Transparency from Space? How Non-Governmental Actors Use Satellite Imagery for Security Governance

Olbrich, Philipp

DOI:
10.33612/diss.119584381

university of groningen

Transparency from Space?

How Non-Governmental Actors Use Satellite Imagery for Security Governance

PhD thesis

to obtain the degree of PhD at the
University of Groningen
on the authority of the
Rector Magnificus Prof. C. Wijmenga
and in accordance with
the decision by the College of Deans.

This thesis will be defended in public on

Monday 2 March 2020 at 9.00 hours

by

Philipp Olbrich

born on 10 August 1987
in Paderborn, Germany

Supervisors

Prof. A.J. Zwitter
Prof. J. Herman

Co-supervisor

Prof. D.U. Shim

Assessment Committee

Prof. J.H. de Wilde
Prof. G.C. van Roozendaal
Prof. D. Nabers
Prof. M.J. van den Hoven

Contents

Part I

Tables

Figures

Acknowledgements

While much of academic work is a rather lonely endeavor, this PhD project certainly was not. Over the four years I have benefitted from and enjoyed many conversations with friends and colleagues about the role of technology in global security, (wild) theoretical approaches to the relation of matter and politics, and the reasons for becoming and, frankly, staying an academic these days. On all of these topics and more my supervisors, Andrej Zwitter and David Shim, have not only led by example but always offered their invaluable insights and guidance for which I am immensely grateful. Early on they motivated me to start writing and present and publish my work in different settings which, I think, was the key to finish in time. They were always interested, knowledgeable and accessible and have certainly become more than my academic supervisors over this period. Moreover, I would like to thank my fantastic colleagues at the Department of International Relations and the Graduate School for the Humanities. In the office, at conferences or simply over coffee or drinks I have learned a lot from you. Before coming to Groningen, Nina Witjes early on shared my interest in space and remote sensing. As a result, she was one of the few who did not need any convincing why this topic was important and interesting. Essentially, our time together at the Austrian Institute for International Affairs laid the foundation for this thesis and how I approach academic research so that she deserves a special thanks. Of course, the foundation of any research project is data. In the course of my studies I was fortunate enough to be able to interview more than 50 informants especially in the U.S. I am grateful for their patience and their willingness to share their knowledge with me. While Groningen might not be the biggest place, it surely feels like one at the beginning. Thanks to Agha, Bin, Cong, Desiree, Eric, Frank, Mustafa, Sandra, Sjoukje, Qi and Yara and all the other outstanding friends and colleagues it does feel like home now. I also would like to take this opportunity to thank my parents for their trust in me as well as my sister Tine, Eva and Wibke. Finally, I want to say thank you to Marina who has always supported me in pursuing this project made personal sacrifices for it and probably knows more about satellites now than she cares for.

Part I

1 Introduction

1.1. Introduction

"Within the past week, unmistakable evidence has established the fact that a series of offensive missile sites is now in preparation on that imprisoned island. The purpose of these bases can be none other than to provide a nuclear strike capability against the Western Hemisphere" (John F. Kennedy Presidential Library 2019). On October 22, 1962, President John F. Kennedy informed the American public and the world about what U.S. spy planes had discovered on Cuba. Until then, only a handful of people were aware of the emerging situation that later became known as the Cuban Missile Crisis. The intense thirteen-day showdown is regularly portrayed as one of the most dangerous moments in human history when the Cold War stand-off between United States and the Soviet Union brought the world to the brink of nuclear destruction (Allison 1971; Dobbs 2008; Parshley 2012). Following the failed U.S.-orchestrated invasion of Cuba one year earlier, the Soviet Union set out to secretly place nuclear-capable missiles on the island. On October 15, 1962, U.S. intelligence took photographs of the ongoing stationing of the weapons from a U-2 reconnaissance aircraft. Based on this visual evidence, the so-called Executive Committee of the National Security Council (EXCOMM) struggled for days to find an appropriate response. After almost a week of weighing the pros and cons of a military response and non-military alternatives, President Kennedy presented the result in his address to the nation: The U.S. would implement a naval quarantine to stop the military buildup on Cuba and, for now, refrain from further military action. Prior to this announcement, neither the American public nor the Soviet leadership were aware that the administration had known about the missile sites less than 150 km off the U.S. mainland. Also, the existence of the U-2 photographs or even the nature of the evidence remained secret. The days following Kennedy's announcement were characterized by uncertainty of each other's motives and capabilities, high-risk confrontations between U.S. and Soviet forces as well as back-channel diplomacy and personal correspondence between Kennedy and Khrushchev. In the end, the Soviet Union agreed to withdraw the missiles in exchange for a public pledge by the U.S. not to invade Cuba and a silent removal its missiles from Turkey. The nuclear catastrophe was averted.

Now, imagine the photographs of the Soviet missiles were not taken by a government spy plane but a commercial satellite and publicized by a non-governmental organization (NGO). Arguably, the administration would not have a chance to deliberate on a public response for almost a week. As the satellite images dominate the headlines, the U.S. Congress, journalists, experts and foreign governments become part of the conversation about the nature of the threat and the right response. More likely than not, at least some of them side with the early opinion of the Joint Chiefs

of Staff calling for a military solution. At the same time, non-governmental analysts might challenge the "unmistakable evidence" Kennedy referred to in his address: Disagreements could concern the readiness, reliability, or strategic importance of the missiles in the context of the overall military balance. Moreover, public opinion turns into an important factor – especially if the next mid-term elections are less than a month away as in 1962. Taken together, the commercial satellite image, at once, empowers new actors to participate in the controversy about the security threat, influences what is considered a proper response and alters the ways in which decisions are produced. Importantly, the scenario does not prescribe whether the Cuban Missile Crisis still comes to a peaceful end or not. However, it illustrates that the technological advancement and commercialization of Earth observation (EO) satellites change security governance. The thesis explores this change.

1.2. Political Promises of Satellite Imagery

The commercialization of satellite imagery is part of a growing interest in space that is driven by decreasing costs in the development and launching of spacecraft, international competition and advanced analytical capabilities (Davenport 2018; Pyle 2019). Instead of launching one custom-made, large government satellite on an expensive rocket, companies launch dozens of small, capable spacecrafts at once with commercial providers. The commercialization of space – which is sometimes dubbed New Space – has attracted 18 billion USD of equity capital investments in more than 400 space companies worldwide since 2009 (Space Angels 2019). EO companies in particular seem to make use of the technological and economic opportunities: More than 60% of the 1,900 satellites in orbit are for remote sensing (Datta 2018). The largest constellation of satellites is currently operated by the private EO company Planet which uses its more than 150 satellites to image Earth's landmass at least once a day. The commercial efforts are complemented by international government programs which continue to provide lower-resolution satellite imagery often free of charge (Borowitz 2017). The value proposition of the EO industry lies in the satellite imagery. Northern Sky Research (2018) estimates that "Earth Observation satellite data and services will represent a $54 billion cumulative opportunity over the next ten years." Such projections build on the assumptions that the growing number of EO satellites drives down imagery prices and lowers entry barriers for organizations without prior experience in remote sensing. The central premise is that there is significant value in the information that can be derived from EO data for a variety of users across industries. Such expectations have given rise to what is called a geospatial revolution (Masback 2015; O'Connell 2017). This revolution assumes that the value of commercial satellite imagery is harnessed by users beyond the traditional government domain. Giving NGOs, journalists, think tanks and universities access to the former intelligence technology allegedly amounts to a power shift in that governments lose parts of their informational sovereignty. The technological expectations fuel the enthusiasm about wide-

ranging political promises: “This avalanche of images will create an unprecedented database of the entire planet, one that can be used to stop forest fires and maybe even wars” (Burningham 2016). In this narrative, commercial satellite imagery expands the reach and efficiency of security governance. It becomes a universal technology for non-governmental actors to monitor and promote global security.

1.3. Overview of the Literature

1.3.1. Studying the Force of Technology

Technology has been afforded great empirical interest in both in International Relations (IR) and Security Studies. In doing so, scholars have repeatedly singled out technologies to examine their implications for the balance of power, the conduct of warfare, governance of security or the risk of conflict. Among others, this includes autonomous weapons, aircraft carriers, artificial intelligence, ballistic missiles, drones, information and communication technologies (ICT), nuclear weapons, robots or quantum computing (Byman 2013; Der Derian 2013; Erickson and Wilson 2006; Hanson 2002; Kroenig 2018; Mettler and Reiter 2013; Owen and Gorwa 2016; Rosenau 2002; Scharre 2018; Singer 2009). Certainly, it is more than justified to devote serious attention to this variety of technologies and their significance for global security. At the same time, the analytical treatment of technology has remained rather stable. The conceptual understanding of technology is largely restricted to instrumental and determinist ideas rendering technology apolitical and exogenous to the analysis (Herrera 2006; McCarthy 2013). The marginalized theoretical examination of technology in security research also becomes manifest in reflections upon the future of Security Studies when scholars single out the development and ramifications of emerging technologies as pivotal empirical and theoretical sites of study (P. Burgess 2014: 39; Carpenter 2016b: 94).

Against this background, the thesis moves beyond instrumental and determinist understandings to point to socio-material presuppositions, interactions and risks in the use of satellite imagery by non-state actors. Taking the force of technology seriously is as consequential as it is counterintuitive. While political leaders accept the importance of technological development, they consider it another tool to own, control and wield power over others. Russian President Vladimir Putin has famously stated that “artificial intelligence is the future not only of Russia but of all mankind” and that “whoever becomes the leader in this sphere will become the ruler of the world” (Gigova 2017). The U.S. Department of Defense (DoD), too, eagerly works on innovative applications for artificial intelligence to retain its dominant position. All the while, “[t]he official DoD position is that machines are tools, not independent agents themselves” (Scharre 2018: 228). Even common parlance suggests that we use technology to achieve specific means: Humans

command matter. However, ignoring the ubiquity and importance of technology and the material environment puts serious limits to understanding political action including security governance:

> *The dissemination and circulation of technoscientific objects (e.g. computers, digital networks, medical drugs), but also phenomena such as El Niño, melting glaciers and polar bears (Passoth 2010), floods, viral epidemics, genetically modified materials, nano-particles, etc. enact our world for the better or the worse. Hence, the social world remains inadequately understood if we conceive agency as the sole power of human action or unintended consequences of rational human choices that govern it* (Passoth, Peuker, and Schillmeier 2012: 3).

With this in mind, one of the challenges the thesis faces, is to develop a meaningful analytical approach that takes into account how human and technological factors interact in non-governmental remote sensing. There is no systematic, decades-old research tradition that flips perspectives and looks at how technologies govern human behavior (Jasanoff 2016). More recently, however, a growing number of scholars have discovered socio-material interactions as a relevant research topic in the study of global security.

The thesis compiles and ties into an emerging research program that it calls socio-material approaches to security (SMAS). SMAS combine a diverse group of scholars that draw on various disciplines including Anthropology, Feminist Studies, (Political) Philosophy, Sociology, and Science and Technology Studies (STS) (Barad 2007; Bennett 2010; Connolly 2013; Coole and Frost 2010; DeLanda 2009; Deleuze and Guattari 1987; Jasanoff 2004a; Latour 2005; Law 2009; Ong and Collier 2005). Yet, they share a common interest in the ways in which technologies shape, enact or govern security practices (Acuto and Curtis 2014; Amicelle, Aradau, and Jeandesboz 2015; e.g. Amoore 2009; Aradau 2010; Bellanova and Duez 2012; Bourne 2016; Bousquet 2014; Leese and Hoijtink 2019; Mayer 2012; McCarthy 2018; Schouten 2013). In spite of their diversity, the thesis identifies three common features that pertain to the study of technology in global security. All contributions to SMAS attribute technologies some degree of material agency, focus on human-material relations within networks and assume those networks are volatile so that most researchers propose empiricist approaches to trace how the networks emerge and are stabilized.

As the commonalities remain rather abstract, there is a large diversity in how individual scholars undertake their research. Frequently, data collection and analysis are portrayed as a form of some kind of "theoretically informed empiricism" (Barry 2013b: 419). Ironically, while SMAS repeatedly remind readers about the importance of detail, description and specificity, there is considerable silence on the specifics of research practice. Put crudely, the underlying argument of SMAS is that a priori specifying methods of data collection and analysis or drawing on explicit

theoretical categories curtail analytical freedoms. The anxiety of forcing data justifies the lack of method. In turn, of course, researchers operate without clear guidance about what data is relevant enough to be included or excluded or how it is interpreted. Accordingly, SMAS-inspired studies at times alienate other security scholars because of their awkward terminology and metaphor-laden descriptions (Bueger 2013). The methodological freedom also leads to charges of arbitrariness and subjectivity (Fine 2002). The first part of the thesis tackles these shortcomings. For doing so, it retains the analytical strengths of SMAS but introduces clear guidelines for data collection and analysis. As a result, the findings but also the socio-material approach to security become more accessible for security scholars of varying traditions.

