Securing Judgement
Rethinking Security and Online Information Threats

Hedvig Ördén
Securing Judgement
Rethinking Security and Online Information Threats

Hedvig Ördén

Academic dissertation for the Degree of Doctor of Philosophy in Political Science at Stockholm University to be publicly defended on Friday 13 March 2020 at 13.00 in hörsal 11, hus F, Universitetsvägen 10 D.

Abstract
The contemporary debate in democracies routinely describes online information threats such as misinformation, disinformation and deception as security-issues in need of urgent attention. Despite this pervasive discourse, policymakers often appear incapable of articulating what security means in this context. Turning to EU policy and previous research on cybersecurity, this dissertation empirically unpacks, critically interrogates and theoretically rethinks the meaning of security in relation to online information threats. In so doing, the articles elucidate a new ‘referent object’ implicitly guiding securitization. Contemporary interventions can be seen as grounded in assumptions about the protection of human judgement. Using Hannah Arendt’s writings on ‘political judgement’ as a point of reference for critically evaluating contemporary policy, the dissertation points to several problems with existing approaches to security in a democratic context where free debate constitutes a legitimizing element of political authority. The rethinking of security departs from this problematic and shows that treating human judgement as a ‘referent object’ – if firmly grounded in the interplay between independent human communicating subjects – can better address some problematic questions about legitimate authority and political community currently haunting security interventions in cyberspace.

Keywords: security studies, critical security studies, cyber security, disinformation, Arendt, post-foundationalism, political theory, EU security policy.

Stockholm 2020
http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-178239

ISBN 978-91-7797-937-1
ISBN 978-91-7797-938-8
ISSN 0346-6620

Department of Political Science
Stockholm University, 106 91 Stockholm
SECURING JUDGEMENT
Hedvig Ördén
Securing Judgement
Rethinking Security and Online Information Threats

Hedvig Ördén
'Imagination abandoned by reason produces impossible monsters; united with her, she is the mother of the arts and source of their wonders.'

Francisco Goya
Publications included in the PhD thesis

This PhD thesis consists of three articles preceded by an introductory chapter which describes the wider contribution of the thesis and how the articles relate to each other. Two of the articles have been published in peer-reviewed journals, and one is in submission.

Article 1

Article 2
Ördén, H. ‘Securitizing cyberspace: protecting political judgement’.

Article 3
ABSTRACT

The contemporary debate in democracies routinely describes online information threats such as misinformation, disinformation and deception as security-issues in need of urgent attention. Despite this pervasive discourse, policymakers often appear incapable of articulating what security means in this context. Turning to EU policy and previous research on cybersecurity, this dissertation empirically unpacks, critically interrogates, and theoretically rethinks the meaning of security in relation to online information threats. In so doing, the articles elucidate a new ‘referent object’ implicitly guiding securitization. Contemporary interventions can be seen as grounded in assumptions about the protection of human judgement. Using Hannah Arendt’s writings on ‘political judgement’ as a point of reference for critically evaluating contemporary policy, the dissertation points to several problems with existing approaches to security in a democratic context where free debate constitutes a legitimizing element of political authority. The rethinking of security departs from this problematic and shows that treating human judgement as a ‘referent object’ – if firmly grounded in the interplay between independent human communicating subjects – can better address some problematic questions about legitimate authority and political community currently haunting security interventions in cyberspace.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgements</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>- The Online Information Threat in a Democratic Context</td>
<td>5</td>
</tr>
<tr>
<td>- The Problem of Security</td>
<td>8</td>
</tr>
<tr>
<td>- Research Question and Arguments</td>
<td>11</td>
</tr>
<tr>
<td>Security and the Online Information Threat: The State of the Art</td>
<td>13</td>
</tr>
<tr>
<td>Conceptualizing Security</td>
<td>17</td>
</tr>
<tr>
<td>Methods and Material</td>
<td>22</td>
</tr>
<tr>
<td>- The Case of the European Union</td>
<td>24</td>
</tr>
<tr>
<td>- Unpacking Security through the Online Information Threat</td>
<td>26</td>
</tr>
<tr>
<td>- Critiquing Security and the Online Information Threat</td>
<td>29</td>
</tr>
<tr>
<td>- Rethinking Security through the Online Information Threat</td>
<td>31</td>
</tr>
<tr>
<td>Summary of the Articles</td>
<td>32</td>
</tr>
<tr>
<td>- Article 1. Deferring Substance: EU Policy and the Information Threat</td>
<td>32</td>
</tr>
<tr>
<td>- Article 2. Securitizing Cyberspace: Protecting Political Judgement</td>
<td>34</td>
</tr>
<tr>
<td>Conclusions</td>
<td>36</td>
</tr>
<tr>
<td>Contributions</td>
<td>39</td>
</tr>
<tr>
<td>Limitations and Future Research</td>
<td>41</td>
</tr>
<tr>
<td>References</td>
<td>42</td>
</tr>
</tbody>
</table>

Article I: Deferring Substance: EU Policy and the Information threat

Article II: Securitizing Cyberspace: Protecting Political Judgement

Article III: Instilling Judgement: Counter-narratives of Humour, Fact and Logic

Sammanfattning
Acknowledgements

When I presented the first fledgling draft of this dissertation, I was full of criticism for certain absurd policies on online information threats. Early policy proposals list humour as a key strategy for online counter-radicalization. Why, I queried, would humour be used to counter Islamist propaganda or right-wing extremism spread online? Do we expect the reader to laugh himself to death, like in the famous Monty Python episode about the funniest joke in the world? What were they trying to protect through the dissemination of such hilarities? In a particularly scathing passage, I remember questioning the idea of countering online Islamist propaganda by pointing to the lack of Nutella in IS territory. I rhetorically asked: do policymakers really believe we can change people’s minds by informing them about the shortage of chocolate spread?

The discussant of my paper turned out to be the very man who drafted the policy. It was an embarrassing moment for both of us. For my part, however, it was also a moment of insight. The man exclaimed: ‘What should we do then? At least we should tell the kids that there is no Nutella in Syria!’ At that point I realized some crucial things about critical research. I had confused the pursuit of critique with simple criticism. But as I learned, any serious form of critical reading must begin by trying to understand how even the most absurd suggestions can make sense. For that, we need to suspend criticism – at least momentarily.

Writing a thesis is a long and arduous process. You need a space to work, help, inspiration, encouragement, sincere feedback, linguistic input, comradeship, and (yes) laughter along the way. Probably in equal doses. There are many I would like to thank for giving me all this, and much more.

As Virginia Woolf underlined, there are essential physical aspects to the writing process – so I will begin here. A big thank you to the Political Science Department at Lund University and Björn Badersten who offered me a workspace so close to home. It has been invaluable for me. I am also grateful to Amir Parhamifar who always was there to offer me a hand with any practicalities (I will never forget that time when you, in a wizard-like fashion, produced a laptop for me when mine broke down just in time for the holidays). I would also like to thank the research group on Intelligence Analysis, for offering me interesting seminars to teach, and Jens Bartelson for giving insightful comments and encouragement when I was struggling with my introduction.

For giving me the fantastic opportunity (sometimes curse) to write this dissertation, I owe a great debt to the department of Political Science at Stockholm University. A special thanks to Anneli Lindén – without you I would never have found my way out of the administrative maze! Also thank you to all the people involved in my three seminars, giving me important, useful, and productive feedback: Elín Hafsteinsdóttir and Simon Birnbaum; Karim Zakhour and Kjell Engelbrekt; Ulrika Mörth, Jouni Reinikainen and Niklas Bremberg.

For help, inspiration, encouragement and sincere discussions, I would like to thank my supervisors. I am most grateful to Maria Wendt for her unwavering support in the fragile fledgling stages of this project, but also for her guidance as I began supervising undergraduate students. I could not have found a better cicerone in the teaching profession! I would also like to thank Hans Agné for earnest feedback, support and great optimism. You were always on hand for answering any questions – central or trivial – and giving perceptive comments and holistic feedback on my work. For great inspiration, encouragement and brilliant feedback, thank you Sharon Rider. You were always thinking with me, but never shared my occasional desire to take a shortcut. Also,
without the enthusiasm and the new ideas you brought to the project it might never have left the ground. Finally, some people tend to arrive at just the right moment. For joining me in the last difficult phase when a million parts are to be tied up into a whole, I would like to thank Stefan Borg. Your careful readings, meticulous comments, deep knowledge in the field, and your keen encouragement made the whole difference to my project. In relation to all my supervisors, and our numerous sessions, I can honestly say that there was never a dull moment over the years.

For patiently assisting me in expressing my thoughts in writing, and for a thousand other matters besides, I am most grateful to Rob Farren. Your dedicated copy editing and proofreading put an end to all the superfluous adjectives and commas invading my drafts. I am so sorry about the so-called ‘dangling participles’ putting years on you. Thank you also Colm Farren for proofreading the last article included in this dissertation, making the text flow in an eloquent way, and Carin Ördén for the careful reading of my Swedish abstract.

For comradeship, emotional support and laughter, thank you all colleagues on floor five in Stockholm and all those sharing my workspace in Lund over the years. Thank you Tua Sandman for walking beside me over the years, for our ever-ongoing conversations and many pints. You were always there for me. Thank you Markus Furendal for being a great friend and the best co-worker I have ever had during our time in Doktorandrådet. Thank you Karim Zakhour, Ragnhild Nilsson, Tarek Oraby and Magnus Christiansson for making the first difficult year into a time of friendship, thank you Karin Sundström for always knowing the answer to my confused questions about institutional policy, and Tyra Hertz, Helena Hede Skagerlind, Eleonora Stolt, Jasmina Nedevska, Karin Gavelin and Faradj Koliev for fun lunchtime breaks. Thank you Karin Harborg and Hampus Nilsson for putting up with me in a tiny space, and for never failing to underline the humorous absurdities of everyday life. Thank you Niklas Altermark and Linda Nyberg for listening to my worries and providing encouragement. Thank you Johanna von Bahr for all the enthusiastic discussions over coffee and helpful tips at the end of this journey and Fredrika Larsson, for all those words of encouragement. Thank you Sofia Helander for witty conversations and escapist dreams about a life with chickens. A very special thank you also to Elín Hafsteinsdóttir for being my mentor when I most needed it.

For moral support and hours of childminding, I want to thank my family: my parents and their spouses, my sister and grandmother.

