Play on Implementation of Measures.” Report. http://www.statewatch.org/news/2015/sep/eu-council-ct-implementation-plan-12139.-15.pdf.

3. Interviews

Five background interviews were conducted with practitioners and experts on European security policy, especially regarding the topics of police cooperation and counter-terrorism. These interviews are not directly quoted in the text, but provided important background information for the analysis.

4. Bibliography

Adamson, Paul. 2016. “Security, Terrorism, Technology ... and Brexit.” *E!Sharp.eu*, May. http://esharp.eu/conversations.

Adler, Emanuel, and Vincent Pouliot, eds. 2012. *International Practices*. Cambridge University Press.

Åhäll, Linda, and Stefan Borg. 2013. “Predication, Presupposition and Subject-Positioning.” In *Critical Approaches to Security: An Introduction to Theories and Methods*, edited by Laura J. Shepherd, 196–207. London ; New York: Routledge.

Alimi, Eitan Y., Chares Demetriou, and Lorenzo Bosi. 2015. *The Dynamics of Radicalization: A Relational and Comparative Perspective*. Oxford University Press.

Amicelle, Anthony, Claudia Aradau, and Julien Jeandesboz. 2015. “Questioning Security Devices: Performativity, Resistance, Politics.” *Security Dialogue* 46 (4): 293–306. doi:10.1177/0967010615586964.

Amoore, Louise, and Marieke De Goede. 2008. “Transactions after 9/11: The Banal Face of the Preemptive Strike.” *Transactions of the Institute of British Geographers* 33 (2): 173–85. doi:10.1111/j.1475-5661.2008.00291.x.

Bacchi, Carol Lee. 2009. *Analysing Policy: What's the Problem Represented to Be?* French Forest, N.S.W: Pearson.

Balzacq, Thierry, Didier Bigo, Tugba Basaran, Emmanuel-Pierre Guittet, and Christian Olsson. 2010. "Security Practices." In *The International Studies Encyclopedia*, edited by Robert Allen Denemark, 17. Malden, MA: Wiley-Blackwell. http://www.blackwellreference.com/subscriber/uid=3/book?id=g9781444336597_9781444336597.

Banks, Martin. 2016. "Online Terrorist Propaganda Being Done on a Scale Not Seen Before, Says EU Police Chief." *The Parliament Magazine*. May 30. https://www.theparliamentmagazine.eu/articles/news/online-terrorist-propaganda-being-done-scale-not-seen-says-eu-police-chief.

Bartlett, Jamie, and Ali Fisher. 2015. "How to Beat the Media Mujahideen." *Demos Quarterly*. February 5. http://quarterly.demos.co.uk/article/issue-5/how-to-beat-the-media-mujahideen/.

Bigo, Didier. 1996. *Polices en réseaux : l'expérience européenne*. Paris: Presses de la Fondation Nationale des Sciences Politiques.

———. 2000. "When Two Become One." In *International Relations Theory and the Politics of European Integration. Power, Security and Community.*, edited by Morton Kelstrup and Micheal Charles Williams, 171–204. London & New York: Routledge.

———. 2005. "L'impossible cartographie du terrorisme." *Cultures & Conflits*, February. https://conflits.revues.org/1149.

———. 2006. "Security, Exception, Ban and Surveillance." In *Theorizing Surveillance: The Panopticon and Beyond*, edited by David Lyon, 46–68. Cullompton, Devon: Routledge.

———. 2008. "Globalized (In)Security: The Field and the Ban-Opticon." In *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes After 9/11*, edited by Didier Bigo and Anastassia Tsoukala, 1sted., 10–48. London ; New York: Routledge Chapman & Hall.

———. 2011. "Pierre Bourdieu and International Relations: Power of Practices, Practices of Power." *International Political Sociology* 5 (3): 225–58. doi:10.1111/j.1749-5687.2011.00132.x.

Bigo, Didier, Laurent Bonelli, Dario Chi, and Christian Olsson. 2007. "Mapping the Field of the EU Internal Security Agencies." *The Field of the EU Internal Security Agencies*, 5–66.