1.3.2. The Need for a Comprehensive Analysis of Non-Governmental Remote Sensing

The existing literature on non-governmental remote sensing generally falls into two categories characterized by their respective interpretation of its effects. The first and larger category emphasizes the use of satellite imagery by NGOs and think tanks and how this weakens governmental control of information. The second category points to the more unfavorable consequences of how satellite imagery, even in the hands of non-governmental actors, re-reproduces established power structures.

Early debates about the commercialization of satellite imagery revolved around the challenges it brings to U.S. national security (Florini 1988; Baker, O'Connell, and Robertson 2003). However, this has quickly given way to arguments that understand the loss of the governmental monopoly on satellite imagery as an effective power-shift to non-governmental actors including journalists, humanitarians, human rights NGOs, environmental groups and think tanks (Baker, Williamson, and O'Connell 2001; Livingston and Robinson 2003; Dehqanzada and Florini 2000; Wang et al. 2013; Baker and Williamson 2006; Baker and Williamson 2000). As a result, non-governmental agendas appear more prominently in global media and challenge government-controlled narratives on technical and evidentiary grounds rather than moral arguments (Livingston and Robinson 2003; Baker and Williamson 2000). According to this literature, NGOs and other civil society actors use satellite imagery to highlight injustices and security threats where governments remain silent making them "imagery activists" (Baker 2001; Baker, O'Connell, and Robertson 2003). Commercial satellite imagery is used to identify human rights violations and mass atrocities and supports advocacy efforts by corroborating eye-witness accounts or other reports with visual evidence (Levinger 2009; Marx and Goward 2013; Wang et al. 2013). Moreover, scholars illustrate how non-governmental remote sensing supports humanitarian actors in post-conflict or disaster settings (Meier 2014; Meier 2015) or can be applied to monitor and manage environmental security (Kansakar and Hossain 2016; Markowitz 2002). Lastly, others make the case that the advent of commercial satellite imagery empowers non-state actors to reveal

security-relevant information such as the operational status of nuclear programs or clandestine drone programs (Aday and Livingston 2009; Laygo et al. 2012; Livingston 2015). Overall, the usage of commercial satellite imagery by NGOs and think tanks are consistently expected to increase over time. Therefore, governments continue to lose control over information so that "[g]reater transparency in international affairs seems likely, if not inevitable" (Livingston and Robinson 2003: 21; see also Olbrich 2019c). Overall, this group of scholars comes to rather positive assessments of non-governmental remote sensing by highlighting the successes and benefits of particular projects. In doing so, it joins a number of policy experts, business analysts and space enthusiasts that celebrate the beneficial and revolutionary effects of non-governmental remote sensing (Burningham 2016; Clem 2016; Hutson 2011; Jablonsky 2018; Larsson 2016; Marshall 2014; Masback 2015; O'Connell 2017; Tarr and Marshall 2017).

More critical accounts of non-governmental remote sensing are less frequent and argue that although NGOs and think tanks now have access to satellite imagery, they commonly remain within statist discourses. This qualifies assertions about a power-shift from governments to non-state actors but focuses on the reproduction of existing power structures. First of all, critical scholars disagree with assertions that non-governmental actors can use satellite imagery to effectively oppose governments on factual rather than moral grounds. To support this, they point to the necessity of interpretation of satellite imagery – frequently citing the example of Colin Powell's presentation of satellite imagery in the UN Security Council to prove the existence of weapons of mass destruction in the run-up to the Iraq War (Campbell 2007; Shim 2013; Olbrich and Witjes 2015). Others warn to not overstate the power-shift given the remaining government influence, limited resources, selective incentives for NGOs to publicize satellite imagery (Litfin 2002; Perkins and Dodge 2009; Witjes and Olbrich 2017). Finally, some scholars argue that non-governmental remote sensing rarely challenges dominant government discourse but is rather complicit in reaffirming Western-centric policies and reinforcing the status quo (Herscher 2014; C. Hong 2013; Parks 2009; Rothe and Shim 2018; Shim 2014).

Albeit researchers of the respective categories disagree on some substantial issues, they share two major shortcomings. First, the existing academic literature largely ignores the role of technology in shaping the emerging practice of non-governmental remote sensing (for an exception see Rothe 2017). Instead, they fall back on established technological understandings. Mostly, commercial satellite imagery is taken as a new instrument at the disposal of non-governmental actors to pursue their interests. Determinist understandings relate the commercialization of satellite imagery to existing discourses about the growing impact of ICT and growing international transparency. In essence, however, technology remains outside of the political analysis and does not impact the researchers' conclusions whether commercial satellite

imagery challenges or reproduces existing power structures. Second, previous studies have relied on a rather thin empirical foundation. Most of the time, they use anecdotal evidence and prominent pilot projects of large NGOs to make rather broad statements about non-governmental remote sensing as a whole. While this serves the purpose of providing and illustrating initial insights into the practice of non-governmental remote sensing the validity is limited due to the narrow scope. Research is restricted to specific actors, areas of application and points in time. It carries the risk of impermissibly generalizing from idiosyncratic incidents. This is exacerbated by the fact that non-governmental remote sensing is a very dynamic field given that it deals with an emerging technology (cf. Olbrich 2019c). The ongoing technological development, very diverse technical know-how and open-ended experimentation undermine findings based on individual projects. Even if more than one case is included in the sample, the literature is frequently limited to desk research. Again, this serves as a useful starting point. However, analyses are restricted to reports and documents the non-governmental actors deemed worthy of making public. As such, any analysis remains blind to the constitutive networks, practices and technologies behind official imagery reports and publications.

Taken together, a number of caveats apply to previous research on the use of commercial satellite imagery by non-state actors and leaves open questions (Notely and Webb-Gannon 2016). This results in a limited authority to make a comprehensive, empirically grounded assessment of non-governmental remote sensing as a security practice. The thesis addresses these shortcomings and presents a critical examination of non-governmental remote sensing as a security practice based on a comprehensive empirical foundation.

1.4. Purpose and Goals of the Thesis

1.4.1. Outline of Research Questions

As has been shown above, the commercialization of satellite imagery has produced a number of remarkable pilot projects by NGOs, think tanks and the media. The majority of scholars, companies, commentators and journalists compiles an impressive record of how satellite imagery can be used to effectively monitor deforestation, human rights violations and weapons programs. They argue that this increases global transparency and produces information to review policies and hold governments and other powerful stakeholders accountable. Collecting positive cases of non-governmental remote sensing serves the purpose of informing the public about its benefits and practitioners about ongoing operational frustrations. However, these accounts tend to be rather repetitive by drawing on the same pilot projects. The significance of contextual factors further complicates transferring findings to other areas of application or filtering out common practices. Most importantly, the focus on pilot projects, operational practices and effects neglects relevant aspects including underlying assumptions of non-governmental remote sensing, the

socio-material potential and constraints as well as more abstract but lasting risks and consequences.

Against this background, the thesis rather adds to the second group of researchers who is skeptical towards the linear power-shift from government to non-governmental actors. It seeks to complement overly positive assessments that emphasize operational benefits over structural risks. For this purpose, the thesis produces a comprehensive empirical base and moves beyond the widespread approach of singling out individual projects of non-governmental remote sensing to draw wide-ranging conclusions. Instead, it engages a variety of documents such as satellite imagery analyses, regulations, statistics and technical reports as well as commercial satellite imagery experts. Multiple interview series include former government imagery analysts, NGOs and think tanks from various sectors, satellite operators, government officials and scholars. Building on such a broad empirical base, it becomes possible to more comprehensively explore non-governmental remote sensing as an emerging security practice. Moreover, introducing the role of technology into the analytics points towards how non-governmental actors react to the socio-material potentials and constraints of commercial satellite imagery. As a result, the following chapters focus on how NGOs and think tanks address insecurity with commercial satellite imagery, how they differ from each other and what this means for global security beyond operational aspects. More specifically, the research questions can be summarized as follows:

1) How do human and technological factors interact in non-governmental remote sensing to credibly problematize and create security threats?
2) What types of non-governmental remote sensing have emerged in terms of users, practices, goals and issue areas?
3) What kind of transparency is produced by non-governmental remote sensing and what are the security risks and implications?

The first research question looks at the working level of non-governmental actors that integrate satellite imagery into their operations. On the one hand, it challenges the taken-for-granted human control over how security threats are constructed via commercial satellite imagery. On the other hand, it examines how security threats appear valid and credible in light of the socio-material interaction. The second research question moves up one level of abstraction to look at the coordination of actors, technologies and practices and how this translates into distinct, stabilized forms of non-governmental remote sensing. Environmental and human rights NGOs probably diverge on problem sets, priorities and technological know-how. The same applies to security think tanks and humanitarian actors. In order to account for the differences, the research question examines how NGOs and think tanks respond to the potentials and constraints of

commercial satellite imagery. The final research question looks at the most abstract level to examine the broader consequences and risks of non-governmental remote sensing. For doing so, the thesis re-constructs the understanding of transparency associated with non-governmental remote sensing. Based on this, it complements assertions about the benefits of global transparency with a view on the risks and potentially unintended consequences.

1.4.2. Principal Findings of the Thesis

In answering these research questions, the thesis adds to conceptual approaches to the role of technology in security governance. Moreover, it complements and revises large parts of the existing scholarship on non-governmental remote sensing. Two central contributions are highlighted here.

A Structured Approach for Socio-Material Analysis of Security

The thesis translates into research practice the notion of many SMAS to pursue a "theoretically informed empiricism" (Barry 2013b: 419). Hitherto, security research into the role of matter and technology is characterized by theoretical and methodological flexibility. The insistence on data-driven approaches lacks detailed descriptions about data collection and analysis. This obscures how those studies have arrived at their findings and it makes SMAS-inspired research difficult to access for other security scholars. Overall, this hampers efforts to appropriately establish the study of technology in IR and Security Studies. In order to address this shortcoming, the thesis both introduces a conceptual framework and draws on grounded theory methods to organize data collection and analysis.

Working with a conceptual framework is controversial among SMAS scholars because they fear that theoretical concepts predetermine the empirical analysis (Barry 2013b; see also Bueger 2013; Bueger 2014). Cognizant of these risks, the thesis develops a conceptual framework that both guides research practice but remains sensitive to the empirical material at hand. As such, it assembles theoretical reminders and makes explicit what to focus on in the empirical investigation. The framework pre-structures data collection and analysis. In doing so, it reins in excessive interpretations that are difficult to comprehend after the fact. Introducing ex-ante theoretical notions to inform the empirical analysis does not prescribe empirical findings or seek to squeeze empirical data into a conceptual corset. Instead, the conceptual framework increases coherence and accessibility for other scholars because it makes explicit the theoretical assumptions and empirical foci that otherwise remain hidden. Going further, the thesis draws on grounded theory methods to guide data collection and analysis. Originally developed in the 1960s (Glaser and Strauss 1967), grounded theory has become an established qualitative approach across the humanities and social sciences. The thesis argues that it is compatible with many

requirements of SMAS including an empirical sensitivity, data-driven theorizing and acceptance of all kinds of data sources including interviews, documents, imagery etc. At the same time, grounded theory conveniently offers solutions to recurring questions related to SMAS concerning data collection and analysis. The notions of open and focused coding as well as theoretical saturation and constant comparison operationalize the kind of interpretive but theory-guided approach many SMAS scholars call for.

Overall, the conceptual part of the thesis does not aim for classic theoretical development. Rather it offers a pragmatist perspective on the diversity of SMAS. It extracts central conceptual notions in order to devise research-practical guidelines for the study of technology in security governance. As a result, the approach is particularly suitable for exploring an emerging technology-driven security practice such as non-governmental remote sensing.

The Socio-Materiality of Non-Governmental Remote Sensing

On an empirical level, the thesis challenges and amends the predominantly positive narrative of the commercialization of satellite imagery. Most importantly, highlighting the force of satellite technology in non-governmental remote sensing reveals a number of qualifications for the ways in which NGOs and think tanks make use of satellite imagery, the coordination of actors and practice, and consequences for global security. Adopting a socio-material perspective shows the limits of human control over which and how security threats are addressed and what kind of transparency is pursued.

The thesis traces the force of technology throughout the process of satellite imagery analysis, i.e. during imagery acquisition, interpretation and reporting. The thesis specifies the limits of imagery acquisition with respect to the orbits of satellites, legal regulations, sensors, market conditions and the power context. Effectively, it shows the techno-political limits to the promise of global transparency. In the non-governmental domain, the socio-material conditions that produce commercial satellite imagery amount to the "the law of what can be said" (Foucault 1972: 129). The available imagery constrains the space of possible security problematizations. Once imagery is acquired, the interpretation also constitutes a socio-material process. This means that security threats are largely limited to material proxies; they are limited to material manifestations on the ground. Despite assertions of journalists and policymakers you cannot see a security threat. Instead, analysts define material proxies so that untended fields become indicators for forced displacement or vehicle activity a stand-in for suspicious behavior at a nuclear site. They translate matter into security threats. Immaterial threats and structural violence are invisible to non-governmental remote sensing. Moreover, the reduction to material proxies neglects important contextual factors and, thereby, risks simplifying or even misrepresenting security threats. All the

while, it becomes difficult for the observed to discursively escape the hierarchy of material evidence. In essence, the material and visual dimensions of non-governmental remote sensing render security problematizations as intuitively legitimate and credible.