Last but not least, thank you Nimo for being an ardent defender of life outside of the academy, always producing convincing arguments in favour of visits to the swimming pool, movie nights, raspberry pie, Saturday sweets and no homework. Your small but powerful force helped me to forget about work and remember about fun.
Introduction

In recent years, cyberspace has increasingly come to be seen as a potentially destabilizing element of political life. The online information threat – false, misplaced or distorted information shared online – is said to skew political discussions, encourage vulnerable individuals to join cause with terrorist or extremist groups, and even affect election results. A Chatham House report describes a situation where democracies are ‘being “out-communicated” – not only by our enemies but by a wide range of alternative voices and perspectives that are sometimes hostile, sometimes indifferent’ (Turnbull 2011, vii). These aspects make online information-sharing a central contemporary security issue, but also an intractable problem for democracies grounded in principles of freedom of expression, public debate and transparency of information. But what happens to security, what does security become, when online information is construed as a threat?

The Online Information Threat in a Democratic Context

For a long time it was taken for granted that cyberspace and the communicative possibilities it offers extend the individual freedom of citizens and enhance democratic life. Popular uprisings against authoritarian regimes, which spread and were amplified through social media – in particular during the 2011 Arab Spring – worked to confirm this view among politicians in democratic regimes. Preserving the openness of the online sphere even formed a central part of democratic foreign policy (Kiggins 2015, 102), particularly in the US. Driven by a belief in the inherent democratizing power of online communication, the George W. Bush and Obama administrations spent ‘millions of dollars’ on providing ‘technological assistance to anti-censorship activists’ (Schneier and Farrell 2018, 12) in the belief that cyberspace was a tool for democratization in an age of globalization.

It is only quite recently that online information has come to be seen instead as a threat to democracies. The 2013 World Economic Forum ‘Global Risk Report’ is one of the first accounts portraying online communication as a widespread problem. Describing ‘digital wildfires’ as a ‘global risk,’ the organization highlights potential issues emerging from a horizontal sphere of communication connecting ‘many
to many’, rather than the traditional ‘one to many’ (Howell 2013, 23). Pointing to the speed of online communication, the report argues that, whether ‘intentionally or unintentionally misleading or provocative,’ the ‘rapid viral spread of information’ can have serious societal consequences – particularly in situations of ‘high tension’ (Howell 2014, 23-25). The problem of cyberspace as a communication channel connecting ‘many to many’ became acute with the rise of the Islamic State (IS) in Syria. As of 2013, European democracies have seen a growing rate of citizens travelling to join the cause (Bakker and Singleton 2016, 13) – a development that has been partly explained with reference to online ‘radicalization’ and widespread ‘extremist propaganda’ on social media (RAN 2012, 2). Yet, while online radicalization gave rise to intense political debate and calls for countermeasures, the perceived danger was largely specific to violent extremism and did not yet extend to cyberspace in general.

The final turning point in the perception of cyberspace as an inherently democratizing force came with the Russian annexation of Crimea in 2014. Russia’s strategy in Ukraine, which included an informational dimension in social media targeting European democracies, was a wake-up call for politicians and policymakers, particularly within the European Union (EU) (Hedling 2018, 158). In the years that followed the initial events in Ukraine, democratic states saw explicit attempts to influence democratic processes through intentional disinformation, which led to a surge in discussions about the online information threat. With the 2016 US election came the now well-established term ‘fake news’ (Silverman 2016), reflecting what has been described as an ‘epistemic crisis’ of democracies (Benkler et al. 2018, 20). Media firm Cambridge Analytica’s harvesting of millions of Facebook profiles for personal data to be used in targeted ads (Cadwalladr and Graham-Harrison 2018) highlighted the troubling pivotal position of social media companies in democratic discussion. Once a weapon for democratization, online information was now revealed as a threat to democracy, with the potential to undermine our ‘collective capacity to tell truth from falsehood and reason from its absence’ (Benkler et al. 2018, 4).

To better understand in what ways online information is a threat to democracy, we need to consider the centrality of information-sharing and citizens’ communication in the context of democracy. As Robert Dahl puts it, a fundamental ideal in any democratic system is the pursuit of the ‘common good’ (Dahl 1989, 307). Yet, most of the time, this common good is not a substantive goal, but consists rather of a set of ‘practices, arrangements, institutions, and processes’ that promote the well-
being of ourselves and others (Dahl 1989, 307). An essential feature of such processes is that ‘each citizen ought to have adequate and equal opportunities for discovering and validating [...] the choice on the matter to be decided that would best serve the citizen’s interests.’ (Dahl 1989, 307. Orig. italics.) This, in turn, implies individual autonomy, equal opportunity for expressing preferences, and open access to information that is of importance for decision-making (Dahl 1989, 111-112). For some, these elements are specifically connected with liberal democracies, but Dahl argues that they are key for any democratic regime.\(^1\) In short, transparency of information, as well as free debate, are fundamental preconditions for democratic decision-making. As Dieter Grimm suggests, we might go so far as to say that there can be ‘no democracy without public discourse and no public discourse without freedom of speech, freedom of the media, and freedom of information’ (Grimm 2009, 11). If we take this to be a minimal requirement for any democratic system, we can see how the online information threat turns this backbone of democracy into its core vulnerability.

Although the research is only in its infancy, several studies articulate the specific problems posed by the online information threat in a democratic context. Asking in what way online information presents a threat, Bruce Schneier and Henry Farrell conceptualize democracy as a particular form of ‘decentralized’ information system (Schneier and Farrell 2018, 3). In contrast to autocracies, which require common knowledge about ‘who is in charge’, democracies ‘draw upon the disagreements within their population to solve problems’ and fundamental contestation about ‘who the rulers should be’ (Schneier and Farrell 2018, 8). Nevertheless, despite the decentralized nature of the democratic system, democracies are still dependent on a shared understanding about the rules of the game. While any democracy will be comprised of a ‘wide variety of collective actors,’ it will be essentially organized around ‘common political knowledge’ or a set of ‘consensus beliefs’ (Schneier and Farrell 2018, 2. Orig. italics.). These beliefs, in turn, work to hold democratic systems together. In short, common political knowledge allows citizens to agree on what they disagree about. Regarded in this way, online information threats can be seen as inserting fundamental disagreements about the minimal feature holding democracy together – common political knowledge.

\(^1\)In this way, Dahl divides up the ‘universe of possibilities into democracy and nondemocracy’ (Dahl 1989, 316).
What is more, without this shared understanding of the rules of the game, collective democratic decision-making itself is under threat.

The Problem of Security

The meaning of security is inherently linked to the nature of an envisaged threat. For much of the history of Security Studies, security has been synonymous with national security. The most notable wars in the first half of the 20th Century were inter-state wars, and the protection of sovereign territory became a natural focal point. With the breakdown of the bipolar world order after the Cold War, and an increase in intrastate conflicts (Holsti 1996, Kaldor 1999), the state-centric approach to security was called into question. Criticising the empirical ‘unhelpfulness’ of state-centrism in a world of domestic conflicts, scholars turned to ‘human security’ (Peoples and Vaughan-Williams 2010, 154). A similar change of perspective can be seen in the contemporary focus on transnational risks, moving the discussion to ‘civil security’ (Bossong and Hegeman 2015). Given this intricate relationship between threat and security, how can we understand security in relation to the online information threat purportedly emerging in democracies today? A turn to contemporary policy provides no clear answer. On the contrary, proposed countermeasures are highly diverse, including the introduction of special ‘cyber commands’ and the production of positive ‘counter-narratives’ (Missiroli et al. 2016), enhanced ‘critical thinking’ skills (Nordbruch 2016), encouraging ‘mindfulness’ (Ivan 2019), governmental screening of content (Pherson and Mort Ranta 2019, 9) and even the construction of an ‘alternative internet’ (Pherson and Mort Ranta 2019, 9).

Taking democracy as a scope condition, this dissertation explores how we can conceptualize security in relation to the online information threat. In seeking to make sense of policy initiatives and how the threat is understood, it confronts the following set of conceptual, methodological and theoretical problems.

First, given that security is understood in relation to the nature of the perceived threat, a key question for this dissertation is not ‘what is the threat?’, but how is the purported threat perceived? In existing research, the purposeful dissemination of problematic information by certain actors is commonly described in terms of ‘information warfare’, ‘hybrid warfare’, or ‘information operations’ (Omand 2018,
Yet, such concepts spring out of research assuming a state-centric approach, often conducted in the fields of Defence, Intelligence, and Strategic Studies. While this dissertation in no way denies that such threats exist, these concepts fail to capture the multifaceted and sometimes unintentional threat commonly evoked by contemporary politicians and policymakers today. An illustrative example is found in a report by Elżbieta Fotyga for the EU Parliament Committee on Foreign Affairs that characterizes the threat as a conglomerate of ‘disinformation, misinformation, and deception’ spread through ‘new technologies’ (Fotyga 2016). More recent discussions add to this mix a concern for ‘fake news’ (Silverman 2016). In a report published by Facebook focusing on ‘civic discourse,’ for example the term ‘information operations’ comes to denote the spread of ‘false news’ and ‘disinformation’ disseminated online (Weedon et al. 2017, 4). A minimal criterion guiding the political discussion seems to be that the information in question is dangerous, and that it is spread through new technologies. To allow for a more comprehensive approach that captures the wider contemporary policy discussion of the threat in democracies, this dissertation introduces the term ‘online information threats’ to denote all forms of information or communication spread online considered dangerous by political actors, policymakers and policy intellectuals, and in need of active intervention. While familiar concepts such as ‘information warfare’ appear in some parts of the dissertation, they form objects of investigation rather than points of departure.

Second, how can we explore security? In Security Studies, but also in ordinary language, the meaning of security is linked to something that should be protected. In the parlance of Critical Security Studies, this is called a ‘referent object’ (Buzan et al. 1998, 36). Asking questions about security thus implies that we already possess an answer to the question of what to protect. Constructivist scholars have widened the scope of possible objects by pointing to the constructed nature of the threat and introducing concepts such as ‘securitization’ (Buzan et al. 1998, 25). Such approaches still assume the existence of an explicit referent object employed by securitizing actors mobilizing the threat discourse. In this logic, security can only appear as result of a speech act, a claim that something is under threat. In the case of the online information threat, however, this something, in itself, is what constitutes the object of investigation. Exploring security in relation to the online information threat therefore requires a different understanding of the referent object. To deliver this, the
dissertation conceptualizes the referent object as a *preconception about of protection that grounds and guides proposed interventions*. In the context of empirical investigations, this can be translated into the question: ‘Security of what?’ The meaning of security is thus unearthed by elucidating the assumptions about protection underpinning the reports, threat descriptions, technologies and policies produced in relation to the online information threat. In contrast to the bulk of research in Critical Security Studies, the focus is not on processes or practices of securitization (Waever 1995, 53), or on how securitization is achieved in relation to particular audiences (Côté 2016), but rather on what we assume to be protected through proposed interventions. In other words, the referent object, as understood here, can be seen as a first step in the process of securitization.