Bigo, Didier, Laurent Bonelli, Emmanuel-Pierre Guittet, and Francesco Ragazzi. 2014. "Preventing and Countering Youth Radicalisation in the EU." Study for the LIBE Committee. Brussels: European Parliament. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509977/IPOL-LIBE_ET%282014%29509977_EN.pdf.

Bigo, Didier, and Anastassia Tsoukala. 2008. *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes After 9/11*. 1sted. London ; New York: Routledge Chapman & Hall.

Bijker, Wiebe E., Thomas P. Hughes, Trevor Pinch, and Deborah G. Douglas, eds. 2012. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Anniversary edition. Cambridge, Mass: The MIT Press.

Bond, Robert M., Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle, and James H. Fowler. 2012. "A 61-Million-Person Experiment in Social Influence and Political Mobilization." *Nature* 489 (7415): 295–98. doi:10.1038/nature11421.

Bonse, Eric. 2015. "Neue EU-Taskforce: Infokrieg Gegen Russenpropaganda." *Die*

Tageszeitung, sec. Europa. https://www.taz.de/Neue-EU-Taskforce/%215260851/.
Bossong, Raphael. 2008. “The Action Plan on Combating Terrorism: A Flawed Instrument of EU Security Governance.” *JCMS: Journal of Common Market Studies* 46 (1): 27–48. doi:10.1111/j.1468-5965.2007.00766.x.
Brey, Philip. 2005. “Artifacts as Social Agents.” In *Inside the Politics of Technology: Agency and Normativity in the Co-Production of Technology and Society*, edited by H Harbers, 61–84. Amsterdam University Press.
Brown, Ian, and Josh Cowls. 2015. “Check the Web -- ASSESSING THE ETHICS AND POLITICS OF POLICING THE INTERNET FOR EXTREMIST MATERIAL.” Oxford Internet Institute / VOX-Pol Network of Excellence. http://voxpol.eu/wp-content/uploads/2015/11/VOX-Pol_Ethics_Politics_PUBLISHED.pdf.
Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers.
C.A.S.E. Collective. 2006. “Critical Approaches to Security in Europe: A Networked Manifesto.” *Security Dialogue* 37 (4): 443–87. doi:10.1177/0967010606073085.
Cohen, Fred. 2002. “Terrorism and Cyberspace.” *Network Security* 2002 (5): 17–19. doi:10.1016/S1353-4858(02)05015-8.
Conway, Maura. 2006. “Terrorist ‘Use’ of the Internet and Fighting Back.” *Information and Security* 19: 34.
Coolsaet, Rik. 2011. “Epilogue: Terrorism and Radicalisation: What Do We Now Know?” In *Jihadi Terrorism and the Radicalisation Challenge: European and American Experiences*, edited by Rik Coolsaet, 259–68. Farnham: Ashgate Publishing, Ltd.
Council of the EU. 2002. *COUNCIL FRAMEWORK DECISION of 13 June 2002 on Combating Terrorism*. Vol. L 164/7. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33168.
———. 2008. *COUNCIL FRAMEWORK DECISION 2008/919/JHA of 28 November 2008 Amending Framework Decision 2002/475/JHA on Combating Terrorism*. Vol. L 330/21. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33168.
———. 2014. “Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism.” Strategy Paper 5643/5/14. Brussels: General Secretariat of the Council. http://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf.
———. 2015a. “Fight against Terrorism: Follow-up to the Council (Justice and Home Affairs) of 12-13 March 2015 - Implementation of Counter-Terrorism Measures.” Meeting Document 9418/15. Brussels: Presidency. http://www.statewatch.org/news/2015/jul/eu-cosi-ct-9418-15.pdf.
———. 2015b. “The Functioning of the Internet Referral Unit (EU IRU) on the Basis of the Future Europol Regulation.” Meeting Document DS 1497/15. Brussels: General Secretariat of the Council. https://netzpolitik.org//wp-upload/council1497-15.pdf.
Crenshaw, Martha. 1981. “The Causes of Terrorism.” *Comparative Politics* 13 (4): 379–99. doi:10.2307/421717.
Daase, Christopher. 2010. “Der Erweiterte Sicherheitsbegriff. Sicherheitskultur Im Wandel.” In *Workingpaper 1 2010*. Frankfurt am Main.
Dachwitz, Ingo. 2016. “Hatespeech-Verabredung Zwischen EU-Kommission Und Internetfirmen: NGOs Kritisieren Willkür.” *Netzpolitik.org*. June 1. https://netzpolitik.org/2016/hatespeech-verabredung-zwischen-eu-kommission-und-internetfirmen-ngos-kritisieren-willkuer/.
de Goede, Marieke. 2011. *European Security Culture: Preemption and Precaution in European Security*. Amsterdam University Press.
de Goede, Marieke, and Stephanie Simon. 2013. “Governing Future Radicals in Europe.” *Antipode* 45 (2): 315–35. doi:10.1111/j.1467-8330.2012.01039.x.