The potentials and constraints of satellite technology also take effect in defining different modes of non-governmental remote sensing. These modes differentiate along two dimensions that are characterized by the goals of non-governmental actors as well as if they actualize the imagery or data potential of remote sensing. Building on the diversity of empirical data, the thesis draws up a typology of four distinct ways how non-governmental actors integrate commercial satellite imagery into their operations. Security think tanks often use satellite imagery to monitor known security threats and produce public information. Human rights NGOs rather seek to advocate for human rights and create a sense of accountability. Both, however, rely on the visual dimension of a handful of satellite images to convince the public and policymakers of the urgency and credibility of insecurities. Humanitarian actors and environmental groups, on the other hand, usually cover large areas of interests that are affected by disasters or environmental degradation. As a result, they tend to actualize the data potential of remote sensing as they are interested in the geographic distribution of accessible roads, affected populations, illegal logging or the extent of oil spillage. Although remote sensing presents its users with the same set of socio-material potentials and constraints, the variation is a result of how non-governmental actors react to and actualize them.

Finally, the thesis challenges prevalent ideas about the effects of transparency non-governmental remote sensing is promised to bring about. Transparency is declared a virtue by a large coalition of scholars, practitioners, NGOs and policymakers and any additional contribution should be commended. Somewhat counterintuitively, then, the thesis argues that non-governmental remote sensing leads to forced transparency. NGOs, think tanks and satellite imagery analysts understand transparency as the amount of publicly available information about a security threat. It is a quantitative measure. Taken together, transparency is idealized as a quantifiable virtue that should be maximized. The relatively easy access and global reach of remote sensing allows small groups of actors to pursue this goal on a broad scale. In turn, a lack of transparency is rendered suspicious so that non-governmental users feel justified to force transparency if the required information is not voluntarily provided. Effectively, this blurs the lines between transparency and surveillance. This calls for a reassessment of the consequences of non-governmental remote sensing that in addition to the benefits of transparency examines the risks and implications of the maximization of transparency. Among other things, the thesis examines how commercial satellite imagery contributes to risks that reinforce remote governance practices which disproportionally affect non-Western countries, draws the observers into the security situations and complicates

diplomatic crisis management – as the alternative scenario about the Cuban Missile Crisis illustrates.

1.5. Structure of the Thesis

The thesis is divided into two parts. Part I discusses theoretical considerations concerning the study of technology in security governance. Following this introduction, chapter 2 offers a reading of how the classic security governance literature has analytically treated the impact of technology. While security governance decidedly addresses the growing importance of non-traditional security actors and threats, technology remains exogenous to the analysis. From there, the chapter turns to SMAS to conceptually grasp how material devices affect security practices. It organizes the diverse literature to extract three common features that commonly introduce matter to political analysis. Building on this, chapter 3 develops the conceptual framework of the thesis to address the considerable interpretive flexibility and at times peculiar theorizing of SMAS. The framework seeks to guide the subsequent analysis without imposing an artificial rigidity. For doing so, it introduces the conceptual notions of problematization, stabilization and durable effects. Each of them highlights the respective role of technology during the construction of security threats, the emergence of stabilized assemblages of actors and practices, and the consequences of technologized security governance. Chapter 4 presents the origins and foundational concepts of grounded theory. It outlines how grounded theory methods can usefully structure research practice. This addresses the silence of other socio-material studies that remain silent on this issue. For this purpose, the chapter offers clear guidelines for the collection and analysis of empirical data in accordance with the conceptual framework.

Part II of the thesis explores non-governmental remote sensing as an emerging security practice. In doing so, each of the three empirical chapters incrementally raises the level of abstraction. Chapter 5 shows how security threats are co-produced by both social and material factors. It follows the established process of satellite imagery analysis and reveals how technological potentials and constraints become relevant during imagery acquisition, interpretation and dissemination. On a higher level, Chapter 6 develops a typology of four distinct modes of non-governmental remote sensing. Depending on the goals and technological choices of NGOs and think tanks, different practices have stabilized. After all, satellite technology does not determine but co-determine the manifestation of emerging security practices. Chapter 7 looks at the risks and implications of non-governmental remote sensing at the level of global security. It demonstrates how commercial satellite imagery gives rise to a particular kind of forced transparency that comes close to surveillance. Starting from there, it discusses a number of risks and implications that are neglected by large parts of the literature on non-governmental remote

sensing. The concluding Chapter 8 summarizes the findings of the thesis, considers its limitations and outlines avenues for further research.

1.6. Conclusion

Of course, the alternative scenario of the Cuban Missile Crisis is highly hypothetical. Being aware of the technological potential of non-governmental remote sensing, the Soviet Union arguably would have included this fact into its calculations when making the decision whether to deploy missiles to Cuba. Nevertheless, it illustrates how the commercialization of satellite imagery affects the foundation of global security. Hitherto large parts of the literature have highlighted the benefits of granting NGOs, think tanks and journalists access to satellite imagery to promote human rights and security. The thesis moves beyond collecting successful and problematic uses of EO data by non-state actors. Instead, it builds a broad and diverse empirical base to dare a more critical examination of non-governmental remote sensing as an emerging security practice.

This contributes to growing scholarship on the role of technology in security governance. Socio-material approaches have helped to highlight the expanding role and importance of technological development for security. However, the diversity of the research program and its – at times – theoretical eccentricity have made it difficult for other security scholars to engage their approaches and findings. By offering a condensed reading of SMAS, developing a conceptual framework and introducing clear guidelines of data collection and analysis, the thesis seeks to remove barriers and to facilitate a dialogue about the security-technology nexus across research programs. On a practical level, the socio-material analysis seeks to further thinking about practices and effects of non-governmental remote sensing. Ongoing debates about operational uses of satellite imagery can only benefit from a growing awareness for the hidden material potentials and constraints of satellite technology. Without ignoring the benefits of transparency for security, practitioners of non-governmental remote sensing should consider the accompanying risks and implications and forcing transparency.

2 Technology in Security Governance

2.1. Introduction

Non-governmental remote sensing of security threats is a form of security governance that has technology at its center. Against this background, the chapter assesses the current state of research concerning theoretical approaches to the nexus of security governance and technology. First, the more classic security governance literature in International Relations (IR) is reviewed in light of its analytical treatment of technology. This helps to delineate the underlying understanding of security and isolate recurring central themes. By and large, the review reveals a conceptual neglect of technology. While classic security governance considers technology as a driver, tool or context of politics, it does not integrate it into the political analysis. Second, the chapter turns to socio-material approaches to security (SMAS). They introduce a theoretical sensibility for technology that allows investigations for its impact on practices, actors, norms and goals. However, their focus on micropolitics, everyday practices and empiricism complicates theory-led investigations of security governance. The structured review of the hitherto scattered literatures on the role of technology in security governance lay the foundation for developing a more consolidated conceptual framework (see chapter 3).

The chapter suggests a reading of the security governance literature that accounts for its origins in the wider governance debate. Security governance entered the scene as an alternative approach to then-dominant theories of International Relations to conceptually address newly emerging threats, the re-definition of security, and the proliferation of relevant actors in the wake of the Cold War. Moreover, three core themes of security governance are identified. Presenting research on actors, coordination and consequences of governance serves as a starting point to discusses the analytical neglect of technology in the classic security governance literature. Then, the chapter turns to early attempts to introduce a technological sensitivity into International Relations. Going further, three common features of the growing research interest in socio-material approaches to security are outlined. They introduce the notion of material agency, focus on relationality and a call for descriptive empiricism to account for the role of technology in security governance. The chapter concludes, however, that radically opening the definition of agency and replacing analytical categories with empiricism entails particular complications for theorizing and researching technologized security governance.

2.2. A Changing Security Environment: The Widening and Deepening of Security

Global governance and its security variant have become a staple in International Relations scholarship. The concept gained traction in the aftermath of the Cold War and especially since

1995 when the Commission on Global Governance released its final report, defining global governance as

> *"the sum of the many ways individuals and institutions, public and private, manage their common affairs. It is a continuing process through which conflicting or diverse interests may be accommodated and co-operative action may be taken. It includes formal institutions and regimes empowered to enforce compliance, as well as informal arrangements that people and institutions either have agreed to or perceive to be in their interest"* (Commission on Global Governance 1995: 2).

The thematic focus and three-year efforts of the UN-backed commission illustrate that practical as well as conceptual debates about the content of governance were and are shaped by a constant back and forth between academic and policy circles (e.g. Weiss 2013a; Weiss and Wilkinson 2015; Hänggi 2005). Around the same time, Rosenau and Czempiel's (1992) seminal volume *Governance without Government: Order and Change in World Politics* set the tone for the ensuing theoretical debate. Due to its appeal in academia and policy, global governance has been ascribed a "near-celebrity status" (Barnett & Duvall 2005: 1) and has become a regular part of IR syllabi, academic journals, government strategies, international conferences, policy initiatives and institutions.

From an IR theory perspective, the disruption of the bipolar system after the demise of the Soviet Union made room for questioning central assumptions underlying largely structural theories of security and international affairs (D. D. Avant, Finnemore, and Sell 2010b: 4; see also Barnett and Duvall 2005: 5).[1] IR scholarship struggled to account for varying empirical phenomena such as increases in the number of NGOs and corporations that were playing an international role, collective regulation of environmental problems, technological advances that impacted warfare and communication, an ongoing European integration or multi-variate economic interdependence. More generally, transborder problems took center stage that could not be handled by individual states but required collective coordination and action among various types of actors (Weiss & Wilkinson 2015: 391). In the security realm, the often-cited monopoly on the legitimate use of force as the exclusive hallmark of the state came into question when private actors from rebel groups and terrorist organizations to private military companies created a "market for force" starting in the 1990s (Avant 2005: 253). In light of these changes, the security governance debate takes the end of the Cold War as a significant breaking point from "traditional security analyses" which focus on the state as the central actor and its actions within the military dimension as the locus of (in)security. Instead, non-traditional security issues or so-called new

[1] While the end of the Cold War was an incisive moment, there were earlier calls in IR scholarship for a widening and deepening of security as a concept starting in the 1980s (cf. Buzan & Hansen 2009).

threats were proliferating at that time which required new analytical approaches and a modification of security concepts (Hänggi 2005: 5). In short, the global governance terminology and its variants are a child of the 1990s and contemporary discourse and analysis of empirical phenomena that were assessed as radically different from the Cold War times.

The common thread in the governance literature that world politics experienced various changes at that time is differently labeled and accentuated as globalization, economic interdependence, privatization, technological development, revolution in military affairs, the burgeoning of NGOs or the marketization of violence among other things. A combination of these developments is thought to have undermined the capacities of the nation-state to cope with global problems in substantial ways:[2] In the economic area, the largely unrestrained movement of capital and labor exacerbates its ability of taxation. Similarly, states are integrated into various collective security arrangements, and international bodies. The United Nations (UN) or NATO have established rules on the legitimate use and conduct of military force. In both areas, this calls for international coordination to set common rules and norms which effectively requires to compromise and find common ground as it shifts governing beyond the nation-state. Of course, globalization as an empirical phenomenon is not unprecedented and understanding the actions of rebel groups, conflicts over pollution or food insecurity as "new" threats is a debatable terminology. However, Mary Kaldor and Joseph Stiglitz (2013: 2-4) argue that globalization and its consequences only intensified, became visible and controversial after the Cold War as the dominant analytic frame of a bipolar security system faded and gave way for global governance to enter the scene. So, there is a shift in the understanding of security as military protection against an attack by another state towards a range of new international threats such as terrorism, human rights violations, famines, pandemics, financial crises, climate change and the proliferation of weapons of mass destruction. In an even more greater historical context, John Ikenberry (2013) explains the emergence of security governance as a diversification of the global security environment over the past roughly 150 years. It evolved from concepts of military defense in the nineteenth century to Cold War national security to more comprehensive understandings such as human security in the twenty-first century that embraces a more diverse set of security issues (Ikenberry 2013: 97).

This diversification of perceived security threats or increasingly varied issues that are securitized can be grasped with the notions of a widening and deepening of security (cf. Buzan & Hansen 2009: 136). On the one hand, the widening of security refers to the expansion of the concept beyond the military arena to include environmental, societal, economic and political sectors as

[2] Especially in the study of security governance in the European Union, this has implications for the conceptualization of sovereignty as it leads to the ideal-type of the post-Westphalian state which struggles with the control of flows of people, goods and ideas into its territory and is more receptive to mutual governance agreements and the force of international law (e.g. Sperling 2014b: 101).

relevant security arenas. In this sense, discussions about the usefulness of the effective securitization of non-military aspects or the dissolving of the internal/external distinction can be understood as pertaining to this discourse as well (see also Hänggi 2005: 6). On the other hand, deepening points to a multiplication of referent objects that not only includes the nation-state but also the individual, regional and international level. This is consistent with the preceding discussion: For example, weakened government institutions are limited to particular geographic areas within a so-called failed state or environmental insecurity affects individuals and communities to different extents. In essence, while there are varying degrees of how wide and deep security is actually conceptualized in the literature, scholars of security governance generally challenge narrowly-focused notions of military state-centrism and highlight the multiple faces of security challenges and referent objects.