Third, what constitutes a satisfactory or desirable referent object? The elucidation of preconceptions guiding policy interventions serves both a critical and theoretical purpose in this dissertation. Like other work in Critical Security Studies, the articles strive to highlight the political dimension of security and bring the political ‘back in’ (Edkins 1999). Departing from a core insight in post-foundational political theory – that security cannot be considered *apart* from questions of political life (Walker 1990) – the readings draw attention to the relationship between political authority and political community in claims about security. In a democratic context, the online information threat constitutes a particularly intricate case. As Rob Walker notes, state sovereignty was long a successful referent object because it superficially reconciles an ‘apparent contradiction’ in claims about state autonomy, legitimate authority and political community by reference to territorial boundaries (Walker 1990, 10). Or, as Matt Whitt puts it, by ‘transferring the composition of the sovereign’s collective subject onto what appears as the pre-political givenness or facticity of territory, the territorial ideal of modern sovereignty presents the people as *given* by social *facts*, rather than *constituted* through political *acts*’ (Whitt 2010, 201). Yet, security in relation to the online information threat demands that political authority be exercised in a space currently lacking territorial boundaries. This poses distinct problems for frameworks of national security. Furthermore, in a democratic context, political authority implies authorization by ‘the people,’ while political community involves an acknowledgement of independent communicating human subjects.

Critiquing security, the dissertation scrutinizes the demands and conditions connected to each proposed referent object in the light of these overarching problems. Specific
attention is paid to two objects of protection: the cybersovereign state and human judgement. Taking as its starting point problems that have been identified in critical readings, the dissertation then proceeds to rethink the referent object by considering the meaning of democratic legitimacy in the light of these changed circumstances. In so doing, the articles provide useful guidelines for policymakers currently grappling with the online information threat.

Research Question and Arguments

This dissertation investigates the problem of security in relation to the online information threat in three separate articles, using three different kinds of material. The first article explores EU policy on the online information threat empirically; the second engages with previous research on cybersecurity and influential policy in order to rethink security; and the third critically analyses EU policy on online counter-radicalization strategies.

While diverse with regard to the materials analysed, the articles are all guided by the following overarching research question:

- What does security mean in relation to information threats online?

In answering this question, the articles empirically unpack, critically interrogate, and theoretically rethink the meaning of security in relation to online information threats. Elucidating a new ‘referent object’ implicitly guiding securitization, and drawing on EU policy and previous research in cybersecurity, the articles argue that many contemporary interventions can be seen as grounded in assumptions about the protection of human judgement. Using Hannah Arendt’s writings on ‘political judgement’ as a point of reference for critically evaluating contemporary policy, the dissertation points to several problems with existing approaches to security in a democratic context where free and inclusive debate constitutes a legitimizing element of political authority. Against the backdrop of this problematic when rethinking security, the articles show how treating human judgement as a ‘referent object’ – if it
is grounded in the interplay between independent human communicating subjects – can better address some problematic questions about legitimate authority and political community currently haunting security interventions in cyberspace. By understanding judgement in relation to the intersubjective dimension of human communication, policymakers can distinguish between desirable and less desirable approaches to security-making in relation to the online information threat in a democratic context.

The key contribution of the dissertation, with implications for and beyond Security Studies, is the introduction of human judgement as a referent object of security. Explicating human judgement as a referent object, and specifying the conditions for instilling the particular form of political judgement appropriate to a democratic context, the articles offer a new conceptualization of security in relation to the online information threat, as well as guidelines for policymaking. The theoretical analyses shed light on the difficulties inherent in pursuing security in a democratic cyberspace in relation to threats spread through human communication. This discussion provides crucial arguments against existing proposals for applying a national security framework to contemporary online information threats, which is a remedy suggested in contemporary policymaking and research within Defence Studies. The critique also speaks against the individualistic approaches to judgement pursued within the fields of Defence, Intelligence, and Strategic Studies, which draw heavily on ‘mind sciences’ such as cognitive psychology and behavioural studies.

In addition, the dissertation makes methodological and conceptual contributions to Critical Security Studies, as well as empirical and theoretical contributions to the growing body of literature on security and online information threats within Strategic Studies. By conceptualizing the referent object as a preconception that guides proposed interventions, the articles present a new approach to investigating objects of protection in the absence of explicit speech acts. This perspective is useful for critical security scholars interested in exploring the starting points of securitization in policy material. Finally, the dissertation offers an empirical illustration of the multifaceted nature of security-making in relation to the threat. By investigating cross-sectoral policy produced and funded by the European Union, the empirical studies illuminate a number of crucial differences in how the contemporary online information threat is perceived within different policy communities. Describing how these differences in perceptions may contribute to contradictory approaches to security, the analysis brings to light the
potential pitfalls of the comprehensive approach to ‘hybrid’ threats commonly suggested by Strategic scholars.

The rest of this introduction proceeds in the following way. First, I provide an overview of contemporary scholarly work on the online information threat. Second, I outline the conceptualization of security employed throughout this dissertation. Third, I describe why EU policy and policy work are used to explore the question of security and the online information threat and introduce the different methods and materials used for unpacking, critiquing and rethinking security. Third, I briefly summarize the three articles and discuss the dissertation’s broader contributions to Security Studies in general and to Critical Security Studies in particular, as well as the implications of the findings presented.

Security and the Online Information Threat: The State of the Art

Current scholarship on security and security-making in relation to the online information threat is largely coloured by implicit or explicit assumptions about the envisaged object of protection. Different bodies of literature thus address the threat in slightly different ways. This section provides a brief summary of the research on online information threats to date, together with the primary criticism directed at each body of research, paying particular attention to the question of security.

Most research on the online information threat has been conducted within Defence and Intelligence Studies, employing the concept of ‘information warfare’ or more specific military-operational terms, such as ‘information operations’ or ‘psychological operations’, to describe the online information threat. These studies are

---

2 Information operations are defined by the US Department of Defense as ‘the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own’ (Porche et al. 2013, 103).

3 Psychological operations are defined by the US Department of Defense as ‘planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator’s objectives’ (US Department of Defense 2010, GL-8).
based on an understanding of information as a strategic weapon employed in state-to-state relations. As Daniel Ventre (2016) writes, a successful information operation is intended to ‘destroy, deteriorate, disrupt, deceive, exploit and influence enemy functions’ by targeting ‘leaders’ and other ‘human decision makers’ (Ventre 2016, 44). The aim is to impair ‘the enemy’s information and its functions while seeking to protect those on which one’s own military effort depends’ (Nincic 2003, 141). While cyberspace is considered a complicating factor in security-making, the envisaged path to security is still pursued within the traditional state-centric framework. Security is in the hands of a ‘cyber-defence’ (Heckman et al. 2015). In more extreme versions, the aim is ‘cybersovereignty,’ the establishment of Westphalian virtual-territorial boundaries in cyberspace (Demchak and Dombrowski 2014), or even the launching of a government-operated ‘alternative internet’ (Pherson and Mort Ranta 2019). On a strictly operational level, however, threat-descriptions and security-making practices focus on individual human vulnerabilities. Most notably, securitizing actors themselves as well as scholarship on security draw heavily on the ‘mind sciences’ of cognitive psychology, social psychology and evolutionary perspectives in psychology (Palmertz n.d. 3-4). Outlining the ‘theoretical foundations of information operations’, Björn Palmertz, for instance, argues that we need to understand the ‘mental processes and social circumstances that govern how we form attitudes, make decisions and implement them’ (Palmertz n.d. 3-4 and 34) when developing a defence against enemy operations. Such insights into the cognitive aspects of decision-making can also provide pointers for the conduct of powerful offensive information operations. In the light of this envisaged efficiency of perception-management, however, critics point to the potential dangers of countering enemy operations online. Miroslav Nincic, for instance, emphasizes that offensive information operations conducted in cyberspace – a sphere without state territorial boundaries – might blur the line between domestic and interstate practices for perception management (Nincic 2003, 147 and 141). In other words, when messages are directed at (foreign) enemies in cyberspace, they may still ‘convey the distortions to a domestic audience’ (Nincic 2003, 141). Such distortions, furthermore, can undermine ‘the public’s ability to form an autonomous judgement of government actions and to hold it accountable for these actions’ (Nincic 2003, 141). Countering online information threats through offensive information operations could essentially lead to problems with transparency and accountability – key principles in any democratic context.
In contrast to this clear-cut national security perspective, many contemporary scholars within Strategic Studies conceptualize the online information threat in relation to the problems caused by increased digitalization. Describing the threat as a key part of ‘hybrid warfare’ – ‘the synchronized subversive use of multiple instruments of power tailored to specific vulnerabilities (including cyber vulnerabilities)’ (Omand 2018, 13) – this literature opens up for new non-state enemy actors and a broader object of protection.\(^4\) Regarding the civil population as vulnerable to Islamist fundamentalist ‘radicalization’ (Jasper and Moreland 2014) or as ‘psychologically’ unprepared for Russian ‘info-war’ (Aro 2016, 127), security goes from being the protection of the territorial state to the protection of the citizens within the state. In turn, protecting the democratic public requires a ‘comprehensive’ form of security (Aaronson et al. 2011 and Omand 2018). A widely embraced method is ‘strategic communication’\(^5\) (Taylor 2002) – communication with ‘clear objectives’ used to inform, influence and persuade the target audience (Paul 2011, 5). The idea of protecting the democratic public from outside threats spread through online communication, however, builds on a set of problematic assumptions. Arguing that the proposed countermeasures rest on a ‘fundamentally flawed’ understanding of the premises for communication, Cristina Archetti highlights the neglected ‘network’ dimension of meaning creation (Archetti 2018, 83). In short, the depiction of strategic communication as having ‘clear objectives,’ or the assumption that communication can be a ‘powerful weapon’ used by enemies, leaves out the fundamentally intersubjective nature of communication. Communicative ‘truth’ cannot simply be inserted top-down, but is the outcome of a collective process of interpretation (Archetti 2018, 93). In a democratic context, such assumptions are even more problematic, since the intersubjective production of political ‘truth’, arising out of communication, is also a means of drawing the boundaries for legitimate authority.