della Porta, Donatella. 1992. *Social Movements, Political Violence, and the State: A Comparative Analysis of Italy and Germany*. 1sted. Cambridge England; New York: Cambridge University Press.
Edkins, Jenny, and Véronique Pin-Fat. 2004. “Introduction: Life, Power, Resistance.” In *Sovereign Lives: Power in Global Politics*, edited by Jenny Edkins, Véronique Pin-Fat, and Michael J. Shapiro, 1–23. London: Routledge.
EDRi. 2012. “Clean IT – Leak Shows Plans for Large-Scale, Undemocratic Surveillance of All Communications.” *EDRi*. September 21. https://edri.org/cleanit/.
———. 2016. “EDRi and Access Now Withdraw from the EU Commission IT Forum Discussions.” *EDRi*. May 31. https://edri.org/edri-access-now-withdraw-eu-commission-forum-discussions/.
Elshimi, Mohammed. 2015. “De-Radicalisation Interventions as Technologies of the Self: A Foucauldian Analysis.” *Critical Studies on Terrorism* 8 (1): 110–29. doi:10.1080/17539153.2015.1005933.
ENER. 2008. “Radicalisation Processes Leading to Acts of Terrorism.” A concise Report prepared by the European Commission’s Expert Group on Violent Radicalisation. Brussels. http://www.rikcoolsaet.be/files/art_ip_wz/Expert%20Group%20Report%20Violent%20Radicalisation%20FINAL.pdf.
Ericson, Richard, and Aaron Doyle. 2004. “Catastrophe Risk, Insurance and Terrorism.” *Economy and Society* 33 (2): 135–73.
Eroukhmanoff, Clara. 2015. “The Remote Securitisation of Islam in the US Post-9/11: Euphemisation, Metaphors and the ‘logic of Expected Consequences’ in Counter-Radicalisation Discourse.” *Critical Studies on Terrorism* 8 (2): 246–65. doi:10.1080/17539153.2015.1053747.
———. 2016. “Counter-Radicalisation and Its Impact on Freedom of Expression.” In , 9. Cambridge. http://www.free-expression.group.cam.ac.uk/pdfs/workshop-paper-clara-eroukhmanoff-draft.pdf.
EU Counter-Terrorism Coordinator. 2015a. “EU CTC Input for the Preparation of the Informal Meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015.” DS 1035/15. Brussels: General Secretariat of the Council. http://www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf.
———. 2015b. “Follow-up to the Statement of the Members of the European Council of 12 February 2015 on Counter-Terrorism: State of Play on Implementation of Measures.” Note 12139/15. Brussels: General Secretariat of the Council. http://www.statewatch.org/news/2015/sep/eu-council-ct-implementation-plan-12139.-15.pdf.
EuroparlTV. 2016. *Panorama of the Combat against Terrorism*. http://europarltv.europa.eu/en/player.aspx?pid=3c4a0d5d-a3b2-4d85-9ac9-a62700f22bec.
European Commission. 2014a. “Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU’s Response.” Communication from the Commission COM(2013) 941 final. Brussels: European Commission. http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/crisis-and-terrorism/radicalisation/docs/communication_on_preventing_radicalisation_and_violence_promoting_extremism_201301_en.pdf.
———. 2014b. “On the Implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 Amending Framework Decision 2002/475/JHA on Combating Terrorism.” Communication from the Commission COM(2014) 554 final. Brussels: European Commission. http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/crisis-and-