While the widening and deepening of security has been identified as one of the driving forces of global security governance, it is also the reason for its complexities, difficulties and deficiencies. In particular, this is attributed to "the intertwining of global economic flows and the politics of everyday security and peace" (Aas 2012: 235; see also Branovic and Chojnacki 2011). Along those lines, security analyses cannot be limited to one special type of international actor or the military dimension but start from the assumption of complex nets of relations among the variously involved actors including the state, advocacy groups, international organizations, medical and humanitarian organizations, think tanks, charities, financial institutions, and so on.

What does this mean for the concept of security in governance approaches? Although security governance scholars rarely position themselves clearly in this respect, it is argued here, that this approach is compatible with an empirical understanding of security as "essentially contested concept" (see e.g., Buzan 1991). The approach embraces Baldwin's (1997: 12) critique that this definition does not once and for all resolve conceptual contradictions. Instead, it turns the attention to the empirical analysis of by whom and how security is negotiated, constituted and what it does. In short, it calls upon the analyst to look at the politics of security. Also, this does not mean that other central concepts such as peace or the state are less contested or have somehow produced a general consensus among scholars of IR. However, in an analysis of security governance, the understanding of security emerges out of the relations among the varying actors and the specific situation. Moreover, engaging security in this way opens interesting points of contact of the security governance literature with Critical Security Studies whose succinct defining

feature which sets it "apart from the mainstream is the consensus that security is – or should be – an 'essentially contested concept'" (Schouten 2014: 26).[3]

2.3. Accounting for 'New' (In)securities in Theory and Practice

The widening and deepening of security in co-occurrence with globalization entail various challenges for IR scholarship. Notions of new or emerging threats, human security (UNDP 1994; Paris 2001), "new wars" (Kaldor 1999), climate change and environmental insecurity (Mathews 1989), development and humanitarian action (Weiss 2013b; Duffield 2001), or the further institutionalization of NATO, the UN and European Union (e.g. Kirchner and Dominguez 2014; Sperling 2014b; Christou et al. 2010; Webber et al. 2004; Börzel 2010; Lepgold 1998; Miller 1999) pose serious questions. How to account for the growing international role played by non-state actors? What are the implications for conceptions of sovereignty and the state? How are differing norms and interests accommodated? Are power-shifts related to these developments and who benefits from them? Why and how is cooperation initiated at certain points of time and then maintained or given up? What is "good" governance?

Early accounts present security governance not only as a flexible way to analytically get a hold of these questions but, at times, also as a practical necessity that serves the demand of governance at the sub-national, regional and global level (cf. Barnett and Duvall 2005; Rosenau 1992). Many scholars identify the crux as the proliferation of transborder problems, such as terrorism, natural disasters or weak states, that are impossible to tackle by individual governments; the ensuing erosion of the state's monopoly of violence creates the need for greater coordination and cooperation (Held & Young 2013: 371).

In fact, the urge for theorizing how to account for new insecurities partly "emerges out of a frustration with parsimony and a determination to embrace a wider set of causes" (Sinclair 2012: 69). More specifically, Whitman (2007: 101) identifies two central theoretical concerns:

> *"The first is 'uncovering' the information relationships and norms which underpin global order, arising in part from the belief that 'international anarchy' (the absence of an overarching world government) is not a vacuum. The second is the extent to which some combination of state and non-state actors […] can in their totality suffice to ensure that managing and controlling mechanisms are in place for all of the world's more important dynamics."*

[3] More extensively, Browning & McDonald (2011) identify three central themes that unify Critical Security Studies which are a (1) common critique of realist, state-centric approaches; and more importantly, (2) an interest in the function of (representations of) security in terms of legitimating actors, defining groups or enabling certain policies as well as (3) a preoccupation with the ethics of security as to what constitutes progress in the conception and practice of security.

However, despite the overarching narrative of security governance to fill an analytical and practical gap in the post-Cold War void, its recognition and significance in IR theorizing is limited. It merely makes selective appearances in theory textbooks of the discipline or Security Studies, respectively. A closer look at potential reasons for this are helpful in identifying ambivalences, shortcomings and narratives connected to the concept.

First, security governance is often applied or (mis)understood as a functional, problem-solving approach that attempts to identify 'real-world' processes and structures that determine how security is provided and monitored in a given situation (Bryden 2006: 5-6; Hänggi 2005: 7). This "problem-solving bias" (Mayntz 2009) implicates that involved actors are genuinely interested in and working towards the solution of societal problems. Therefore, it dismisses certain kinds of questions that more critically engage matters of power, motive and authority. Arguably, this development is rooted in the close entanglement of academic and policy circles working with the concept. Writing on the privatization of security, Leander (2010b: 202) notes that scholarly work is – different from and perhaps uncommon for other disciplines – partly formulated in "dialogue with those engaged in the practice who discover, document and denounce the sector." However, recent work has started to question the instrumental and problem-solving understanding of security governance. Instead, there are attempts to turn towards the ambivalences within security governance, open up space for alternative questions and tackle the underlying power structures to make the concept more accessible for Critical Security Studies (see esp. Ehrhart, Hegemann, and Kahl 2014b).

Second, security governance does not come with a coherent and agreed-upon set of assumptions and propositions but largely remains pre-theoretical (Sperling 2014a; Sperling and Webber 2014).[4] In fact, security governance is understood as a way to analyze both processes and systems and, hence, "entails an implicit and sometimes explicit importation of theoretical premises (e.g. on institutions and norms) but makes no significant stand-alone theoretical claims" (Sperling and Webber 2014: 129). Accordingly, it can be employed as a useful analytical tool or "heuristic" to make sense of international politics, but it lacks "prescriptive power" to make normative claims about the future (Weiss 2013a: 42). Despite its conceptual flexibility, though, it is often reduced to few empirical foci and equated with European-centered security research on international institutions (Wilkinson 2002). To be sure, similar to research in global governance, international organizations do constitute regular focal points of analysis (e.g. Weiss 2012; Barnett and Finnemore 2004). Also, the European Union (EU) is often made use of as an exemplary case of

[4] While the pre-theoretical status here is deemed a strength in terms of analytical flexibility to account for various empirical phenomena, there are also attempts to formulate a more coherent security governance approach (e.g. Christou et al. 2010).

security governance and its different facets as it can represent both an actor as well as a system of coordination (e.g. Sperling and Webber 2014; Börzel 2010; Schroeder 2011; Christou et al. 2010; Webber et al. 2004; Kirchner and Sperling 2007; Mérand, Hofmann, and Irondelle 2011). However, it would be shortsighted to reduce security governance to EU security studies. There is an increasingly diverse set of publications that deal among other things with transnational governance from a postcolonial perspective (Hönke and Müller 2012), peacekeeping and peacebuilding (Hänggi 2005; Diehl 2000), security logics and governance in failed states (Branovic and Chojnacki 2011; Risse 2012), the role of private security and military companies (Leander and van Munster 2007; Abrahamsen and Williams 2011; D. D. Avant 2016; D. D. Avant 2005), violence and organized crime (Friesendorf 2007a; Friesendorf 2007b; Jakobi and Wolf 2013), or the governance of technological systems (Allenby 2011; Rappert and Croft 2007).

Lastly, a substantial share of the literature has a somewhat positive or favorable view towards (security) governance which to a certain degree can be traced back to its problem-solving bias mentioned above: Governance is often benignly framed because it is seen as a functional way forward for state and non-state actors alike to tackle mutual problems and work towards common goals (Barnett & Duvall 2005). This does not mean that such research is naïve or completely ignorant of negative side effects or unintended consequences. However, the establishment of global rule-making and norms are portrayed as a preferred solution to transnational problems (e.g. Kaldor and Stiglitz 2013: 11). In this spirit, security governance is perceived as "a good thing" although it still needs some changes and improvements. For example, in accordance with the narrative outlined above, Kaldor (2013) acknowledges the changing face of insecurities that has emerged after the end of the Cold War and the erosion of the nation-state's capacity to monopolize violence.[5] Affirming the positive take on multi-actor governance, she suggests a return to the eroding Weberian notions in the form of governance structures that "reestablish a monopoly of legitimate violence" (Kaldor 2013: 128) through the inclusion of multiple state, non-state and civil society actors. Taken together, the positive perception of governance is furthered by a normatively loaded language that heralds cooperation and the provision of public goods. This also holds for the definition of the Commission on Global Governance introduced above that speaks of the accommodation of diverse interests and cooperative action (Commission on Global

[5] Kaldor (2013: 117-127) illustrates the need for a restructuring of global security governance based on three observations in how "contemporary forms of organized violence" (Kaldor 2013: 120) are different from interstate war. First, civilians have become the main victims in that they are either directly targeted by militarized groups or that counter-terrorism tactics, e.g. drone usage, effectively kill more civilians than so-called combatants. Second, the privatization of violence highlights the involvement of non-state actors in harmful actions including paramilitary groups, mercenaries or (voluntary) self-defense forces which effectively are more difficult to monitor and sanction. Third, organized crime is increasingly entangled with political violence in that it profits from social and political instability in the form of illicit trade, looting, hostage-taking, extortion or other acts of transnational crime.

Governance 1995: 2). Such normative assumptions are at odds with large shares of research in IR. In fact, cooperation itself cannot only be a mechanism to achieve dreadful ends, but what appears as cooperation might as well be undergirded by hidden structures of power, exploitation and domination (D. D. Avant, Finnemore, and Sell 2010b: 7-8).[6] As a consequence, while the introduction of certain security governance structures might be sound policy advice in some situations, it is not a "good thing" per se.

2.4. Central Themes of Security Governance

After outlining the narrative of the widening and deepening of security that governance approaches are thought to account for, the following part attempts to identify common themes within the seminal literature and authors on (security) governance.[7] The emergence of such prevalent themes is taken as a result of certain moves of demarcation that are driven by post-Cold War observations of an increasing role of non-state actors, a broadening security agenda and the eroding state monopoly on legitimate violence. For reasons of pragmatism, brevity and coherence, the number of selected publications to be discussed in more detail is limited. Indeed, the list could be supplemented by additional titles and authors that have gained authority in the academic debate on security governance (e.g. Kirchner and Sperling 2007; Slaughter 2004; Bevir and Hall 2014; D. D. Avant 2005). In any case, such a consolidation comes with particular downsides as it might obscure or underrepresent the importance of certain aspects of governance research. However, carving out broad categories allows for a structured discussion of classic security governance literature and creates reference points for later discussions.

In one of the founding governance texts, James Rosenau opens the often-cited edited volume with his chapter *Governance, Order, and Change in World Politics*. Echoing many co-contributors, he stresses the "who" of governance. Because if the approach stands to characterize a rule-making system that is different from traditional governments, then which actors are responsible for making and implementing such rules (Rosenau 1992: 1)? This move of delineating governance against an ideal-typical understanding of government has remained quite typical due to the common narrative of an eroding authority of the state or a shift of governing functions from governments towards new loci of power. Effectively, the "who" is a variegated constellation of actors that comes to an understanding of shared goals and that constitutes new systems of rule

[6] For a detailed discussion of the hidden disregard and the re-introduction of power into analyses of global governance see Barnett & Duvall (2005).

[7] Ehrhart et al. (2014b) follow a similar approach in identifying essential characteristics of security governance in what they call prerequisites, structures and consequences. Our approaches depart when in a next step they formulate "critical questions" corresponding to each of those categories to render security governance into a "critical tool." One of the purposes of this chapter is rather to show the development of the security governance literature towards more critical understandings of security. Consequently, their valuable contribution to security governance is a testament of this tendency and becomes part of the present analysis.

without being backed by formal authority or an elaborate executive branch to enforce such rules (Rosenau 1992: 4). This relocation of authority from intra-government hierarchical relations towards supra- and subnational entities elicits two further questions: How are governance arrangements initiated? And, how do the different actors communicate with and coordinate each other (Rosenau 1992: 2-3)? Because no matter the maturity or development of a given system, certain functions always need to be performed "to cope with external challenges, to prevent conflicts among its members or factions from tearing it irretrievably apart, to procure resources necessary to its preservation and well-being, and to frame goals and policies designed to achieve them" (Rosenau 1992: 3). This applies to any system irrespective whether it is made up of local, national, regional or global actors, or a combination of them. In short, it requires coordination. Continuing the dichotomous elaboration of governance, any governance arrangement is only effective when it is accepted by a critical mass of those affected, while governments can rule against an opposition (Rosenau 1992: 4). In this argument, authority is at once a prerequisite and a consequence of effective governance: Carrying this argument to its logical conclusion, Rosenau states that "governance is order plus intentionality" (Rosenau 1992: 5) in that a group of actors coordinates itself to effect agreed-upon consequences.