Distancing themselves from the notion of purposefully disseminated information threats, critical voices in a wide range of fields, including Critical Security Studies, Communication Studies and Computer Science, point to the inherent difficulty

\(^4\) This view is also present in contemporary Intelligence and Defense studies to some extent, but the discussion of hybrid warfare focuses more directly on the broader vulnerabilities.

\(^5\) The concept is a product of military doctrine, but has increasingly been seen as a method that should be embraced by democratic governments. Cornish et al. (2011), for instance, describes strategic communication as a ‘constitutional obligation’ (Cornish et al. 2011, 11).
of strategic action in an environment characterized by complexity and change (cyberspace). While some point to the fertile ground cyberspace provides for the spread of conspiracy theories (Marwick and Lewis 2017), others stress the commercial incentives driving the online information threat (Benkler et al. 2018, Allcott and Gentzkow 2017; Bakir and McStay 2017), or the technical dimension, as in the case of ‘bots’ used for spreading information (Kollanyi et al. 2016) without the direct involvement of human actors.\(^6\) A weakness in many of these studies, however, is that they rarely engage with the concept of security per se. Consequently, how to understand security beyond the framework of purposeful action commonly applied in Security Studies, and what to protect in an environment characterized by complexity, ambiguity and change, are still questions largely left unanswered. However, there are a few notable exceptions. In a study of the role of citizens as ‘curators’ of ‘disinformation’ during the war in Ukraine, Yevgeniy Golovchenko et al. (2018), for instance, point to individual internet users as influential actors in spreading both disinformation and counter-disinformation online. This case highlights the complex, and largely civil, dissemination of the online information threat, but also the individual dimension of security-making. From a different point of view, Henry Farrell and Paul Schneier draw on computer security literature to argue that online information threats must be understood as attacks on the ‘common political knowledge’ holding together the ‘decentralized’ democratic system (Schneier and Farrell 2018, 1). Making ‘no strong distinction between insider and outsider effects’ on the democratic system, the approach helps to explain why ‘state-to-state logics’ fail to offer appropriate solutions to the online information threats (Schneier and Farrell 2018, 18 and 1). While opening up new avenues for understanding security from the perspective of democratic politics in a digital age, Schneier and Farrell nevertheless fail to consider the core question of ‘the people’ in the light of the threat (Schneier and Farrell 2018, 5). Treating democracies as given entities (albeit held together by common political knowledge), and starting on the ‘level of the nation-state’, their account steers past more fundamental questions about the boundaries of democracy addressed in this dissertation (Scheier and Farrell 2018, 5).

\(^6\) These factors are touched upon by Omand (2018), but the focus is mainly on enemy actors and their intentions.
Conceptualizing Security

The meaning of security is often summed up in the question: ‘security of what?’ At the heart of the matter is an idea of something to be secured – a ‘referent object’ (Buzan 1998, 38). For much of the history of the wider field of Security Studies, this object has been the sovereign state. Thus security, in the most traditional sense, means national security, which essentially entails the protection of sovereign territorial boundaries from the actions of other states. This particular conceptualization of security can be understood in relation to a specific set of historical circumstances, but it is also a consequence of the intellectual links between Security Studies and International Relations (IR). Security scholars working in the tradition of political realism traditionally borrowed much of their analytical substance from the larger state-centric discipline of IR (Walt 1991). In what is referred to as the ‘critical turn’ in Security Studies, however, normative, empirical and methodological arguments were forwarded in favour of a simultaneous broadening and analytical specification of security as a concept.

Taking human emancipation as a normative starting point, early work in Critical Security Studies pointed to both the empirical unhelpfulness of state-centrism in a world of domestic conflicts and the obscuring of human suffering such conceptualizations reproduce (Wyn Jones 1999 and Booth 1991). Arguing that states often emerge as the main threat if the human being is seen as the referent object of security (Booth 1991, 318), this perspective turned the tables on traditional understandings of security as inextricably linked to physical territory. Scholarship connected with the Copenhagen School instead criticized national security from an analytical viewpoint, using the concept of ‘securitization’ to demonstrate connections between security and politics (Waever 1995). Security is here conceptualized as a ‘self-referential practice’ (Buzan et al. 1998, 23-24). In other words, rather than assuming that threats exist independently of claims to security, this literature describes security as the result of state actors forming existential threats in relation to a variety of ‘referent objects’ of protection (Buzan et al. 1998, 23-24). This decoupling of security

---

7 In the UK, the field is known as ‘Strategic Studies’.
8 Buzan et al. (1998) emphasize that other entities may be involved in securitization processes, but their main focus is states (Buzan et al. 1998, 24).
and sovereignty allowed for a highly diverse set of ‘securities.’ Suddenly, it was possible to speak of ‘military security’, ‘environmental security’ and ‘political security’ etc. (Buzan 1998 et al). Furthermore, each referent object came with its own inherent logic. Whereas the object of protection in military security is usually the state, in political security it is sovereignty, and, in environmental security, it is the survival of a particular species (Buzan et al. 1998, 22-23). Indeed, almost anything can be made a referent object of security as long as it is framed in relation to an existential threat.

By opening up for new innovative approaches to security, the critical voices made possible more fine-grained analyses that go beyond the protection of territorial sovereign boundaries. But this problematization of security also led to questions about how to understand the suggested link between security and politics (Balzacq 2019). A notable problem with the Copenhagen School’s conceptualization of ‘securitization’ is that security and democratic politics turn into opposite poles on a continuum (Vuori 2008). While more analytically than normatively driven, the literature on securitization nonetheless springs from an explicit critique of state actors outlining and mobilizing existential threats in the name of security. Security entails the justification of actions and policies ‘outside of the normal bounds of political procedure’ as well as the use of ‘extraordinary means’ (Buzan et al. 1998, 24). As a consequence, the proposed remedy for securitization is ‘desecuritization’ – a rolling back of security (Waever 1995). By envisaging security as a negative ‘mirror-image’ of democratic politics, the resurrection of such procedures becomes an obvious underlying goal (Aradau 2004, 389). In the words of Barry Buzan, desecuritization can be achieved by shifting ‘issues out of emergency mode and into the normal bargaining process of the political sphere’ (Buzan et al. 1998, 29). One problem with this vision, as Claudia Aradau highlights, is that a reinstating of democratic politics must be tackled ‘politically’ rather than ‘analytically’ – a dimension underdeveloped in the Copenhagen School framework (Aradau 2004, 388). What is more, while traditional securitization theory is certainly useful for conceptualizing parts of security discourse, it fails to capture both ‘silent’ forms of insecurity – instances where insecurity ‘cannot be voiced’ (Hansen 2000, 287) – and cases where security and politics are pursued in tandem. As critics underscore, securitization is not necessarily divorced from everyday politics, but may be an inherent part of it (Aradau 2004, 396). In other words, security-making can also take place in the absence of explicit speech acts or references to objects of protection.
In response to these challenges, Paris School scholarship, drawing on approaches from International Political Sociology (IPS), has suggested that the meaning of security is articulated by bureaucratic professionals engaging in threat discourses. In this way, security and insecurity become closely intertwined in a ‘self-sustaining dynamic’ that allows security professionals to expand and uphold their own power (Bigo 2008, 124). Rather than trying to understand the meaning of security, or a proposed referent object, we should focus on the reproduction of power among these groups ‘authorized to state what security is’ (Bigo 2006, 195). Pointing to mundane bureaucratic processes as drivers of (in)security, this literature thus modifies the conceptualization of securitization as necessarily connected with explicit speech acts and exceptional measures (C.A.S.E. 2006, Bigo et al. 2007, Ceyhan 1998). Arguing that a state of exception might, in fact, be unrecognizable when cloaked in bureaucratic terms, it is suggested that we should pay attention to everyday practices of security-making. The sociological assumptions underpinning such studies undermine the notion of intention underlying much research within Security Studies: if security professionals are the drivers of (in)securitization, then individual intentions are largely unimportant, since security does not emerge from a single actor, but is rather the outcome of innumerable competitive bureaucratic processes (Bigo 2008, 124). Moreover, in terms of critique, it appears as if the collapsing of distinctions between security and insecurity makes all attempts at ‘desecuritization’ impossible. There is simply no way of ‘rolling back’ security within the Paris School framework. Instead, critical scholarship argues for a continuous unveiling of power relations: a ‘disruption of the ‘regime of truth’ created by the professionals of security’ (CASE 2006, 456). In practice, however, the preferred focus on the ‘power positions’ of securitizing actors, coupled with a dismissal of any possibility of ‘individuals creating new frames’ (Bigo 2002, 74), tends to make the question of meaning secondary to (rather than an inherent part of) the bureaucratic power struggle.

Considering these developments, we can see how the conceptualization of security has gone from denoting the protection of sovereign territorial boundaries to recognizing a wider constellation of referent objects and, in the end, an outright dismissal of such objects altogether. We seem to be left with two options in approaching the question of security. Either we conceive of security as a meaningful concept resting upon a clearly articulated and overt object of protection, as suggested in traditional
Security Studies and – in a slightly different way – by the Copenhagen School. Alternatively, we depart from a conceptualization of securitization which renders this question largely irrelevant, as indicated by scholarship drawing on sociological approaches to security. But agreeing with the Paris School – that securitization may be an everyday bureaucratic matter – does not necessarily entail dismissing the question of how to understand the referent object. It may well be the case that policymakers or security professionals engage in routines to extend their own powers. Nevertheless, all the activities pursued in relation to a threat – that is, the security interventions, threat descriptions, technologies and suggested policies – also reflect and reproduce certain understandings of security. In short, answers to the question ‘Security of what?’ may be implicit, while still guiding securitization.

This dissertation argues that engaging with such questions opens up the possibility of understanding what security means in relation to the online information threat, but also offers a way to conceptualize security in relation to other ‘complex threats’ that seem to require the involvement of many different policy sectors. The Copenhagen School regards securitization as inherently performative, demanding an overt referent object to mobilize speech acts. This dissertation suggests another approach to language, in line with two working assumptions: firstly, that securitization is achieved through all the active interventions envisaged and produced in relation to the online information threat; and secondly, that these active interventions are guided by a number of preconceptions about what to protect, which can be explored by focusing on the language used for describing these interventions. The role of language is by no means denied by the Paris School, for instance, but their focus is usually on processes of (in)securitization. Since security and insecurity are intimately tied together, discussions about what to secure are viewed as an instrumental part of a bureaucratic power game, not as aiming at security. But any critique of bureaucratic power would be incomplete if we fail to pay close attention to the preconceptions guiding securitization processes. In short, if we assume that policymakers and security

---

9 The 2015 European Agenda on Security describes complex threats as threats which are ‘cross-border’ and ‘cross-sectoral’ in nature, and therefore in need of a coordinated and comprehensive approach to security (European Commission 2015, 2).