terrorism/general/docs/report_on_the_implementation_of_cfd_2008-919-jha_and_cfd_2002-475-jha_on_combating_terrorism_en.pdf.
———. 2015. “European Agenda on Security - State of Play.” European Commission - Fact Sheet. Brussels: European Commission. http://europa.eu/rapid/press-release_MEMO-15-6115_de.htm.
———. 2016a. “Delivering on the European Agenda on Security to Fight against Terrorism and Pave the Way towards an Effective and Genuine Security Union.” Communication from the Commission COM(2016) 230 final. Brussels: European Commission. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents/docs/20160420/communication_eas_progress_since_april_2015_en.pdf.
———. 2016b. “European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech.” Press Release. Brussels: European Commission. http://europa.eu/rapid/press-release_IP-16-1937_en.htm.
European Council. 2015. “Special Meeting of the European Council - Statement.” European Council Statement EUCO 18 / 15. Brussels: General Secretariat of the Council. http://ec.europa.eu/dorie/fileDownload.do;jsessionid=jeSxzMm7FWkq2g1w8-L_fqIxkN-Be_A75tLbPuSPQK4RGL9GpSbJ!-2142749860?docId=2098892&cardId=2098891.
Europol. 2015a. “Terrorism Situation and Trend Report 2015.” Threat Assessment. TE-SAT. The Hague: European Police Office. https://www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015.
———. 2015b. “The Internet Organised Crime Threat Assessment 2015.” Threat Assessment. IOCTA. The Hague: Europol. https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.
———. 2015c. “Changes in Modus Operandi of Islamic State Terrorist Attacks.” Review. The Hague: European Police Office. https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks.
———. 2015d. “EU Internet Referral Unit at Europol - Concept Note.” The Hague: European Police Office. http://www.statewatch.org/news/2015/may/eu-council-internet-referral-unit-7266-15.pdf.
———. 2015e. “Europol’s Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda.” Press Release. The Hague: Europol. https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda.
———. 2015f. “Enhancing Counter Terrorism Capabilities at EU Level: European Counter Terrorism Centre (ECTC) at Europol and Counter Terrorism Related Information Sharing.” The Hague: European Police Office. http://www.statewatch.org/news/2015/nov/eu-council-europol-ECTC-14244-15.pdf.
———. 2015g. “Europol Strategy 2016-2020.” Strategy Paper 796794v19B. The Hague: European Police Office. https://www.europol.europa.eu/content/europol-strategy-2016-2020.
———. 2016a. “Europol’s European Counter Terrorism Centre Strengthens the EU’s Response to Terror.” Press Release. The Hague: Europol. https://www.europol.europa.eu/content/ectc.
———. 2016b. “Migrant Smuggling in the EU.” Europol Public Information. The Hague: Europol. https://www.europol.europa.eu/sites/default/files/publications/migrant_smuggling__e