Barnett and Duvall (2005) make similar observations regarding the lines of inquiry predominant in research on global governance when they state that "[m]ost definitions revolve around the *coordination* of *people's* activities in ways that achieve more desirable *outcomes*" (Barnett and Duvall 2005: 6; emphasis added). Starting from there, they lament that research on global governance leaves out discussions of power which are buried under liberal conceptions of mutual interests and collaboration.[8] Concerned with the ways how such global outcomes are produced, they identify four variants of power that include the coercive type, institutional power, structural power as well as productive power that involves the creation of specific subjectivities (Barnett and Duvall 2005: 3-4). While being sympathetic to their suggested research direction, which zooms in on the four expressions of power within governance arrangements, their initial generic definition does not per se preclude these discussions that can be perceived as being embedded within the coordination among different actors to initiate a governance arrangement, exclude others, determine certain rules and "mutual" goals.

Another suitable source to identify the central questions that global governance revolves around is Weiss & Wilkinson's (2014) attempt to "rethink global governance." Starting with their observation that the concept has come to merely denote an increasingly crowded global stage and

[8] Similar arguments are made by Sending & Neumann (2006: 654; see also Neumann and Sending 2010) who argue that governance approaches "fail in exploring both the power at work in the actual practices through which governance takes place, as well as the more specific content or logic of the relations between state and nonstate actors."

to be a descriptor of managing globalization starting in the 1990s, they do not give up on its analytical value. In their call to revive the concept of global governance, they highlight the utility to make the approach applicable to certain issue areas such as the environment, economic affairs or global security. Moreover, while not giving up the policy-orientation, they suggest to pay particular attention to the involved groups of actors, their coordination mechanisms and how they reach certain consequences: "We should not only describe who the *actors* are and how they *connect* to one another, but also how a particular *outcome* has resulted and why and on what grounds authority is effectively or poorly exercised" (Weiss and Wilkinson 2014: 211; emphasis added). Moving beyond merely descriptive analytics, focusing on the actors of governance can reveal how different levels of interaction, e.g. at the local, national and regional level, create not only common understandings but also frictions in terms of authority and effectiveness. With respect to coordination, they take up Barnett & Duvall's (2005) concern by emphasizing the central role and myriad expressions of power that are exercised in the establishment and maintenance of global governance. Lastly, any investigation of global governance should be zooming in on the consequences that are brought about by particular arrangements (Weiss and Wilkinson 2014: 207).

In line with Weiss & Wilkinson's (2014) suggestion to look at governance from an issue-specific perspective,[9] Webber et al. (2004: 4) offer one of the most often-cited definitions of security governance in the context of an analysis of European security so that for them

> *"governance involves the coordinated management and regulation of issues by multiple and separate authorities, the interventions of both public and private actors (depending upon the issue), formal and informal arrangements, in turn structured by discourse and norms, and purposefully directed toward particular policy outcomes."*

While there are various potential themes to be drawn from this definition, the authors specifically highlight heterarchy as an organizing principle, the coordination among a large number of actors, some degree of institutionalization, the role of norms in shaping relations, and political consequences (cf. Webber et al. 2004: 8). Accordingly, they acknowledge that security governance presupposes a group of different state and non-state actors working towards a shared objective. The larger share of the analytical focus is allocated to the way these actors interact and coordinate to achieve the common objective. For them security governance is characterized by the presence of varying power relations that cannot be subsumed under a clear hierarchy. Moreover,

[9] It is a common move in security governance to tie on to the host debate of global governance and restrict the definition to a given issue area (e.g. Hänggi 2005: 9; Farrell 2007: 117).

coordination and the individual relations among actors are influenced by their respective norms as well as formal and informal institutions that regulate expectations and behavior.

Elke Krahmann (2003), one of the contributors to the foregoing definition, also offers an individual, more restrictive version, which features a similar focus on coordination. She delineates governance as the structures and processes that allow a group of diverse actors "to coordinate their interdependent needs and interests through the making and implementation of binding policy decisions in the absence of a central political authority" (Krahmann 2003: 11). While her account also includes the relevance of a constellation of actors, coordination, and consequences, she adds the emphasis of the absence of a central political authority in order to more clearly distinguish it from government.

Building on the above discussion of seminal works in security governance and its host debate, the definitions revolve around three core themes, which are the (a) constellation of actors, their (b) coordination and the (c) consequences in terms of effectiveness, authority and accountability.

(a) Although the classic security governance literature accounts for new insecurities and emphasizes the growing importance of private actors, statist definitions prevail that categorize specific governance arrangements according to the involvement of the state, i.e. governance by, with or without government (e.g. Zürn 1998; see also Barnett and Finnemore 2004; Daase and Engert 2008; Kaldor and Stiglitz 2013). Depending on the particular case, this might import other problems such as particularly state-centered understandings of legitimacy, ideal-typical hierarchical coordination, and (formal) institutions. However, this also stresses one of the key tenets of the governance literature, namely that the government is merely one of many actors so that the focus on who governs in certain arrangements is of paramount importance (Webber et al. 2004: 5). These actors represent more than nodes in a given network. They are carriers of norms and interests, active agents of change or resistance that are not only coordinated but coordinate, set rules, solve problems and effect consequences. The constellation of actors is "thus engaged in processes that are both quintessentially political and dynamic, even transformational" (D. D. Avant, Finnemore, and Sell 2010b: 1).

(b) It is important to acknowledge the force and dynamism of actors as even though systems of governance are said to be "in place", it would be more accurate to say that they are "kept in place" as the involved actors continuously enact and perform it. Accordingly, some definitions especially emphasize the role of coordination in security governance (Webber et al. 2004; Krahmann 2003). Along these lines, Risse (2012: 2) defines governance as the "modes of social coordination to produce and implement collectively binding rules, or to provide collective goods." In contrast to other authors, he focuses on coordination and the mere intention to provide public goods while

avoiding the inclusion of effectiveness and authority, which for him are empirical categories that are not a prerequisite for governance (Risse 2012: 2). Coordination among governance actors is different from the hierarchical relations typical for governments. It is constituted by heterarchical interactions between different types of actors at various levels which are institutionally or normatively structured (Sperling and Webber 2014: 133).

(c) The common theme of consequences is the most elusive as it can refer to agreed-upon policy outcomes, unintended effects, the effectiveness measured by pre-defined targets as well as the authority and accountability of certain governance arrangements in the security realm. The preoccupation with authority is probably a result of the negative definition of governance as *not* government and the subsequent transfer and persistence of Weber's ideal-type of the state equipped with a monopoly of legitimate violence. Generally, legitimacy has become a recurring theme and some even find that "the decoupling of coercive force and legitimate rule is the most striking feature of contemporary global governance" (Adler and Bernstein 2005: 302; see also D. D. Avant, Finnemore, and Sell 2010b: 8-9). Precisely because coercion is often no option of (security) governance, the consequences become relevant. On the one hand, governing actors weigh joining an arrangement based on the output. On the other hand, the consequences influence whether the governed accept or resist a form of security governance.

2.5. Technology as an Epiphenomenon

After organizing the classic security governance literature, a more focused review shows that technology is excluded from analytical consideration in all three central themes. For the most part, it is considered a neutral driver of political developments. In other cases, it is a tool that serves purposeful, intentional actors to achieve their goals without having an effect on their formulation or later results.

2.5.1. Governance without Technology

The pluralization of security actors beyond the nation-state is a major trend in security governance. Research on the privatization of security highlights that non-state actors are not only the source of new security threats but also relevant providers of security (e.g. Singer 2003; Kaldor, Albrecht, and Scheder 1998; Susman and O'Keefe 1998; Held and Young 2013; D. D. Avant 2005; Friedrichs 2010). For the most part, however, the state remains a central player, too, as its monopoly on the legitimate use of force is still largely intact despite the privatization of security (Leander 2010a: 211-212; Webber 2014: 34; Wagnsson and Holmberg 2014). Yet, the

privatization and security governance literature imply a power shift from state to non-state actors (Hall and Biersteker 2002; Kaldor and Stiglitz 2013).[10]

Interestingly, globalization, technological progress and the development of information and communication technologies (ICT) are often depicted as the drivers of the advent of these new actors in global security. They are believed to bring about fundamental change in terms of temporality, geography and knowledge structures. Technologies are attributed a "transformative effect on national defence, international finance, and education, to say nothing of less welcome activities including money laundering and the facilitation of criminal and terrorist networks" (Whitman 2007: 92). In a way, technology is used here as a catch-all term that empirically introduces structural changes or alters the environment global actors inhabit. One characteristic example for how technology is utilized to illustrate the increasing complexity of world politics is offered by Avant et al. (2010b: 5-6):

> *"New technologies facilitated globalization by easing communications, population flows, and the interchange of ideas […] The same technology that enabled corporations in the United States to outsource computer support to India (challenging the ability of the U.S. government to affect its labor market) also allowed communication among Al Qaeda operatives […] New technologies have also enhanced the capacities of states. They allow the creation of ever more sophisticated communications, weapon systems, and infrastructure support, yet each innovation also brings with it new vulnerabilities that can be exploited by those with technological expertise."*

The description is representative of a re-current shortcoming of major security governance studies: the *analytical* disregard of technology and objects. Technology is indeed attributed paramount influence but is seen as an exogenous factor to fundamental political shifts such as the transfer of power or authority from (legitimate) governments to a set of non-state actors. In this respect, it is constructed outside of the political analysis itself and rather treated as a "deus ex machina" that factually leads to a diversification of authority in security governance. After asserting this incidental role of technology, it is excluded from the further analysis of security governance.

There is quite a diversification of security governance research that goes beyond the traditional focus on international organizations such as the European Union and NATO. Security governance

[10] Sending & Neumann (2006: 652) criticize that most global governance approaches feature a zero-sum conception of power in that "an increase in the power and influence of nonstate actors is ipso facto defined as a simultaneous reduction in state power and authority." In contrast, they argue that non-state actors are variously embedded and entangled in state-led governance initiatives. In this respect, non-state actors are not taking over government functions but rather become instrumental in their exercise of power (see also Neumann and Sending 2010; Leander 2010a).

is located in the actions and self-regulation of business actors (e.g. Börzel, Hönke, and Thauer 2012; Flohr et al. 2010) or in the ways rebel groups and militias provide security for a delimited group of people (Branovic and Chojnacki 2011; Bryden 2006). The growing interaction between state and non-state actors across geographies makes it increasingly difficult to uphold the global/local and public/private distinction (Abrahamsen and Williams 2011; Berndtsson and Stern 2011; Webber 2014). Questioning such fundamental distinctions gives rise to research that embraces complexity and takes into account everyday security practices as relevant objects of study (e.g. Leander 2010a; Shepherd 2013; Berndtsson and Stern 2011; Wibben 2011; Shim 2016; Hönke and Müller 2012). Effectively, taking the 'who' seriously has produced studies that find counterintuitive actors providing security, move away from Western organizations to 'smaller' non-traditional security case studies and increasingly leave behind the normative bias of global governance. Despite this diversification of actors, however, they stay restricted to human actors such as IGOs, nation-states, warlords, terrorist networks, NGOs, think tanks or private companies (Wilkinson 2002: 2). Material, objects or technologies are reduced to anonymous drivers of change (e.g. technological progress), opportunity structures (e.g. natural resources), geographical delimitations (e.g. topographical features), infrastructure (e.g. highways) or instruments of violence (e.g. weapons). As notable exception, one line of research assigns technology a more prominent role as object of governance (e.g. Allenby 2011; Sarewitz 2011; Rappert and Croft 2007; Farrell 2007). The security governance of certain technologies addresses issues such as WMD proliferation or the conduct of warfare. More generally, this kind of research is preoccupied with the ways and effects of the control of military technology, i.e. arms control (Farrell 2007: 118), the use of drones (Casey-Maslen 2014) or the impact of emerging technologies as technological advances often outpace international rule-making (Whitman 2007: 94; Wittes and Blum 2015).

Overall, security governance research acknowledges a more diverse set of actors in line with its assumptions of a wider and deeper security concept. Technology, however, largely remains outside of the political analysis of governance but rather figures as an exogenous conditioning factor in terms of the diversification of involved actors, complexity of issues and the alleged empowerment of non-state actors.

2.5.2. Coordination of Governance and Technological Constraints

The proliferation of actors, the introduction of market logics and newly emerging security issues change the way of governing from an authoritative to a more informal and less institutionalized mode (Daase and Engert 2008: 481). From a coordination perspective this can be framed as a loss of state control due to the functional and geographical differentiation of security governance and its actors (Krahmann 2003: 20). However, this is no necessary consequence since states might

seek to diversify or depoliticize certain security practices through the deliberate inclusion of private actors and an effective distribution of responsibility (Ehrhart, Hegemann, and Kahl 2014b: 152-153). Although security governance involves more heterarchical coordination, this does not eliminate the centrality of power in actor relations. Moreover, bringing together a variety of actors, goals and interests renders security governance a dynamic process in that changes within those relations can have an impact on the structure, rules and outcomes. In fact, relations among governance actors "may be cooperative and additive, leading to far-reaching effects, or tense, dysfunctional, and even conflictual [..], leading to failed action and potentially weakened authority" (D. D. Avant, Finnemore, and Sell 2010b: 17). Therefore, understanding security governance as relational and dynamic means to focus analytic attention on how coordination is put into practice.