10 A notable exception is Thierry Balzacq, who, citing Bourdieu, raises the question of implicit goals guiding policymakers (Balzacq 2010, 2). The approach described by Balzacq is, however, concerned with a wider constellation of securitization practices, and the role of the audience, rather than the referent object implied in such practices.
professionals are key actors in driving securitization in relation to complex threats, we also need to pay attention to how they describe the threat. This does not mean that we should attempt to disclose the intentions of central actors, as in traditional Strategic Studies, but rather that we should seek to find shared preconceptions about what to secure that direct securitization processes. Accordingly, the approach to security outlined here involves a novel conceptualization of the referent object. The present study does not treat the referent object of security as constituted through intentional or overt speech acts; rather, it approaches preconceptions of protection as a frame that is taken for granted and implicitly guides security-making. Furthermore, there may be several overlapping answers to the question of what constitutes the object to be protected, rather than just one.

Lastly, in contrast to the ‘unmaking’ of securitization proposed by the Paris School, or the demand for ‘desecuritization’ by the Copenhagen School, this dissertation takes up Aradau’s suggestion that we tackle the question of security ‘politically’ (Aradau 2004, 388). In critiquing and rethinking the referent object, the dissertation draws on a core insight from post-foundational political theory: that the meaning of security cannot be understood apart from political community. For a long time, the territorial sovereign state was the referent object of security par excellence. As Walker (1990) argues, this is because sovereignty allows for a double picture, superficially reconciling the demands of political community and political authority through territoriality. But authority necessarily implies authorization. And in a democratic context – which what we are concerned with here – legitimate authority implies authorization by ‘the people’. By describing political community as the people living within a predefined territory and legitimate authority as synonymous with state authority (Walker 1990, 9), the collective authorization of authority is essentially obscured. While admitting that the persistent foregrounding of state security makes it difficult to consider and reasonably argue for other alternatives to political community, Walker claims that such visions can be called into question by focusing on the ‘constitutive account of the political’ (Walker 1997, 69). In other words, by first asking how the modern political subject ‘can be reconstituted’ and, then, what security ‘can possibly mean in relation to it’ (Walker 1997, 78), it becomes possible to rethink security. A similar take is proposed by Dillon (1996), who urges us to ‘recover’ the political dimension of security in a more normative sense – in relation to what he takes
to be the ‘human being as a possibility’ (Dillon 1996, 2). If we embrace the understanding of freedom as grounded in the human being as a possibility, it becomes clear that politics can only ever be democratic (Dillon 1996, 38), and only ever public, in the sense of creating new possibilities through human action. Guided by such notions, the process of critiquing and rethinking security means scrutinizing the political dimension underpinning referent objects proposed in policy, but also asking how we might reasonably conceive of political community in a manner suitable for a democratic context: acknowledging ‘the people’ or the demos as the basis for legitimate authority\textsuperscript{11}, rather than simply assuming that security can be considered and achieved apart from it.

Methods and Material

In exploring the meaning of security – asking the question ‘The security of what?’ – this dissertation focuses on language use. The aim, however, is not to propose a universal definition of security. Investigating the referent object means paying close attention to the way the online information threat is described as a security problem, but also to how remedies are articulated in relation to the threat. To this end, the methods employed involve close readings of texts on the topic: policies, reports and policy discussions. Yet the situation also matters for meaning: not everything can be securitized in the same way under all circumstances. As noted in the second article included in this dissertation, the concept of state sovereignty is tied to an idea of territoriality, and is fundamentally different in a non-territorial cyberspace. As a result, fundamental preconceptions about what to secure play out differently depending on context – they might make sense in one situation, but not in another. This, in turn, invites further questions. What conditions are implied in a particular preconception of security, and how do they play out in the context of cyberspace? What problems arise in the pursuit of one referent object that might be alleviated if we conceptualize security from some other vantage point? Pursuing such questions, the dissertation draws on extensive empirical material: primarily EU policy and policy discussions on the online

\textsuperscript{11} In his discussion on ‘extraordinary politics,’ Michael Williams describes a similar conceptualization of securitization that incorporates the political (Williams 2015).
information threat (Ördén 2019 and Ördén 2018), but also material produced by securitizing actors such as NATO, as well as reports by policy research institutions such as RAND Corporation. The emphasis is on publicly available empirical material of an informative nature that is likely to be disseminated to other actors interested in the online information threat. This material is used to explore contemporary preconceptions of security and their inherent limitations, but also as a point of departure for rethinking the referent object. The primary aim, however, is not to make an empirical contribution. Following Jens Bartelson, we might say instead that how we speak about things reflects ‘underlying presuppositions about the sociopolitical world and the conditions of its intelligibility’ (Bartelson 2000, 189). Hence, the overarching purpose of the exercise is to examine the conditions for thinking about security in relation to the online information threat.

This basic unit of analysis has been articulated in various ways. We might claim to investigate ‘concepts’ (Adcock 2005, 5), ‘conceptions’ (Adcock 2005, 5), ‘acquired and non-reflected modes of thought’ (Foucault 1982, 33), ‘frames’ (Rein 1996), or ‘angle[s] of vision’ (Pitkin 1967, 11). The term employed here is ‘preconceptions’, since ‘concept’ or ‘conception’ indicate terminological continuity, while ‘frames’ or ‘angles of vision’ suggest that preconceptions are temporary and can be altered. Terminology aside, it is important to clarify that preconceptions, as understood here, are not cognitive or mental entities. Instead, they are intersubjective, linguistic, and fundamentally social (Adcock 2005, 24). Unlike much contemporary empirical research on EU policy, then, the aim is not to explicate the intentions of any centrally placed policymaker. To investigate preconceptions is not to divulge conscious strategies or recapitulate carefully crafted arguments – preconceptions cannot be gleaned from individual interviews. The intersubjective focus also sets the methods employed in this dissertation apart from ‘idea analyses,’ which focus primarily on explicit arguments (Beckman 2005, 12). Consequently, when asking why humour is proposed as a remedy for online radicalization, the answer sought is not a cognitive nugget in some policymaker’s mind. Rather, as shown in the first article included in this dissertation (Ördén 2019), the aim is to elucidate referent objects of protection in relation to which the proposed descriptions, policies and strategies to tackle the online information threat make sense. By considering that ‘political and social events and circumstances’ can be read through language, and focusing on the meaning discernible
in language use, the ‘unpacking of security’ pursued in this dissertation has certain similarities with conceptual history (Koselleck 1985, 86). However, rather than tracing conceptual change historically and exploring the different meanings linked to a particular concept over time, the dissertation explores how a phenomenon is described (in diverse ways) as it emerges as a problem in need of political action. As Thierry Balzacq underlines, policy interventions proposed in relation to security problems can in themselves be seen to ‘embody a specific image of the threat’ (Balzacq 2008, 80). Being a collective solution to a problem, policy incarnates an intersubjectively shared view of security. As Balzacq asserts, securitization can, furthermore, ‘be oriented toward a goal without being consciously informed by it’ (Bourdieu cited by Balzacq 2010, 2). The aim of the methods employed is to unearth this often-implicit goal, but also to address this goal critically and suggest alternative perspectives. The latter ambition – critiquing and rethinking security – takes as its point of departure an assumption that alternative visions also should be contextually anchored. As Michael Waltzer underscores, the most desirable form of critical reading is a form of ‘connected’ criticism (Waltzer 1987, 33). In other words, while one must necessarily distance oneself from ‘authority and domination’, critique should appeal to ‘local or localized principles’ and is best seen as an ‘internal argument’ (Waltzer 1987, 52 and 33-34). In this vein, the rethinking of security is anchored in a critical reading of preconceptions guiding existing policy initiatives, and the aim is to address the shortcomings of such initiatives in a context which accepts that democratic legitimacy should be grounded in the people. As a critic, then, I am not ‘a man from Mars’, but a fellow democratic subject (Waltzer 1987, 33).

In the below section, I first outline the arguments for using the EU as a case for investigating security; next, I describe the materials and methods employed in unpacking security empirically; third, I explicate the critical approaches employed; and, fourth, I account for the methods and material used for rethinking security.

The Case of the European Union

This dissertation uses EU policy and policy discussions for exploring the meaning of security in relation to the online information threat. There are three reasons behind this choice of material.
Firstly, from the very beginning, the EU Commission encouraged extensive knowledge production in relation to online information threats, and has greatly contributed to formulating the approaches to security used throughout the EU. Funding a multitude of local and national organizations that produce and disseminate ‘best practices’, the Commission facilitated the spread of specific versions of security to all EU Member States. The online information threat was considered a ‘complex threat’ from the outset, and security-making spanned several different policy areas, making policymakers and policy intellectuals key actors in formulating the meaning of security. An examination of the preconceptions guiding this form of cross-sectoral policy is therefore likely to reflect the multifaceted nature of the contemporary online information threat more accurately than, for instance, an examination of traditional security policy. What is more, given the central role of these policymakers in formulating and disseminating shared knowledge throughout the EU, an analysis of policies, reports, and ‘best practices’ produced by these groups sheds light on preconceptions about protection guiding securitization beyond the narrower scope of these specific policy communities.

Secondly, the EU is an actor with an explicit vision of promoting democracy in cyberspace. As is evident in the first Cybersecurity Strategy, the idea of a democratic cyberspace has been part and parcel of EU policy in the area from the start. The first Cybersecurity Strategy, published in 2013, spoke of cyberspace as a ‘open, safe and secure’ sphere and an ‘area of freedom and fundamental rights’ (High Representative 2013, 1-2). As the focus turned to the communicative side of cyberspace, this question not only gained in importance, but became an intrinsic part of security. The rise of Islamic State and the emergence of ‘hybrid warfare’ during the subsequent crisis in Ukraine put new communicative threats such as online radicalization, Islamist propaganda and Russian disinformation on the EU security agenda. In this security work, seemingly diverse problems came to be addressed together as threats to ‘European values and interests’ that spread with the help of ‘new technologies’ (Fotyga 2016). In just a few years, the idea of cybersecurity went from concerning a rather uncomplicated vision of openness online to focusing on how to manage threats arising from such openness without restricting freedom and fundamental rights. The EU can thus be seen as a paradigmatic case for understanding security in relation to the online information threat in a democratic context.
Investigating the policies proposed in relation to this threat can cast light on the difficulties involved in reconciling security-making with the promotion of democratic principles in cyberspace.