uropol_report_2016.pdf.
———. 2016c. “Europol Joins UK Appeal to Report Extremist and Terrorist Material Online Using red ‘STOP’ button.” Press Release. The Hague: Europol. https://www.europol.europa.eu/newsletter/europol-joins-uk-appeal-report-extremist-and-terrorist-material-online-using-red-stop-but.
———. 2016d. “New Regulation Boosts the Roles of EDPS and Europol.” Press Release. The Hague: Europol. https://www.europol.europa.eu/newsletter/new-regulation-boosts-roles-edps-and-europol.
———. 2016e. “Enhancing Counter Terrorism Capabilities at EU Level: European Counter Terrorism Centre (ECTC) at Europol.” Note EDOC# 831655v2. The Hague: European Police Office.
———. 2016f. “European Parliament Adopts New Regulation for Europol.” Press Release. The Hague: Europol. https://www.europol.europa.eu/content/european-parliament-adopts-new-regulation-europol.
———. 2016g. “Europol and INTERPOL Issue Comprehensive Review of Migrant Smuggling Networks.” Press Release. The Hague: Europol. https://www.europol.europa.eu/content/europol-and-interpol-issue-comprehensive-review-migrant-smuggling-networks.
———. 2016h. “EU Internet Referral Unit – Year One Report Highlights.” The Hague: European Police Office. https://www.europol.europa.eu/content/eu-internet-referral-unit-year-one-report-highlights.
———. 2016i. “Europol’s Internet Referral Unit One Year On.” Press Release. The Hague: Europol. https://www.europol.europa.eu/newsletter/europol%E2%80%99s-internet-referral-unit-one-year.
———. 2016j. “No More Ransom: Law Enforcement and IT Security Companies Join Forces to Fight Ransomware.” Press Release. The Hague: Europol. https://www.europol.europa.eu/newsletter/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-fight-ransomware.
Gartenstein-Ross, Daveed, and Laura Grossman. 2009. *Homegrown Terrorists in the U.S. and U.K: An Empirical Study of the Radicalization Process*. Washington, D.C.: Center for Terrorism Research - Foundation for Defense of Democracies. http://www.defenddemocracy.org/content/uploads/documents/HomegrownTerrorists_USandUK.pdf.
Gill, Paul, and Emily Corner. 2015. “Lone-Actor Terrorist Use of the Internet and Behavioural Correlates.” In *Terrorism Online: Politics, Law and Technology*, edited by Lee Jarvis, Stuart MacDonald, and Thomas M. Chen. London: Routledge.
Gill, Paul, Emily Corner, Amy Thornton, and Maura Conway. 2015. “What Are the Roles of the Internet in Terrorism? Measuring Online Behaviours of Convicted UK Terrorists.” http://doras.dcu.ie/20897/.
Githens-Mazer, Jonathan. 2012. “The Rhetoric and Reality: Radicalization and Political Discourse.” *International Political Science Review / Revue Internationale de Science Politique* 33 (5): 556–67.
Githens-Mazer, Jonathan, and Robert Lambert. 2010. “Why Conventional Wisdom on Radicalization Fails: The Persistence of a Failed Discourse.” *International Affairs* 86 (4): 889–901. doi:10.1111/j.1468-2346.2010.00918.x.
Graham, Mark. 2012. “Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities?” SSRN Scholarly Paper ID 2166874. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=2166874.
Hagmann, Jonas, and Myriam Dunn Cavelty. 2012. “National Risk Registers: Security Scientism and the Propagation of Permanent Insecurity.” *Security Dialogue* 43 (1):