The lack of a vertical authority allows for ad-hoc governance constellations that agree on tackling a specific security threat. As such, they are bound by common interest or the conviction 'to do the right thing.' Participation largely depends on the willingness to join, corresponding perceptions of security threats and an agreement on the objectives (cf. Webber et al. 2004: 7). Such constellations can be considered fragile since an actor's participation is only bound by its interest just as its dropping out. (Daase and Engert 2008: 486). At the same time, the absence of formal authority obscures hidden power structures and normatively embraces governance as a positive way to go forward (Barnett and Duvall 2005; Slaughter 2004). Parts of the security governance literature itself criticize the benign take on purposeful multi-stakeholder coordination: Security governance can be initiated with the best of intentions but lead to unintended consequences that limit the outcomes or even serve to worsen the original problem (Friesendorf and Daase 2010; Friesendorf 2007a). Moreover, complex or horizontal governance structures allow more powerful actors to introduce hidden pressures under a "shadow of hierarchy" (Börzel 2010) that leaves the actual voluntariness of actors in question (Ehrhart, Hegemann, and Kahl 2014b: 153).

Yet, the discussion about common interests, initiation and coordination of security governance misses the influence and co-constitutive forces of technology. More particularly, security technologies can act as a co-initiator of security governance efforts. Governance arrangements can center around certain technologies such as CCTV cameras which, in turn, introduce a multitude of other actors into the arrangement such as producers, data management systems, maintenance companies, algorithms and operators. In this way, technology can be conducive of the initiation of security governance arrangements, introduce new actors and co-determine the ways of coordination. A more active inclusion of technology into the analytics of governance might highlight hitherto neglected effects on the formulation of goals in that material participants to

governance pose particular constraints and potentialities in the initiation and coordination of security governance.

2.5.3. Unintended Consequences of Technologized Governance

With respect to effectiveness, some security governance scholars point to the inclusion of non-state actors because of the incapability or unwillingness of governments to tackle certain security issues (Risse 2012). Non-state actors such as NGOs or MNCs contribute to efficient security policies in terms of burden-sharing or specialized knowledge (D. D. Avant 2005; Friesendorf and Daase 2010). However, unintended consequences are likely to occur with security governance due to the large number of involved actors as well as the conditions of uncertainty regarding other actors' preferences, the problem itself and the ultimate output (Daase and Friesendorf 2010: 8). More generally, measuring an elusive concept as effectiveness of security governance is a difficult task. Quantitative approaches focus, for example, on the persistence and intensity of interaction between governance actors on a structural level (Schroeder 2011) or seek correlations between security provisions of regional organizations and domestic economic and political development measured by common indices such as the Human Development Index (Kirchner and Dominguez 2014). Webber (2014: 34) suggests to focus on particular policy measures "where we can see effects" – for example with treaties banning particular weapons. However, in any case "the effectiveness of security governance refers to more than just the achievement of stated objectives" (Ehrhart, Hegemann, and Kahl 2014b: 153).

Increasing effectiveness and efficiency constitutes a common-sense justification for the application of technology in security governance. Mostly, security technologies such as weapon or surveillance systems are produced for certain purposes. Consequently, an assessment of their effectiveness appears to be more straightforward than with complex constellations of actors in security governance. However, this connotes a mere instrumental understanding of technical devices that help to save money and increase objectivity. Although security governance might successfully achieve certain target goals, this does not preclude unintended consequences from occurring simultaneously. For example, a comprehensive surveillance system might increase the detection of certain crimes but also erode long-held privacy norms, or the use of attack drones reduces one's own casualties but elicits local resentment that prolongs a conflict. Against this background, the discussion of effectiveness in security governance would benefit from a more decided inclusion of technology into the political analysis that goes beyond its neutral, instrumental value.

Overall, the more classic security governance literature neglects the role and workings of technology within governance arrangements and, therefore, misses meaningful parts of empirical and conceptual phenomena. Technology features merely as an epiphenomenon or external

driving force of security governance. Consequently, the governance with technology – also in the form of more mundane objects such as cataloguing systems, folders, performance sheets etc. – is unaccounted for. Moreover, material objects are excluded as actively constructing or affecting security threats and goals despite conceivable opportunities and constraints they present. Rather, the security governance literature features an instrumental understanding of technology that has no effect on the intentions and practices of governance actors. Lastly, the power of technology to create legitimacy of governance is neglected as relations of authority and legitimation are restricted to human actors. In essence, despite the fact that security governance is embedded into a complex material environment and integrates technologies into its fundamental workings, classic security governance research mostly fails to grasp its relevance beyond an instrumental value or as exogenous driver of change.

Despite this exclusion of technology from the analytics, there is a growing tendency to refrain from structural theories and embrace the micropolitics of security governance (e.g. Ehrhart, Hegemann, and Kahl 2014a; Hönke and Müller 2012). More recent security governance literature moves away from broad analyses of global cooperation, international organizations and institutions such as NATO or the EU towards more issue-specific types of analysis. In doing so, it increasingly takes practices and relations among actors into account, embraces complexity, employs ethnographic methodologies and emphasizes the contextual specificity of the phenomena under study. The growing focus on empiricism seeks to compensate for a lack of conceptual clarity. Moreover, it takes seriously the appeal that "a deeper investigation of contemporary global governance has the potential to capture more accurately how power is exercised across the globe, how a multiplicity of actors relate to one another generally as well as on specific issues, [and] make better sense of global complexity" (Weiss and Wilkinson 2014: 207).

2.6. Early Attempts at Bringing Technology Back In

Although technology receives little theoretical attention in security governance research, weapon systems, communication or dual-use technologies regularly stand in the center of questions of international security. This thesis is not alone in wondering about such an omission (Mayer, Carpes, and Knoblich 2014; Fritsch 2011). Therefore, it is useful to briefly reflect on earlier attempts of International Relations scholarship to introduce a sensitivity for technology to the discipline. These attempts pick up on a central controversy in Science and Technology Studies (STS) of two contrasting ideas about the relation between technology and politics.

On the one hand, a determinist understanding theorizes the relation between technology and politics largely as a one-way street. While technology is invested with immense power to bring about societal change, the human factor is scaled down and rendered a mere reaction to an autonomous force. In short, social organization hinges on technological development. The canon

of IR theory is reminiscent of determinist notions of materiality, when thinking about the distribution of power as a function of, among other things, military technology in (neo-)realism (Waltz 1979) or the function of technology to facilitate international cooperation in reducing transaction costs in neoliberalism (Keohane 1984). On the other hand, constructivists question the origin of the alleged autonomous force. They "criticize the one-dimensional, almost teleological view of determinists and the disempowerment of social actors to influence technological development" (Bijker 2010: 71). By proposing to include technology itself in the analysis and not reduce it to social and political effects, they make it "the *explanandum*, not the *explanans*" (Pinch and Bijker 1987: 24; italics in original). Social constructivism of technology problematizes that technical design cannot be taken for granted and instead asks how it came about that a missile is built in such a way and what were the roles of inventors, bureaucrats, users, academia, policymakers and so forth.

Instead of favoring one side over the other, research in IR has tried to develop a so-called middle ground that leaves intact the autonomous force or influence of "mature" technologies while highlighting the social construction in their development phase (Fritsch 2011; Fritsch 2016; Herrera 2003; Herrera 2006). Being among the early participants to the discussion of explicitly introducing STS thought to IR, Geoffrey Herrera (2003; 2006) does not so much focus on how technology is involved in governing security. Rather, he investigates in what way nuclear and railway technologies bring about change to the international system. Mirroring the review of security governance above, he posits that technology in IR theory has regularly been treated as an exogenous factor, hence making it apolitical. For him and Stefan Fritsch (2011), who follows a similar line of argumentation, material objects are not uni-directionally determining behavior of other actors as technological determinists would have it (for a discussion of different variants of determinism, see Bimber 1990; Ellul 1964; Heilbroner 1967). Nor, can technology be grasped as just another social phenomenon that can be fully understood in linguistic terms as in social constructivist accounts (Bijker 2010; Pinch and Bijker 1987). It is argued that to study the relation of technology and politics both are of limited use. Determinism too nonchalantly accepts fixed effects and eschews social agency, while social constructivism overemphasizes the development phase of technology while omitting the political implications of established technological systems. Embracing a middle ground acknowledges the social construction of technology in that actors participate in shaping, changing and using a technical device while retaining a sense of its autonomous force once it has reached maturation. In other words, the progress of a technology co-determines the direction of analysis. As a consequence, it becomes possible to consider established technological systems such as nuclear weapons or the railway as fundamentally changing the interaction capacity of actors so that "technology must be considered as an important, transformative element of the international political system" (Herrera 2006: 11).

A related dichotomous understanding of the relationship between technology and society is re-introduced to Security Studies by Columba Peoples (2010) and Mike Bourne (2012).[11] They contrast an instrumentalist and a substantivist conception. The former takes technology as a neutral tool that is employed in line with the user's norms and intentions while itself not exerting any power over the formulation or achievement of goals. The substantivist variant sees society and politics as determined by technology regardless of the norms and intentions underlying its use. In an extensive and well-researched study, Peoples (2010) offers a thusly-framed dichotomous account of technology-society relations. However, he does not follow Herrera and Fritsch in developing a combination of two opposing approaches. Instead, he highlights the value of retaining the distinction in his analysis of the U.S.-American ballistic missile defense (BMD) project. He shows how various social actors utilize and combine both contradictory conceptions in order to legitimize the controversial development of BMD against economic, strategic and scientific critique. Retaining the differences in the notion of technology, therefore, "suggests that at least as important as the type of understanding of technology employed […] is the way these understandings overlap, intersect and contradict each other. Moreover, it suggests that where such contradictions exist they do not necessarily lead either to the collapse of an argument (as would be expected by logical analytical thought) or to an improved, synthetic argument" (Peoples 2010: 36).

While both lines of research contribute to a more nuanced thinking about technology in global security, they keep up a strict separation between politics and technology. Moreover, Peoples analysis remains on the discursive level by focusing on the contradictory use of instrumentalist/substantivist understandings of technology to justify BMD. On the other hand, the proposed middle ground of determinist and constructivist understandings of technology could be criticized in that it does not offer a synthesis but rather a sequencing of approaches. It adds a temporal dimension to determinist arguments in that only complex, large and mature technological systems have an autonomous bearing on the international system; until then they are conceptually approached as socially constructed (cf. McCarthy 2013). In sum, the discussed attempts do not provide a qualitatively different approach to the role that material objects play in security governance. However, they draw attention to the wide-ranging consequences of particular concepts of technology for global security in theory and practice. The remainder of chapter, therefore, turns to socio-material approaches to security in order to gain a deeper understanding of the entanglement of technology and politics.

[11] Both of them extensively refer to Richard Wyn Jones (1999) who himself has drawn on Andrew Feenberg's (1991) typology.

2.7. The Entanglement of Technology and Politics

2.7.1. Setting the Scene: Socio-Material Approaches to Security

Socio-material approaches to security (SMAS) represent a diverse research program that takes seriously the materiality of global security. In doing so, they introduce a sensibility to the power of objects, highlight the importance of relations among (non-)human entities, and question the prevalent divide between human and material, and politics and technology. As such, SMAS are well-suited to amend classic security governance research and include technology as an analytical, forceful category. The SMAS terminology introduced here should not be understood as a rigid disciplining move that prescribes definite theoretical positions. Rather, it is an auxiliary label to come to terms with a diverse set of scholars and a multi-disciplinary research program that focuses on the role of technology in political and social analysis. As such, SMAS bring together scholars from multiple backgrounds that engage with the role of materiality in global security. In doing so, they draw on contributions from Anthropology, Feminist Studies, (Political) Philosophy, Sociology, and Science and Technology Studies (STS) (e.g. Barad 2007; Bennett 2010; Connolly 2013; Coole and Frost 2010; DeLanda 2009; Deleuze and Guattari 1987; Jasanoff 2004a; Latour 2005; Law 2009; Ong and Collier 2005). In light of this diversity, one of the objectives is to filter out central, shared tenets of SMAS to address the analytical neglect of technology in security governance.

For this purpose, the chapter picks up on an interjection by William Walters (2014) that socio-material approaches to security have largely been focusing on issues of governance. They reveal the hidden politics of security assemblages in acknowledging how material objects are entangled in political action. At the same time, he cautions that a restriction of SMAS on governance bears the risk of reasserting a technocratic view of politics. Similar to the problem-solving bias within classic security governance literature, it gives up the inherent contestability of technology and its importance for political controversy. While this constitutes an important call to remain vigilant to not lose sight of power and resistance within security governance, it rather appears as an issue of research focus and case selection than a theoretical blind spot or general weakness of SMAS. In fact, various studies of SMAS decidedly trace the power politics and controversies in what appears to be technocratic management of security and, therefore, paint a picture of material politics that is anything but consensual, mechanistic or apolitical (e.g. Mayer 2012; Schouten 2014a; Voelkner 2011). With that said, Walter's categorization of socio-material approaches to security as largely focused on governance is taken up as an invitation to carve out an analytically useful conceptual understanding of technology for security governance.