Thirdly, the EU has recently emerged as a key global actor in the area of information and communication technologies. Early on, the work surrounding the online information threat gave rise to a forum for dialogue between the EU Commission, leaders of Member States, and internet companies such as Google, Facebook, YouTube and Twitter (EU Internet Forum 2016). Later, as the Cambridge Analytica scandal broke, the Commission gained ground when it threatened Facebook with massive sanctions unless the company saw to it to ‘inform consumers how the social network gets financed and what revenues are derived from the use of consumer data’ (European Commission 2018). While this dissertation does not consider these recent legislative developments, the early formulations of what security is explored in the articles are likely to persist. It is also possible that early policy interventions in relation to online information threats contributed to the current influential role of the EU. As Thierry Balzacq underscores, ‘policy tools’ such as, for instance, technical instruments for securitization, are ‘powerful strategies for harmonizing what otherwise remains highly disputed, both in terms of what is at stake and what ought to be done about it’ (Balzacq 2008, 78). Hence, the introduction of databases with restricted content shared between Europol and the internet industry, for instance, or the ‘Code of Conduct’ regulating hate speech, today work to guide content deletion online (EU Internet Forum 2016). To understand the preconceptions about protection guiding these early interventions is therefore crucial for making sense of current EU policy. In addition, the contemporary role of the EU as a powerful global actor in relation to the communicative side of cyberspace makes it likely that the suggested solutions have influenced how other actors understand security in this area.

Unpacking Security through the Online Information Threat

The first article included in this dissertation (Őrdén 2019) turns to policy material, reports and discussions produced by the EU with the aim of unpacking security through the online information threat.
The empirical analysis is pursued in two steps. First, a descriptive analysis of the work pursued by the EU on the topic of online information threats pinpoints the specific policies proposed. The minimal criterion for selection of material has been that the document in question must describe the online information threat as dangerous and in need of political action. As previously noted, this wide scope is very much in line with the comprehensive approach to online information threats pursued within the EU; for this reason, the material considered stretches beyond the narrower field of security and defence policy into such as areas education, internet, culture and media policy. Unearthing the specific policies proposed in these areas, the descriptive analysis pinpoints distinct and identifiable solutions to the problem of online information threats. The process has followed an inductive logic, searching for initiatives on online information threats listed in central EU documents and reports produced between 2015 and 2017. Guided by an ideal of theoretical saturation, this exploration can never guarantee a full mapping of material. It should be emphasized that the approach is not an attempt to offer a complete picture of EU policy, but a starting-point for exploring preconceptions of security in relation to the online information threat.

When analysing the preconceptions, the reading draws on ‘value-critical policy analysis’ (Rein 2012). As Martin Rein highlights, value assumptions guide ‘action and thought’ in policymaking (Rein 2017, ix). Attention to the security-related values guiding proposed interventions allows us to ‘ferret out the implicit, rather than the expressed’ dimension of policy (Rein 2017, ix). A core assumption is that understandings of security can differ between policy communities and the analysis pays attention to the values forwarded by the communities articulating specific policies. The specific forums investigated were selected on the grounds that they are particularly active in articulating knowledge in relation to the policies pinpointed. An illustrative example is how ‘media literacy’ is proposed as a solution in the media and education sector. Investigating the security-related values, the analysis then explores how ‘media literacy’ is described in documents, discussions and policies produced by the influential Media Literacy Expert Group. Asking what ultimate purpose or security-related end value the suggested policy is perceived as serving as well as in what way the approaches proposed serve this end brings to light the intrinsic and instrumental values guiding

---

12 Albeit not in need of exceptional measures, such as one finds in the Copenhagen School understanding of securitization.
policymaking. The referent object is discerned by considering how this desired end goal of policy corresponds to the question ‘The security of what?’ Overall, the empirical material used in this part of the analysis is multifaceted. A minimal criterion for selection of material is that it should reflect shared, rather than personal or individual, understandings of security. In addition, the emphasis is on material that is publicly available. Apart from official policy documents and proposed interventions, the analysis takes into consideration minutes of meetings (3), speeches (1), official press releases (4) and reports (2), joint agreements (1), official declarations (1), recorded meetings available online (1), transcribed presentations (1) and follow-up documents on policy proposals (1). Supporting material cited and directly recommended by selected forums is also used to make sense of the claims found in policy (Taylor 2002 and Cornish et al. 2011). Finally, to shed light on potential practical implications of policy, the analysis situates the policies in relation to the shared values guiding the actors implementing them. Using illustrative empirical cases as well as examples from existing research (Hedling 2018), this analysis is primarily heuristic and intended to highlight potential value-conflicts arising in the implementation process, rather than to make an empirical contribution.

The value-critical approach comes with certain limitations. First, it should be noted that the variety and availability of material differs between forums. While the analysis of media literacy and media pluralism draws on a full recorded meeting, as well as a summary of presentations and two comprehensive meeting summaries, the analysis connected to online censorship relies solely on official press releases and central documents released by the EU Internet Forum. Second, as explained by Rein, the value-critical method serves to ‘construct,’ rather than simply reflect, the preconceptions guiding policy interventions (Rein 1996, 90. Orig. italics). In any interpretive approach, several meanings may correspond to a suggested course of action, leading to potential ambiguity. Yet, empirical material still creates ‘an outer limit for our imagination’, and some ways of describing an issue ‘make more sense than others’ (Alvesson and Kärreman 2011, 61). Hence, by substantiating all claims made, and using illustrative empirical examples consistently, the analysis strives towards a transparent reading.
Critiquing Security and the Online Information Threat

In addition to unpacking the preconceptions guiding policy work empirically, the dissertation engages in critical readings with the aim of describing the conditions under which proposed referent objects make sense, but also fail to make sense, in relation to online information threats. Elucidating the limitations of each preconception of security, the articles juxtapose policy texts with theoretical and philosophical writings selected on the basis of their engagement with the central questions of security: political community and legitimate authority. Two specific referent objects in particular the focus of critical reflection: human judgement and the sovereign state.

As shown in the first article (Ördén 2019), the turn to human judgement is a common feature in EU policy work in relation to the online information threat. In order to interrogate this preconception about protection critically, the third article (Ördén 2018) turns to policy material produced by the Radicalization Awareness Network (RAN) – a broad array of practitioners funded by the EU Commission. The empirical material consists of policies produced by RAN@, the RAN subgroup engaged in producing policy in response to online radicalization. Particular attention is paid to a 2012 policy proposal listing counter-narratives of ‘humour’, ‘fact’ and ‘logic’ to serve as starting points in online counter-radicalization work (RAN@ 2012), as well as to the online collection of ‘good practices’ produced by the group in 2016 (RAN 2016). Teasing out the unquestioned background in relation to which these specific counter-narrative methods make sense as instruments of online counter-radicalization, the analysis focuses on the assumptions about the human mind in RAN policy, drawing on Arendt’s discussions about political judgement. In order to support the explication of potential assumptions underpinning the counter-narrative methods, other philosophical texts engaging with ‘humour’, ‘fact’ and ‘logic’ are also revisited (Kant 1987, Critchley 2011, Bergson 2009, Plessner 1970, Tønder 2014). Reading the policies in the light of two separate categories of judgement – determinant and reflective judgement – where the latter, in Arendt’s view, represents true political judgement, the analysis interrogates the potential for instilling political thinking though the methods proposed by RAN. Reading policy in the light of the specific conditions for Arendtian political judgement, the article critically evaluates the potential of counter-narratives of
humour, fact and logic as strategies for securing the form of political judgement grounding human coexistence.

In recent years, national security approaches to cyber threats and the understanding of sovereignty as a referent object in cyberspace have together come to guide security policy internationally (Dunn Cavelty 2015). This referent object is also notable in its absence in the Westphalian visions of information warfare underpinning EU security interventions outlined in the first article (Ördén 2019). In order to examine how this novel raison d’état in cyberspace is put into practice in policies aimed at countering online information threats, the second article consists of a critical reading of the wider conceptual construction of ‘cyber sovereignty’. First, the specific demands and conditions for this referent object are outlined; the reading then turns to academic material describing how sovereignty can and cannot be protected in cyberspace. The analysis borrows from previous research suggesting a turn to Cyber Westphalia (Demchak and Dombrowski 2014 and 2013), as well as from critical perspectives on national security in relation to cyber threats (Dunn Cavelty 2014) and philosophical work concerning sovereignty and territoriality (Whitt 2010). In a second step, the approach to online information threats is examined by drawing on a report on disinformation published by NATO Strategic Communication of Excellence (Pamment et al. 2018). Paying specific attention to how the threat is described in this report, the reading draws attention to a set of assumptions about democratic legitimacy and political authority that emerge when we understand the online information threat from the perspective of national security. With inspiration from post-foundational theory on the construction of sovereign authority (Whitt 2010) and ‘the people’ (Arendt 1977, Derrida 1986, Honig 1991, Näsström 2008, Whitt 2010), the analysis elucidates the conditions for, and limitations on, the exercise of legitimate authority in cyberspace when the boundaries of the demos are not known. Like the previous critical reading, the interpretations outlined here rely on a combination of empirical and philosophical material. But rather than applying a set theoretical framework, the approach is similar to the method of ‘critical reflexivity’ suggested by Mats Alvesson and Dan Kärreman (2011). Empirical material is primarily seen as ‘a partner for critical dialogue’ (Alvesson and Kärreman 2011, 14. Orig. italics.). The material is employed to illustrate ideas and ‘facilitate and encourage critical reflection’ in relation to previous research, while theoretical writings are employed to describe the demands and conditions for central assumptions illustrated by policy (Alvesson and Kärreman 2011, 4). The
juxtaposition of very different types of texts thus helps to reveal the inherent limitations of the cybersovereign approach in relation to specific threats spread through online communication.