79–96. doi:10.1177/0967010611430436.
Hajer, Maarten. 2008. “Diskursanalyse in der Praxis: Koalitionen, Praktiken und Bedeutung.” In *Die Zukunft der Policy-Forschung*, edited by Frank Janning and Katrin Toens, 211–22. Wiesbaden: VS Verlag für Sozialwissenschaften. http://link.springer.com/10.1007/978-3-531-90774-1.
Hansen, Lene, and Helen Nissenbaum. 2009. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly* 53 (4): 1155–75.
Haverland, M., and D. Yanow. 2012. “A Hitchhiker’s Guide to the Public Administration Research Universe: Surviving Conversations on Methodologies and Methods.” *Public Administration Review* 72 (3): 401–408. doi:10.1111/j.1540-6210.2011.02524.x.
Hawkesworth, Mary. 2006. “Contending Conceptions of Science and Politics -- Methodology and the Constitution of the Political.” In *Interpretation and Method : Empirical Research Methods and the Interpretive Turn*, edited by Dvora Yanow and Peregrine Schwartz-Shea, 5–26. Armonk, NY: M.E. Sharpe.
Hayes, Ben, and Chris Jones. 2015. “Taking Stock -- The Evolution, Adoption, Implementation and Evaluation of EU Counter-Terrorism Policy.” In *The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism*, edited by Fiona De Londras and Josephine Doody, 13–39. Routledge Research in Terrorism and the Law. London [u.a.] Routledge 2015.
Heath-Kelly, Charlotte. 2013. “Counter-Terrorism and the Counterfactual: Producing the ‘Radicalisation’ Discourse and the UK PREVENT Strategy.” *British Journal of Politics & International Relations* 15 (3): 394–415. doi:10.1111/j.1467-856X.2011.00489.x.
Heath-Kelly, Charlotte, Christopher Baker-Beall, and Lee Jarvis. 2014. “Introduction.” In *Counter-Radicalisation: Critical Perspectives*, edited by Christopher Baker-Beall, Charlotte Heath-Kelly, and Lee Jarvis, 1sted., 1–13. New York: Routledge.
Howard, Philip. 2015. “The Myth of Violent Online Extremism.” *Yale Books Blog*. February 6. http://yalebooksblog.co.uk/2015/02/06/myth-violent-online-extremism/.
Hussain, Ghaffar, and Erin Marie Saltman. 2014. “Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter It.” London: Quilliam. https://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/jihad-trending-quilliam-report.pdf.
Huysmans, Jeff. 2014. *Security Unbound: Enacting Democratic Limits*. 1 edition. Critical Issues in Global Politics. London ; New York: Routledge.
Jones, Chris. 2016. “Policing the Internet: From Terrorism and Extremism to ‘content Used by Traffickers to Attract Migrants and Refugees.’” Brussels: Statewatch. http://www.statewatch.org/analyses/no-290-policing-internet.pdf.
Knoblauch, Hubert. 2005. *Wissenssoziologie*. Konstanz: UTB.
Kramer, Adam D. I., Jamie E. Guillory, and Jeffrey T. Hancock. 2014. “Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks.” *Proceedings of the National Academy of Sciences* 111 (24): 8788–90. doi:10.1073/pnas.1320040111.
Krasmann, Susanne. 2006. “Der Feind an Den Grenzen Des Rechtsstaats.” In *Foucault: Diskursanalyse Der Politik : Eine Einführung*, edited by Brigitte Kerchner and Silke Schneider, 233–50. Wiesbaden VS, Verl. für Sozialwiss. 2006.
Kuckartz, Udo. 2010. *Einführung in die computergestützte Analyse qualitativer Daten*. 3., Aktualisierte Aufl. Lehrbuch. Wiesbaden: VS, Verl. für Sozialwiss.
Kundnani, Arun. 2014. “Radicalisation - The Journey of a Concept.” In *Counter-Radicalisation: Critical Perspectives*, edited by Christopher Baker-Beall, Charlotte