SMAS are not limited to sophisticated, large or digital technologies but also attend to everyday devices and mundane objects (Amicelle, Aradau, and Jeandesboz 2015; Neyland 2009). Yet, there

is a perceptible sense of novelty about current technological changes which have been overlooked by IR's restriction to the social (Bellanova and Duez 2012: 111). Scholars highlight the increasing entanglement of the human and material world as evidenced by the global impact and virality of pandemics, the omnipresence of technological infrastructure or the rise of bio- and nanotechnology (Srnicek, Fotou, and Arghand 2013: 397; Lundborg and Vaughan-Williams 2015; Rothe 2015). Within this line of research, "materials experience an emancipation from their role as passive recipients and start to co-articulate agency and shape political practices" (Müller 2015: 35; see also Jacobsen 2015).

In terms of coverage of the reviewed literature, this section's primary focus is on empirical research on security issues that draws on insights from varying research strands concerned with the materiality of the social such as new materialism(s), object-oriented ontology, actor-network theory (ANT), assemblage thinking or speculative realism (Breu 2016; Coole and Frost 2010; Deleuze and Guattari 1987; Harman 2009; Latour 2005). However, where appropriate fundamental texts from STS and other disciplines are included to adequately contextualize the arguments. Still, the goal is not to trace the philosophical traditions of socio-materiality in Security Studies; nor to appraise whether SMAS have properly derived conceptual ideas from the fundamental texts. Such discussions warrant a separate investigation. More pragmatically, this is a reflection on insights from SMAS in light of the preceding discussion of security governance and with the intention to reach an instructive and research-informing understanding of technology in security governance.

2.7.2. Three Common Features of SMAS[12]

As SMAS draw on a diverse set of disciplines and research traditions, they produce an equally varied research program. In order to facilitate a productive discussion of technology in security governance, three broadly shared features of socio-material approaches to security are presented. The emphasis on material agency, relationality and empiricism create further conceptual starting points for the formulation of a conceptual framework in the following chapter.

First, socio-material approaches to security technology have given rise to a prolific research program whose proponents pay renewed attention to the role of materiality in security (e.g. Acuto and Curtis 2014; Amicelle, Aradau, and Jeandesboz 2015; Bellanova and Duez 2012; Bourne 2016; Bousquet 2014; Hoijtink 2017; Jeandesboz 2016; Leese 2015; Mayer 2012; Schouten 2013). Arguably, their most fundamental proposition concerns the question of material agency (cf. Leese and Hoijtink 2019). Initial reactions have made the notion of material agency figure prominently in debates on the raison d'être of new materialism in particular and socio-material approaches in

[12] This section draws on Olbrich (2019a).

general. The notion stirs up especially heated controversies when it is understood as ascribing rationality and intentions to material artifacts, the modernist hallmarks of human agency. Agency, in this modernist sense, is strongly connected to desire and intention leading to the impression that "non-human beings and things evolve, [whereas] we humans, we political animals, go about planning and changing our world" (Cudworth and Hobden 2013: 439). To be sure, there is some diversity in the degrees of material agencies ascribed across the literature. For example, Diana Coole (2013) starts out to dissociate herself from more vitalist-oriented authors such as Latour (2005) and Jane Bennet (2010) who ascribe agency to inanimate things. In their words, material agency can be grasped as an actant that can be "*any thing* that does modify a state of affairs by making a difference" (Latour 2005: 71, emphasis in original) or as thing-power which "draws attention to an efficacy of objects in excess of the human meanings, designs, or purposes they express or serve" (Bennett 2010: 20). At the core of such concepts lies the idea that agency is a function of bringing about change or having efficacy. However, Coole (2013: 260-261) is concerned about giving up reflexivity as a necessary condition for agency as it is a prerequisite to hold actors accountable. The basic claim, however, should not lead to much controversy.

The essential idea of material agency is probably best understood by way of the so-called symmetry principle. It refers to the basic analytical equality of the human and the non-human (Latour 2005).[13] This does not mean that human beings, things, institutions, and concepts matter in the same way, produce equal externalities or are even interchangeable in a given setup. Rather, following the symmetry principle "simply means not to impose a priori some spurious asymmetry among human intentional action and a material world of causal relations" (Latour 2005: 76; emphasis in original). In doing so, material agency takes issue with strict distinctions between humans and things, science and politics, knowledge and policy that suggest a hierarchy in that humans command things without conceptualizing the reverse. Accepting relations between technologies and human actors as reciprocal, the symmetry principle enables what is called material agency. Importantly, however, it needs to be noted that agency here is not understood in the modernist, or moral, sense of (human) agents pursuing a specifiable end with intentional actions (Bennett 2010; Cudworth and Hobden 2013). Rather, agency is to be sought in a distributed assemblage of things and humans that is characterized by its capacity of making a difference in relations rather than by its intentionality (Latour 2005). In effect, materiality gains its force as a part of a constellation so that "[t]he idea that a non-human device or instrument can

[13] The symmetry principle if often related to propositions to overcome the Cartesian dualism. The Cartesian dualism of idea and matter is suspected trap analysis in human-centered approaches (cf. Rekret 2016). Therefore, it does not grasp the inherent imbrication of the human and non-human. As a response, scholars variously suggest to replace it with a "protean monism" (Connolly 2013), "ontological agnosticism" (Schouten 2014a), "ontological symmetry" (Bourne 2012), "principal symmetry" (Mayer 2012; Latour 1993) or "generalized symmetry" (Callon 1986a; see also Jeandesboz 2016).

somehow work autonomously of its multiple connections with other (human and non-human) elements (language, bodies, minds, desire, practical skills, traditions of use) is a fantasy" (Barry 2001: 9). Then again, it is possible to say the same thing about human actors who, in turn, are also not exclusively in control (cf. Voelkner 2011). Socio-material approaches disrupt the common idea of attaching agency to fixed entities and instead locate it in a distributed form across networks of relations. As such, material agency denotes the force of objects to have an impact on actions in terms of dispositions, potentialities, resistance, or constraints.

Second, SMAS are concerned with tracing relations in complex networks. This is grounded in a pertinent skepticism towards taken-for-granted entities such as the state, international organizations, or technology. They are understood as an arrangement of "artefacts, practices and techniques, instruments, language and bodies. These arrangements make up what we tend to think of as persons and institutions: states, markets, families and so on. They are collectivities which include technological components. In principle, the complexity of such arrangements is irreducible to their distinct 'social' and 'technical', 'natural' and 'cultural' elements" (Barry 2001: 11). Accordingly, SMAS take actors and objects as part of assemblages or actor-networks (e.g. Acuto and Curtis 2014; Amicelle, Aradau, and Jeandesboz 2015; Aradau 2010; Bellanova and Duez 2012; Bourne 2012; Bousquet 2014; Ong and Collier 2005; Schouten 2013; Mayer 2012; Voelkner 2011). More specifically, in order to account for socio-material relations security scholars draw on Latour's actor-network theory (ANT) (Latour 2005; Law 1991; Callon 1986b; Leander 2013; Jeandesboz 2016; Mayer 2012) or Deleuzian concepts of assemblage (Deleuze and Guattari 1987; DeLanda 2009; Acuto and Curtis 2014; Srnicek 2014; Voelkner 2011; Meiches 2015). Both ANT and assemblage approaches are frequently treated in parallel, disregarding their differences which are perceived as "one of emphasis rather than kind" (Acuto and Curtis 2014: 5; see also Mayer 2012). In fact, Latour (1999) himself alludes to the proximity of ANT to Deleuze and Guattari's figure of the rhizome and John Law (2004) sees little difference between an assemblage and an actor-network.[14] However, SMAS do not stop at deconstructing networks or assemblages into isolated smaller pieces but instead examines how they are reassembled into functioning wholes (Breu 2016: 18). Consequently, tracing the socio-material relations that make up these entities becomes the responsibility of the researcher as broad notions such as a nation-state cannot do justice to the specific political, historical, and material contexts which they are believed to represent. Taken together, socio-material approaches highlight relationality. They introduce a networked understanding of human-material relations to study the effects of technology within security governance.

[14] Chapter 3 carves out the differences between ANT and assemblage thinking (see also Harman 2014; Müller 2015).

Third, an emphasis on contingency challenges wide-ranging theoretical abstractions and gives an important role to the micro level and empiricism in socio-material approaches. Security assemblages are not perceived as fixed or stable objects but in flux and merely temporarily stabilized (Bourne 2016: 5). This leads to an analytical focus on how actors "perform security by enrolling, assembling and translating heterogeneous elements into stable assemblages" (Schouten 2014a: 32). The contingency of relations makes SMAS well-suited for studying how specific governance arrangements emerge and are kept together in order to reveal the power politics at play behind presumed functional processes (Müller 2015: 27). Accordingly, Adey & Anderson (2012) argue that keeping socio-material governance assemblages intact is hard work and "that more attention needs to be paid to the way in which apparatuses of security fall apart, fail, are disrupted, or are held together by very specific and careful consideration of what these material and contingent relations mean" (Adey and Anderson 2012: 113). In short, governance assemblages are characterized by a contingent and volatile nature in that the heterogeneous relations among human and material actors require constant enactment through material and discursive practices (Mayer 2012: 168-169). An analysis that follows the symmetry principle walks a tightrope in that it neither favors material nor human factors but focuses on their interplay, thereby highlighting contingency over linearity and becoming over continuity. As a consequence, a large part of the socio-material literature eschews investigating macro phenomena but rather concentrates on specific, traceable relations that are accessible through detailed ethnographic, interview, or other qualitative methods. Moreover, the assumed complexity suggests exchanging wide-ranging social concepts for an empiricism that "requires us to attend at once to the specificity of materials, to the contingencies of physical geography, the tendencies of history and the force of political action" (Barry 2013a: 183). SMAS discard preconceived analytical notions and instead prescribe to stay as close as possible to the empirical phenomena under study. The possibility of social science to offer explanations based on pre-formed, transferrable categories is questioned in that they cannot do justice to the complexity of phenomena and provide a "lazy" substitution of empirical description. Effectively, then, "[t]here is no need to go searching for mysterious or global causes outside networks. If something is missing it is because the description is not complete. Period. Conversely, if one is capable of explaining effects of causes, it is because a stabilized network is already in place" (Latour 1991: 130). As a result, SMAS call for empirically tracing the relations of technology in its specific context. In attempts to try to capture the specificity of human–non-human relations, socio-material approaches have a self-understanding of being an interpretative-empiricist program that "provide[s] a parsimonious and open ontological vocabulary meaningful for conducting empirical research" (Bueger 2014: 60).

Taken together, SMAS attribute technologies a sense of material agency, focus on relations within security governance assemblages, and introduce an understanding of such assemblages as contingent and unstable, which implies an empiricist approach to trace performative relations on the micro level.

2.8. Conclusion

A review of theoretical approaches to technology in security governance shows that the more classic security governance literature largely ignores the role of technology. It is excluded from the analysis as apolitical and reduced to an instrumental or determinist capacity. SMAS make up for this gap in that they introduce what Latour (1992) calls the "missing masses" of material artefacts that social actors are surrounded by and entangled with but have so far escaped political analysis.

Around the end of the Cold War, the concept of security governance has entered the scene as an alternative approach to then-dominant IR theories to account for newly emerging threats, the re-definition of security, and the proliferation of relevant actors in the wake of the Cold War, i.e. the deepening and widening of security (cf. Buzan & Hansen 2009: 187-225). However, the dominant conceptual repertoire of security governance does not account for the role of technology. Moreover, it reaffirms statist accounts that characterize security practices in relation to the involvement of nation-states which are axiomatically given a powerful and influential position in governance arrangements. At the same time, a growing amount of research embraces everyday practices, a further diversification of actors and security as essentially contested. It employs historical and ethnographic methods to uncover the complexity of local practices and effects of governance. Correspondingly, SMAS echo this inclination and, in fact, take it one step further. They question the usefulness of grand social explanations but time and again point to the importance of specificity and contingency of complex security relations that need to be empirically traced and described. As a result, technology becomes an active part of security governance assemblages. It is included in the analytical considerations because of its impact on the constitution of security threats and practices.

For many SMAS, however, the focus on the micropolitics and relations involves various complications. For one thing, eschewing the application of large-scale theoretical categories such as the nation-state makes it more difficult to account for macro phenomena, as Daniel Nexon & Vincent Pouliot (2013: 344; see also Müller 2015) point out for the case of ANT:

> *"[I]t is not clear exactly how one may 'scale up' in an ANT framework. This limitation seems problematic in a discipline such as IR, where most phenomena of interest – from war to international organizations – have macro-level dimensions. We understand the need to be*

careful about reifying the state or other such collective entities. But we also suspect that always "following the actors" at times risks eliding the peculiar dynamics of aggregate or macro-social phenomena from those captured by the concept of 'multiple realizability' to emergent properties."