Rethinking Security through the Online Information Threat

The unpacking and subsequent critique of preconceptions not only helps to answer what security means in relation to online information threats: it also fills a distinct methodological purpose. By showing how not all referent objects are equally viable in relation to the online information threat in a democratic context, the readings produce starting points for further exploration. In response to the problems pinpointed, the second article argues that we need to ‘rethink’ security in a way that acknowledges the centrality of independent human communicating subjects in democratic life.

In rethinking security, then, the dissertation is grounded in contemporary policy insofar as it draws on empirical material, while it avoids applying traditional conceptualizations of security. The empirical material used in this reading illustrates and ‘anchors the process of theorization in specific claims about the object under study’ (Alvesson and Kärreman 2011, 61), while theoretical and philosophical texts are used to explore new ways of approaching the issue. The requirements to theory outlined by Dunne et al. (2013) serve as a basic guideline: in a satisfactory theoretical account, ‘ideas should follow logically from one another and, in general, they should not contradict each other, or at the very least they should have some clearly defined relationships to one another, and when contradictions do occur they are seen as potential problems for the theory’ (Dunne et al. 2014, 409). In terms of empirical material, the rethinking of security draws on a recent report on online information threats from the RAND Corporation (Kavanagh and Rich 2018), a report commissioned by NATO StratCom (Bertolin 2019 and Christie 2019) and an online platform on disinformation produced by the EU External Action Service (EUvsDisinfo 2019), as well as on psychological research cited in the RAND report (Roets and De keersmaecker 2017). Explicating the possibilities of safeguarding democratic legitimacy in the context of cyberspace by turning to judgement, the analysis then draws on Arendt’s writings on ‘political judgement’ (Arendt 1982), Linda Zerilli’s outline of a democratic theory of judgement (Zerilli 2016), and critical discussions of Arendt’s philosophy by Jürgen
Habermas and Thomas McCarthy (Habermas and McCarthy 1977). Reading contemporary policy through the proposed normative framework of political judgement, the discussion illustrates how the proposed entry point can point out potential problems in current approaches outlined by NATO StratCom (Christie 2019) and the EU-funded RAN (RAN H&SC 2019).

By specifying a distinctly normative version of judgement which does not rely on assumptions about a pre-existing people, this rethinking of security provides guidance for approaching the online information threat. It should be noted, however, that the aim of this exercise is not to provide a single universal conceptualization of security. Instead, in the spirit suggested by Alvesson and Kärreman, the ambition is to ‘see’ new issues and themes, ask new questions, challenge the established wisdom, open up alternative lines of thinking’ (Alvesson and Kärreman 2011, 27). Nonetheless, in the best case, rethinking security should have both practical and theoretical implications. To this end, a minimal criterion guiding the theoretical reading is that the alternative angle should acknowledge previously neglected aspects of contemporary security policy, while simultaneously opening up for alternative understandings, including a potential revision of existing frameworks within Security Studies at large.

Summary of the Articles

This dissertation comprises three articles written for publication in peer-reviewed journals. The first was published in Intelligence and National Security and the third in Critical Studies on Security. The second article is under submission. In this section, I provide a short summary of the separate articles.

Article 1. Deferring Substance: EU Policy and the Information Threat

The first article explores the meaning of security in relation to the online information threat by looking at EU cross-sectoral policies and policy work. First, it maps EU policy and policy work on the topic; second, it examines the security-related values expressed in policy work; third, it examines the values guiding policy implementation in the light
of previously expressed goals. Since no comparable account of the preconceptions guiding the contemporary and multifaceted online information threat is currently available, the essay makes an empirical contribution to the field of Security Studies. It also provides a basis for the theoretical discussion pursued in subsequent articles.

The investigation finds four proposed remedies to the online information threat: strategic communication, censorship, media literacy, and media pluralism. These remedies, in turn, are articulated in four separate EU policy communities: security and defence, internet, media and the education community. Exploring local knowledge within these policy communities, the essay detects two distinct ways in which they collectively make sense of security. First, the security/defence and internet communities see security-making primarily in abstract procedural terms, emphasizing the values of efficiency and coherence. The information and communication environment is described as a digital ‘battlefield’ that should be protected through continuous management; that is, by the deletion and production of online content. However, any articulations of end values, i.e., specific descriptions of content to be deleted or produced, are here left to experts or private actors. In sum, then, the overarching focus is on taking action, rather than on the substance of the action taken. Second, the media and education communities link security to the production of pluralistic online content and initiatives encouraging internet-savvy citizens to evaluate content critically and seek credible sources of information. In this case, the implicit security-related values, are ‘perspectivism’ and ‘independence.’ The ultimate object of protection can be described as citizens’ independent democratic judgement. Turning to the process of implementation, the essay considers the possible implications of involving three different actors in security-making: civil society, professional communicators and the internet industry. The analysis concludes that the means applied in the security-making process may undermine the stated goal of securing citizens’ independent democratic judgement. Whereas EU policy describes efficiency in abstract terms, professional communicators and the internet industry, driven by media logic and technological solutions respectively, tend to regard efficiency as a value guiding both content production and deletion. At the same time, civil society actors may lose the very credibility that they enjoy as independent actors, if they are seen as messengers recruited by the EU.
All in all, the findings point to a problem connected to policymakers’ reliance on traditional preconceptions of security-making that emphasize an efficient response to threats and presuppose pre-defined enemies operating in a pre-defined space. While technological solutions provided by internet companies and the involvement of actors with extensive knowledge of communication practices may provide a more efficient management of this envisaged ‘battlefield’ online, the question of content cannot be ignored. The online space is no ordinary battlefield, since content is what constitutes the information and communication environment. Paradoxically, then, by focusing on taking action rather than the substance of the action taken – in particular with regard to the deletion of content – policymakers may subvert some of the very values that their security is intended to protect. As a consequence, they lose control over cyberspace, the very thing that they are working so hard to achieve.

Article 2. Securitizing Cyberspace: Protecting Political Judgement

The second article critically explores the paradoxical procedural consequences that seem to follow from the application of traditional conceptualizations of security to the information and communication environment. Analysing specifically the concept of ‘cyber sovereignty’ – located in the nexus between cybersecurity and politics – this essay outlines the limitations inherent in the application of national security frameworks to a perceived online information threat. The question is what kind of answer boundaries of sovereignty in cyberspace provide and, furthermore, whether it is possible to reconcile this approach with democratic legitimacy.

The article argues that approaching the online information threat through the framework of cyber sovereignty ignores the specific characteristics of ever-changing digital materiality, which, unlike physical territory, is notoriously inappropriate for the construction of lasting sovereign borders. The wider conceptual construct of cyber sovereignty also fails to consider the essentially human dimension of sovereignty – that sovereign authority in a democracy should be grounded in ‘the people’. Taken together, these shortcomings have implications for the possibility of security-making on democratically legitimate grounds. In the logic of cyber sovereignty, online information is thought to be illegitimate when it originates from ‘foreign’ actors. Yet, as cyberspace does not come with a pre-defined outside,
practice, the distinction between foreign and domestic is made by the securitizing actors themselves though continuous differentiation between legitimate and illegitimate information. The boundaries of the envisaged cyber sovereign state are thus continuously instated and reinstated in the name of democratic legitimacy. Yet democratic legitimacy cannot be properly articulated without reference to the people. Consequently, the lack of a territorial dimension of cyberspace raises the question of what democracy means when boundaries are not given.

The article rethinks security by showing that treating human judgement as a referent object in relation to online information threats can provide a better solution to these problematic issues of legitimate authority and political community. Moreover, seeing human judgement as the object of protection accounts for many of the unorthodox interventions suggested by securitizing actors in relation to the threat. But the rethinking of security also shows how this referent object, in order to live up to the accepted standards of democratic legitimacy, must be grounded in the interplay between independent human communicating subjects. Drawing on Arendt’s writings on ‘political judgement’, the article provides an understanding of the practice of judging as fundamentally political. Appealing both to human imagination and communicability, this conception of political judgement connects the individual communicating subject to a world shared in common with others.

**Article 3. Instilling Judgement: Counter-Narratives of Humour, Fact, and Logic**

The third article explores the relationship between counter-narratives and counter-radicalization in EU security policy by examining the turn to judgement as a remedy to the online information threat. Reading online counter-radicalization policies proposed by the Radicalization Awareness Network (RAN) in the light of the Arendtian concept of ‘political judgement’, this article investigates political possibilities in relation to the specific counter-narrative forms of humour, fact, and logic.

Drawing on the Kantian distinction between reflective and determinant judgement elaborated by Arendt in relation to political judgement, the essay argues that the appeal to logic, fact, and humour allows RAN to promote a familiar mode of democratic thinking in a seemingly unmanageable information and communication
environment. By equating security with the individual subject’s change of mind, and the threat of radicalization with errors of judgement, the EU attempts to instil either a more rational kind of decision-making or a judgement grounded in an ‘elastic’ and self-aware sociability. Every form of counter-narrative that RAN proposes, however, is predicated on the same instrumental assumption – the logic of measurable and efficient policy practices. Judgement is conceived of in relation to an expected outcomes and measurable results, rather than as an essentially open-ended individual process. Hence, while counter-narratives of humour do live up to Arendt’s description of political judgement proper in that they presuppose an unconditional acceptance of individual freedom, this freedom is circumscribed through the expectation of measurable and, ideally, predictable results. The turn to fact or logic, on the other hand, is not premised on political judgement proper, but on a set of shared standards. Logic and fact can only ever state ‘what is’, which, while appealing for policymakers, leaves little room for individual political agency.

In sum, read through the Arendtian lens, the counter-narratives of humour, fact, and logic proposed by the EU to instil democratic judgement in cyberspace come with a set of limitations. Political judgement proper is a practice grounded in an individual freedom which cannot be reconciled with expectations of measurable policy outcomes. While the turn to counter-narratives (and judgement) allows policymakers to address the problem of online information threats, it cannot solve the problem of security in a democratic context, where politics is grounded in human agency.