Heath-Kelly, and Lee Jarvis, 1sted., 14–35. New York: Routledge.
la Rue, Frank. 2011. “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.” A /HRC/17/27. United Nations Human Rights Council. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf .
Latour, Bruno. 2005. *Von der “Realpolitik” zur “Dingpolitik” oder Wie man Dinge öffentlich macht*. Berlin: Merve.
Martin-Mazé, Médéric, and J. Peter Burgess. 2015. “The Societal Impact of European Counter-Terrorism.” In *The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism*, edited by Fiona De Londras and Josephine Doody, 93–113. Routledge Research in Terrorism and the Law. London [u.a.] Routledge 2015.
Monroy, Matthias. 2015. “„Anti-Terror-Zentrum“: Europols Neuen Kompetenzen Fehlt Bislang Die Rechtliche Grundlage.” *Netzpolitik.org*. November 25. https://netzpolitik.org/2015/anti-terror-zentrum-europols-neuen-kompetenzen-fehlt-bislang-die-rechtliche-grundlage/.
———. 2016. “„Terroristisches Material“ Im Internet: Noch Mehr Löschanträge von Europol Erfolgreich.” *Netzpolitik.org*. May 23. https://netzpolitik.org/2016/terroristisches-material-im-internet-noch-mehr-loeschantraege-von-europol-erfolgreich/.
Münch, Sybille. 2016. *Interpretative Policy-Analyse*. Wiesbaden: Springer Fachmedien Wiesbaden. http://link.springer.com/10.1007/978-3-658-03757-4.
Nakashima, Ellen. 2016. “Obama’s Top National Security Officials to Meet with Silicon Valley CEOs.” *The Washington Post*, January 7. https://www.washingtonpost.com/world/national-security/obamas-top-national-security-officials-to-meet-with-silicon-valley-ceos/2016/01/07/178d95ca-b586-11e5-a842-0feb51d1d124_story.html.
Nasser-Eddine, Minerva, Bridget Garnham, Katerina Agostino, and Gilbert Caluya. 2011. “Countering Violent Extremism (CVE) Literature Review.” DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA543686.
Neumann, Peter. 2008. “Perspectives on Radicalisation and Political Violence: Papers from the First International Conference on Radicalisation and Political Violence.” Conference Paper. London: The International Centre for the Study of Radicalisation and Political Violence. http://icsr.info/wp-content/uploads/2012/10/1234516938ICSRPerspectivesonRadicalisation.pdf.
———. 2013. “The Trouble with Radicalization.” *International Affairs* 89 (4): 873–93. doi:10.1111/1468-2346.12049.
Neumann, Peter, and Scott Kleinmann. 2013. “How Rigorous Is Radicalization Research?” *Democracy and Security* 9 (4): 360–82. doi:10.1080/17419166.2013.802984.
Nouri, Lella, and Andrew Whiting. 2014. “Prevent and the Internet.” In *Counter-Radicalisation: Critical Perspectives*, edited by Christopher Baker-Beall, Charlotte Heath-Kelly, and Lee Jarvis, 1sted., 175–89. New York: Routledge.
Packer, George. 2013. “Change the World.” *The New Yorker*, May 27. http://www.newyorker.com/magazine/2013/05/27/change-the-world.
Paravicini, Giulia. 2016. “Paris Attacks Prompt EU to Share Secrets.” *POLITICO*. January 20. http://www.politico.eu/article/paris-attacks-prompt-share-secrets-eu-security-forces-eurodac-schengen-information-system-terrorism-isis-isil-islamic-state-bataclan/.
Pizzi, Michael. 2014. “The Syrian Opposition Is Disappearing From Facebook.” *The Atlantic*, February 4. http://www.theatlantic.com/international/archive/2014/02/the-syrian-

opposition-is-disappearing-from-facebook/283562/.
Pouliot, Vincent. 2008. “The Logic of Practicality: A Theory of Practice of Security Communities.” *International Organization* 62 (2): 257–288.
Ragin, Charles C. 1992. “Casing and the Process of Social Inquiry.” In *What Is a Case?: Exploring the Foundations of Social Inquiry*, edited by Charles C. Ragin and Howard Saul Becker, 217–26. Cambridge University Press.
Richards, Anthony. 2011. “The Problem with ‘radicalization’: The Remit of ‘Prevent’ and the Need to Refocus on Terrorism in the UK.” *International Affairs* 87 (1): 143–52. doi:10.1111/j.1468-2346.2011.00964.x.
Roy, Olivier. 2016. “France’s Oedipal Islamist Complex.” *Foreign Policy*. January 7. https://foreignpolicy.com/2016/01/07/frances-oedipal-islamist-complex-charlie-hebdo-islamic-state-isis/.
Rudl, Thomas. 2016. “EU-Parlament Beschließt Erweiterte Europol-Befugnisse Und Meldestelle Für Internetinhalte.” *Netzpolitik.org*. May 12. https://netzpolitik.org/2016/eu-parlament-beschliesst-erweiterte-europol-befugnisse-und-meldestelle-fuer-internetinhalte/.
Sageman, Marc. 2008. *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: Univ of Pennsylvania Pr.
Said, Edward W. 2012. *Orientalism: Western Conceptions of the Orient*. Auflage: 25th Anniversary Ed with 1995 Afterword Ed. London: Penguin Classics.
Saltman, Erin Marie, and Jonathan Russell. 2014. “The Role of Prevent in Countering Online Extremism.” White Paper. London: Quilliam. https://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/white-paper-the-role-of-prevent-in-countering-online-extremism.pdf.
Schröder, Ursula C. 2013. *The Organization of European Security Governance: Internal and External Security in Transition*. Routledge.
Schwartz-Shea, P., and D. Yanow. 2012. *Interpretive Research Design. Concepts and Processes*. New York: Routledge. http://library.wur.nl/WebQuery/wurpubs/421002.
Sedgwick, Mark. 2010. “The Concept of Radicalization as a Source of Confusion.” *Terrorism and Political Violence* 22 (4): 479–94.
Seemann, Michael. 2014. *Das neue Spiel: Strategien für die Welt nach dem digitalen Kontrollverlust*. 1 edition. iRights Media.
Shepherd, Laura J., ed. 2013. *Critical Approaches to Security: An Introduction to Theories and Methods*. London ; New York: Routledge.
Soss, Joe. 2006. “Talking Our Way to Meaningful Explanations - A Practice-Centered View of Interviewing for Interpretive Research.” In *Interpretation and Method : Empirical Research Mmethods and the Interpretive Turn*, edited by Dvora Yanow and Peregrine Schwartz-Shea, 127–49. Armonk, NY: M.E. Sharpe.
Stehr, Nico. 2001. *The Fragility of Modern Societies: Knowledge and Risk in the Information Age*. SAGE.
Tsoukala, Anastassia. 2008. “Boundary-Creating Processes and the Social Construction of Threat.” *Alternatives: Global, Local, Political* 33 (2): 137–52.
van Hulst, Merlijn, and Dvora Yanow. 2016. “From Policy ‘Frames’ to ‘Framing’ Theorizing a More Dynamic, Political Approach.” *The American Review of Public Administration* 46 (1): 92–112.
Verloo, Mieke, and Emanuela Lombardo. 2007. “Contested Gender Equality and Policy Variety in Europe: Introducing a Critical Frame Analysis Approach.” In *Multiple Meanings of Gender Equality : A Critical Frame Analysis of Gender Policies in Europe*, edited by Mieke Verloo, 21–49. Budapest ua: Central European UnivPress.
Verloo, Mieke, and Maro Pantelidou Maloutas. 2005. “Editorial: Differences in the Framing

of Gender Inequality as a Policy Problem across Europe." *The Greek Review of Social Research* 117 (B): 3–10.
von Behr, Ines, Anaïs Reding, Charlie Edwards, and Luke Gribbon. 2013. "Radicalisation in the Digital Era - The Use of the Internet in 15 Cases of Terrorism and Extremism." Brussels: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf.
Wagner, Ben. 2013. "Governing Internet Expression: How Public and Private Regulation Shape Expression Governance." *Journal of Information Technology & Politics* 10 (4): 389–403. doi:10.1080/19331681.2013.799051.
Wainwright, Rob. 2016. "Europe's Top Cop Warns More Attempted Attacks 'Almost Certain.'" *Time*, May 16. http://time.com/4336919/europol-terrorist-paris-brussels-rob-wainwright/.
Weimann, Gabriel. 2004. *Www.terror.net: How Modern Terrorism Uses the Internet*. United States Institute for Peace USIP.
Wiktorowicz, Quintan. 2005. *Radical Islam Rising: Muslim Extremism in the West*. Oxford: Rowman & Littlefield Publishers, Inc.
Yanow, Dvora. 2006. "Thinking Interpretively: Philosophical Presuppositions and the Human Sciences." In *Interpretation and Method : Empirical Research Methods and the Interpretive Turn*, edited by Dvora Yanow and Peregrine Schwartz-Shea, 5–26. Armonk, NY: M.E. Sharpe.
Yanow, Dvora, and Peregrine Schwartz-Shea, eds. 2006. *Interpretation and Method : Empirical Research Methods and the Interpretive Turn*. Armonk, NY: M.E. Sharpe.
York, Jillian. 2016. "European Commission's Hate Speech Deal With Companies Will Chill Speech." *Electronic Frontier Foundation*. June 3. https://www.eff.org/deeplinks/2016/06/european-commissions-hate-speech-deal-companies-will-chill-speech.