Conclusions

The empirical readings presented in this dissertation pinpoint two distinct referent objects of protection in relation to the online information threat: human judgement and the cyber sovereign state. On the one hand, policies such as ‘media literacy’ or ‘media pluralism’ aim to create internet-savvy citizens who are capable of making independent judgements in relation to online content. The preconception guiding such interventions is the protection of a form of democratic judgement which, if instilled, allows for continued democratic discussion online. On the other hand, traditional preconceptions
about national security continue to be applied to the online information threat. Describing the threat as ‘the sovereignty of the state, and the legitimacy of open and free debate,’ securitizing actors suggest that sovereignty should be the object of protection in cyberspace (Pamment et al. 2018, 7). In practical security-making terms, however, the lack of sovereign boundaries in cyberspace today means that protection is an ever-ongoing operation. EU policy in the security and defence sectors describes cyberspace as a digital ‘battlefield’, thus emphasizing the negative side of the Westphalian vision. Rather than being guided by ideas of protection, policymaking is largely driven by efficiency. Content management is left to private actors and experts – namely, the internet industry, which provides technical solutions for content deletion, or professional communicators, who may be driven by content reach and exposure. The critical analyses underline tensions between the two preconceptions guiding EU policymaking. In practical terms, the equal emphasis on both independent democratic judgement and efficient action on the online ‘battlefield’ makes for contradictory outcomes. This is especially problematic when security-making is left in the hands of experts and the internet industry. Professional communicators, guided by a logic emphasizing reach and exposure of online content, for instance, may contribute to a radicalized discussion climate, rather than counteract it. Furthermore, EU pressure on the internet industry to delete content without legal review creates a grey area in terms of online censorship. Such outcomes work counter to the desire for a democratic cyberspace long envisioned by the EU, and even undermine the goal of enhancing citizens’ independent democratic judgement.

The analysis of the link between between political authority and political community underpinning notions of security points to a more fundamental problem with policies that embrace traditional frameworks of national security. Drawing on post-foundational political theory, the dissertation argues that the core problem haunting security-making in relation to the online information threat springs from the fact that, in a democratic context, legitimate authority can never be understood apart from the collective subject authorizing it. What we normally call ‘democratic legitimacy’ is grounded in ‘the people.’ The reference to sovereignty allows territory to refocus debate about the essentially ‘political relationship between authority and subject onto geographic features of the social world’ (Whitt 2010, 201. My italics.). But the online information threat does not correspond to any specific territory. Without a
territorial dimension, the protection of cyber sovereignty can only make sense in relation to the collective subject itself, and, in a democracy, communication is the constitutive force of this collective subject. Seen in this way, it is clear that the problem of security in relation to online information threats is not a matter of the technical issues involved in implementation, nor of specific democratic principles, such as freedom of speech; rather the question of what to protect confronts us with questions the basic issues of democratic life. While this form of legitimacy is not grounded in a given demos, neither can it be a feature mobilized by securitizing actors. All this is not to say that democratic legitimacy, or even state sovereignty, is not threatened by malicious information spread online. Rather, the crucial point is that these matters cannot be secured through the evocation of territorial boundaries in cyberspace.

Securitizing actors working in a democratic context need a different referent object, one that corresponds to communicative action. The conceptualization of judgement as a referent object presents a viable path forward in this regard, and this lens can be used to make sense of a wide range of diverse policy initiatives connected to the online information threat. Still, the analyses show that judgement needs to be qualified in order to live up to and resolve the problem of democratic legitimacy. By drawing on Arendt’s writings on political judgement, the critical analysis identifies several contradictions and limitations inherent in the approaches suggested. First, the examination of the premises of EU online counter-radicalization policy shows how policymakers’ use of methods for changing minds are based on expectations of measurable and, ideally, predictable results. On this account, the unorthodox approach of disseminating humorous counter-narratives can encourage self-reflection in individuals who sympathize with extremist causes. But such self-reflection presumes individual agency; laughter, at least the kind of laughter that leads someone to change his mind about something important, cannot be commanded. Second, while it may be true that algorithmically generated messages on social media platforms constitute a fertile ground for bad political thinking, the main preoccupation should not be the individual mental health of internet users currently embraced by securitizing actors. A political judgement is not an individual cognitive state, but must be understood in relation to the intersubjective dimension of speech. Rethinking the referent object in relation to the online information threat, and taking these limitations into account, the dissertation proposes a turn to judgement rooted in public life. This life might be
imagined or factual, but it includes a recognition of our own agency as well as the agency of others.

Contributions

The findings presented as part of this dissertation have methodological, conceptual, and theoretical implications for Security Studies as a whole, and Critical Security Studies in particular, but also for contemporary policymaking in relation to the online information threat. This section outlines the three main contributions made by the articles presented.

The dissertation contributes to Critical Security Studies by suggesting a novel methodological approach to investigating the referent object. The traditional Copenhagen School of securitization theory regards the referent object as a necessarily explicit part of the securitizing act. In other words, it is only by stating that something is under threat that it can be made secure. Yet, as studies drawing on international sociological approaches show, securitization can and does take place even in the absence of explicit speech acts. The dissertation contributes to this body of research by showing how the referent object can be conceived of as an implicit preconception about protection that guides proposed interventions. This conception, in turn, opens up for a different and wider approach to the study of bureaucratic securitization. The Paris School commonly explains securitization with reference to enhanced power for securitizing actors. By turning our attention instead to the referent objects guiding security interventions, the articles presented here bring to light the preconceptions and shared worldview of securitizing actors. Making explicit such implicit points of departure opens up for a critique of the conceptual premises of securitization, in contrast to the more commonplace focus on bureaucratic networks and the reproduction of power within such networks. This change of focus is key in relation to a non-state actor such as the EU Commission, where securitization in relation to the online information threat was initially pursued through knowledge production and the dissemination of ‘best practices’, rather than put into the hands of certain given actors.

Secondly, by pinpointing the limitations of national security in relation to the online information threat, the dissertation outlines a critical argument against suggested methods for security-making within Defence, Intelligence, and Strategic
Studies. The articles underscore how the vision of protecting the sovereign state in cyberspace as a matter of national security – an approach embraced by scholars within Defence and Intelligence Studies – is inherently problematic in connection with non-territorial threats spread through human communication. Similarly, the understanding of security as the protection of a given democratic people as forwarded in current discussions of ‘hybrid threats’ is equally problematic. Highlighting how communication in a democratic context corresponds to the constitutive force of the collective subject in a democracy – the people – it becomes clear that any referent object guiding securitization in a space without given boundaries must accept that ‘the people’ is a self-constituting entity. However we view the problem of online information threats, if, as policymakers suggest, the aim is to ‘protect’ democratic legitimacy, we need a conceptualization of security that takes the agency of the communicating subject into consideration. The remedy, therefore, can never be the insertion of legitimate authority through boundary-drawing strategies such as ‘offensive information operations’, ‘strategic communication’, ‘democratic propaganda’ (Ventre 2016, Paul 2011, Taylor 2002), or the implementation of online filtering services (Demochak and Dombrowski 2014, 98). Rather than serving to ‘protect’ democracy or legitimate authority, such interventions reproduce territorial boundaries in cyberspace with reference to an ungrounded legitimacy. What is more, as is made evident in the empirical analysis, such visions lead to practical problems of implementation. It is not unreasonable to think that the envisaged need for perpetual interventions contributes to the outsourcing of content management to private actors or a turn to experts, thus ironically putting the protection of democratic legitimacy into the hands of the internet industry or communication professionals.

Lastly, by showing how securitization in relation to the online information threat is guided by ideas about protecting human judgement, and by pointing to the limitations and possibilities of this referent object, the dissertation makes conceptual and theoretical contributions both to Security Studies and to contemporary policymaking. By conceptualizing the referent object as human judgement, we can explain many of the unorthodox security interventions proposed in relation to the threat. Understanding security as the protection of judgement throws light on the current turn to humour (RAN 2012) in security-making, but also on the common references to ‘critical thinking’ (Pherson and Mort Ranta 2019, 9), as well as on the myriad ‘online fact-checking services’ that have sprung up in recent times. The theoretical discussion
of political judgement furthermore offers critical arguments against interventions that draw on individual cognitive frameworks of judgement. In recent years, a number of securitizing actors have described security in terms of individual mental fragility. The EU-funded Radicalization Awareness Network, for instance, provides a list of ‘risk factors’ for autistic and mentally ill individuals, arguing that their judgement may be especially compromised in relation to online information (RAN H&SC 2019, 6). Such a psychological understanding of judgement, however, potentially undermines the agency of the democratic subject. In contrast to such views, the Arendtian take on political judgement shows that judgement must be grounded in the intersubjective dimension of speech. Understanding judgement as linked to communicability, this form of judgement straddles the line between the individual and world shared in common with others. Such a conceptualization of the referent object connects security measures for dealing with online information threats into line with the standards for democratic legitimacy.

**Limitations and Future Research**

There are limitations involved in the exploration of a fast-changing field such as security-making in relation to online information threats. This is particularly true with respect to the empirical findings presented in this dissertation. Since the first article was published, the EU has increasingly come to focus on, and work against, the economic drivers behind online information threats, while calling for more technical solutions to the problem and demanding more active involvement of global internet companies. These turns in policymaking, however, point to the relevance of the wider conclusions presented in this dissertation. In particular, they highlight the importance of not understanding the threat narrowly, in terms of intentional messages from foreign actors, but as a wider, and sometimes unintentional, threat to democratic life. In addition, the role of internet companies as securitizing actors, especially the limitations and possibilities of digital technologies, needs more critical scrutiny. This dissertation focuses exclusively on initiatives from securitizing actors, but a logical next step would be to examine the overall potential for democratic action in a cyberspace dominated by powerful internet companies. The fundamental conceptual question of how we should
conceive of online platforms is a pressing one. Are such platforms public infrastructures? Or are they media companies, responsible for content shared by users? Different answers to these questions will lead to different solutions, with divergent implications for questions of both security and democratic politics.

In theoretical terms, some of the limitations of the dissertation are connected with the research process itself: however much one tries, some insights can only come about at the end of a journey. Consequently, a more detailed empirical exploration of contemporary policy, directly drawing on the theoretical discussions about democratic legitimacy, is yet to be undertaken. The question of how to understand democratic legitimacy in relation to security and the online information threat also deserves further scholarly attention. This dissertation shows how claims to protect democracy become an essential part of the meaning of security, and how this change in security-making can be conceptualized by turning to political judgement. Consequently, from the results presented, it should be clear that democratic legitimacy is not only a question for democratic theory or simply a practical problem for security professionals. Instead, it constitutes a key problematic for those seeking to understand security in a democratic society permeated with information and communication technologies. Given that, we need to investigate further the political implications of linking security to democracy, but also to examine what kind of subjects this connection works to produce. In other words, what constitutes the security of democratic judgement, and what constitutes the judgement of security?

References


Taylor, P. M. 2002. ‘Strategic Communications or Democratic Propaganda?’ *Journalism Studies*, 3(3), 437-41.