SMAS call for thick descriptions that account for the emergence of actors, practices and consequences. For this, they promote what is repeatedly called a "theoretically informed empiricism" (Barry 2013b: 419). Accordingly, a universally applicable analytical framework is deemed inadequate to grasp the empirical multiplicity and variance of socio-material security (Marres and Lezaun 2011). Along the same lines, Bueger notes that critics "(rightfully) lament the often-awkward terminology of ANT, its lack of appropriately defined models and concepts, its literary style of presentation, as well as the radical rhetoric that often comes along with it" (Bueger 2013: 338). Taken together, SMAS are rarely clear or open about theoretical guidelines or even methods how they work empirically. This kind of empiricism grants the researcher considerable leeway in shaping the analysis. Avoiding a pre-structuring by way of theoretical concepts leaves the inclusion or exclusion of what counts to certain governance assemblages and what matters at the researcher's intuition and diligence so that they become somewhat "arbitrary in the sense of being subject to analytical choice" (Fine 2002: 216).

In light of these shortcomings, the following chapter develops a conceptual framework that integrates technology into a conceptual framework of security governance. Following Bourdieu's (1988: 774-775) expression that "theory without empirical research is empty, empirical research without theory is blind",[15] Hönke & Müller (2012: 385) remind us that this does not simply pit theory against empirics. Rather, such an approach calls for theory-led investigations of security governance that draws together diverse and thick empirical material from written texts to interviews to observations of everyday practices (Hönke and Müller 2012: 384-385).

Therefore, the following chapter is faced with daunting tasks: It needs to strike an adequate balance between acknowledging the varying roles of material objects and technology while not losing sight of the importance of human intention, reflexivity and responsibility. Similarly, a focus on the relationality, performativity and specific associations among actors cautions against reifying long-held but flawed abstract concepts. All in all, the careful development of a conceptual framework is useful for assessing broader, recurring political implications of technologized security governance.

[15] Bourdieu himself is paraphrasing Kant's (1974) original proposition "Gedanken ohne Inhalt sind leer, Anschauungen ohne Begriffe sind blind." [Thoughts without content are empty, intuitions without concepts are blind.]

3 Conceptual Framework

3.1. Introduction

The literature review has outlined the reservations of socio-material approaches to security (SMAS) towards conceptual frameworks. In this light, the chapter pursues three main goals: First, to reflect on the feasibility, difficulties and benefits of a conceptual framework. Second, to clarify the meaning of major terms used in the thesis such as security governance, material agency, technology and assemblage. Third, to develop a conceptual framework based on SMAS that resonates with classic security governance scholarship. As such, the theoretical contribution of this chapter lies in the combination of two rather segregated research programs to form an approach that is applicable and useful across different cases in which technology has become a central feature of security governance. This runs counter to many socio-material studies that develop their conceptual vocabulary inductively as part of the empirical analysis. In order to retain this interpretive potential, the framework limits itself to central concepts that are useful in thinking about the role of technology in security governance while remaining responsive to the empirical material at hand.

The following section briefly reflects on the difficulties and benefits of combining SMAS and classic security governance thinking. Next, the framework is sketched out in three parts to set the stage for a more detailed discussion. In turn, section 3.3. spells out the thesis's understanding of technology as largely defined by its capacity to condition human action through particular potentials and constraints. Similarly, it is argued that material agency – as the most prominent proposition of SMAS – has served its purpose of re-introducing the importance of the material world into Security Studies in provocative ways. Arguably, this came at the cost of the balance between the human and the material in theoretical and empirical analyses. The section, then, develops the first concept of the conceptual framework: *Problematization* captures the human-material co-production of security threats and creates a desire and legitimacy for technologies to become central for addressing them. Section 3.4. highlights the assembled character of security governance arrangements and outlines the assumed instability of entities such as the state or technological systems. Moreover, it discusses the idea of relationality that is central to socio-material accounts. Here, the section argues for a more differentiated view on relations among human and material actors. This sets the stage for the second concept of *stabilization:* As security governance is constantly formed in volatile assemblages, stabilization turns to the actors, practices and objects that lock in certain patterns and goals. Section 3.5. discusses the *durable effects of* technologized security governance. Essentially, they are understood as a function of the specific problematization and stabilization processes. Once sufficiently stabilized through

routinized practices, objects and technologies, security threats are addressed in repetitive patterns that reinforce particular goals and norms. In this way, these goals and norms become maximized up to a point where they might have unexpected consequences. The conclusion summarizes the thesis's framework and recapitulates the three central concepts: problematization, stabilization and durable effects.

3.2. Combining SMAS and Security Governance into a Conceptual Framework

SMAS and classic security governance seem divided along epistemological and ontological lines. While much of security governance scholarship adheres to the discipline's gold standard of theory testing, socio-material approaches rather follow anthropological and ethnographic propositions of inductive theorizing (Schouten and Mayer 2017: 311). In connection to this, security governance operates with various taken-for-granted entities such as the nation-state, borders, technical devices and international organizations. In contrast, socio-material studies often render them as historically and materially contingent upon specific relations and practices. As such, they are the end point rather than the beginning of analysis. Despite this divide, however, it is argued that a combination of the two research programs usefully promotes the study of technology in global security. SMAS lend themselves to introduce a technological understanding to security governance that moves beyond instrumentalism and determinism alike. In this way, there is no need for re-inventing security governance and its central themes so that discussions about the technology/security nexus more easily connect to existing scholarship on securitization, human security, governance, humanitarian action or the privatization of security (cf. Mayer and Acuto 2015). With that said, the goals of the theoretical part are quite humble. The objective is not to develop a stand-alone theory from the ground up. Instead, the aim is to develop a conceptual framework as a vehicle to think about the specific ways that technologies co-produce, shape and mediate the effects of technologized security governance.

Some scholars have voiced sensible concerns about turning socio-material contributions into an analytical framework for International Relations (IR). Referring explicitly to studies informed by actor-network theory (ANT), Barry argues that they are "undoubtedly weakest when the theoretical ambitions that drive them overdetermine their analysis of empirical evidence. In principle, actor-network theory promotes a theoretically informed empiricism, and a commitment to experimentation in empirical research" (Barry 2013b: 419; see also Bueger 2013; Bueger 2014). As mentioned earlier, the objective here is not to put SMAS or ANT into a corset. But to strike a balance and provide a pragmatic way of analysis that is both useful across cases but open and flexible enough to account for empirical detail. This balance necessarily is delicate and potentially controversial. Therefore, the remainder of the section further explicates the rationale

for a conceptual framework and the arguments for bringing together SMAS and security governance.

(1) Socio-material discussions in IR and elsewhere run the risk of losing other security researchers. They draw on scholarship from a variety of disciplines such as Anthropology, Gender Studies, Philosophy, Science and Technology Studies (STS) or Sociology (Barad 2003; Barad 2007; Bennett 2010; Coole and Frost 2010; Connolly 2013; Deleuze and Guattari 1987; DeLanda 2009; Law 2009; Latour 1992; Latour 2005; Jasanoff 2004b; Ong and Collier 2005). This complicates the task of creating immediate connections to research of many security scholars. Such a development is unfortunate as SMAS offer the vocabulary to grasp the myriad ways technologies influence global security beyond their instrumental value and determinist force. A conceptual framework comes with the advantage to channel this vocabulary in a manner that is aligned with much of security governance scholarship and, thereby, makes it more accessible. By design, scholars from both aisles will find immediate points of connection as well as contestation, which fosters opportunities for common discussions that hitherto are rather confined and restricted.

(2) SMAS and constructivist security governance scholarship share a common foundation in their focus on the workings of power and empirical approach. To some degree, parts of the security governance scholarship already move closer to fundamentals of socio-materiality such as the insistence on in-depth empirical analysis or the prominence of practices and relations. In an attempt to situate a new materialism in IR, Diana Coole (2013: 456) draws the boundaries as follows:

> *"In the context of International Relations it might perhaps be helpful to categorise [new materialism] as opposed to positivism or behaviouralism; as sympathetic to the idea of historical materialism as the study of the historical emergence of matter (albeit while abandoning earlier tendencies towards grand historical narratives, a Newtonian understanding of determining laws of matter and a drift towards reifying obsolete structural logics); and as open to the critical approaches associated with constructivism, especially regarding the way power insinuates and reproduces itself, provided these are integrated, on the one hand, into broader social scientific investigations of emergent material structures and the material interests they serve and, on the other, into more detailed empirical studies of how power maintains itself and its planetary consequences for survival."*

Socio-material concepts cannot simply be exported into any kind of security research. But there are points of contact especially in constructivist approaches to security governance. In short, there is a frame of reference in which socio-material thinking makes sense in security governance – which William Walters (2014) has also observed empirically in that a large share of socio-material

studies focus on governance issues (see chapter 2). Moreover, Coole mentions new materialism's inclination for in-depth empirical work. It was already pointed out in chapter 2 that portions of the security governance literature have become more granular in their empirical material and increasingly embraced ethnographic methods for theory development and data generation. In this vein, calls by scholars for "[a] new generation of global governance research [that] should be both pro-empiricist and anti-reductionist" (Coen and Pegram 2015: 418) resonate with central propositions of SMAS and have already been heard by some researchers in security governance (Avant 2016; Avant and Westerwinter 2016; Hönke and Müller 2012; Leander 2013, 2016). This also points to the potential benefits of bringing together SMAS and security governance as it gives a theoretical language to a trajectory that is already in the making.

(3) A conceptual framework addresses some of the major shortcomings in the security governance and socio-material literature. Most importantly, it introduces objects, weapons and technologies into the analysis. With respect to SMAS, it provides a clear, pragmatic starting point that went missing in many socio-material studies (Bueger 2013: 339). As first-time readers of ANT often come to realize "the language employed can be opaque and lead up to rather quirky concepts and terms. The open-ended character and multi-vocality of the narratives developed and the experimentation with different literary styles tends to simultaneously fascinate and alienate many readers. Indeed, it makes ANT studies at times very difficult to access" (Bueger and Gadinger 2014: 50). Providing ex-ante analytical guidelines should increase accessibility, coherence and clarity as it follows disciplinary conventions and more readily structures the empirical material. SMAS at times appear to get lost in looking inward and use detailed empirical descriptions as sparring partners for the development of ever more intricate and overlapping theoretical language. In contrast, some security governance scholarship might be accused of imposing preconceived theoretical constructs on an abstract reality. A conceptual framework attempts to combine both perspectives by embracing an analytical eclecticism.

(4) Lastly, SMAS's focus on micropolitics, contingency and empiricism not only make it difficult to devise a sensible conceptual framework but also identify, critique and address systemic and recurring problems (Koddenbrock 2015: 247; Feenberg 2017: 644). Even if we accept micro-empiricism and sensation in itself as useful to make sense of the world, in terms of research practice one necessarily makes a selection to include some observations while excluding or overlooking others (Fine 2005: 95-96; see also Rekret 2016). A conceptual framework makes explicit what is included and excluded while retaining an interpretive flexibility towards the empirical data. Given the centrality of SMAS to the framework, the micro level, arguably, predominates. This, however, does not prevent the analysis to be applied to other cases of technologized security governance or make attempts at generalizations. Empirically rich and in-

depth accounts are fit for generating theories and generalizations where other approaches fail (Wedeen 2010; see also Hönke and Müller 2012; Dittmer 2014; Müller 2015). In any case, the level of analysis does not necessarily imply the potential for generalizations as macro-analyses of state behavior can be as idiosyncratic as ethnographic accounts (Krause 2013: 143). In short, with respect to the micro-macro problematique[16], the thesis favors research pragmatism over extreme positions (cf. Rammert 2012). Certainly, socio-material scholars and other proponents of contingency and micropolitics are right in pointing to the hazards of reification of objects such as the nation-state, the market or borders (Nexon and Pouliot 2013). However, it is held that these objects and their effects are accessible through empirical research without accepting them as homogeneous, consistent and determining forces (Krause 2013: 147). As a consequence, the conceptual framework is not conceived as a bureaucratic form to sort data points into abstract categories. Rather, it is a middle way that in broad strokes guides the focus of analysis while encouraging a grounded approach to the empirical data that allows for variation and interpretation.

3.3. The Conceptual Framework: Technologized Security Governance

Scholars have observed a technologization of security. Two contributions explicitly discuss the notion in further detail, i.e. Ayse Ceyhan (2008) and Stefan Kaufmann (2016). After a discussion of technologization, the section outlines the thesis's definition of technologized security governance to formulate an approach that usefully captures how and why technologies become enrolled and stabilized into security governance assemblages and to what effects.

3.3.1. Earlier Uses of Technologization

According to Ayse Ceyhan's (2008) definition, the technologization of security refers to "the making of technology the centerpiece of security systems and its perception as an absolute security provider" (Ceyhan 2008: 102).[17] She argues that the way how biometrics have emerged as the principal means of personal identification is a case in point for a global process of technologization that emanated in the United States in the 1980s and since then has spread to the European Union and other developed countries (Ceyhan 2008). Such an understanding serves the purpose of highlighting the central role of technology in security governance. However, three critical remarks are in order. First, the attempt to identify a beginning of technologization in the last quarter of the 20th century misses the centrality of many earlier technical devices to complex security arrangements including means of transportation, communication and violence. In doing

[16] Despite its prominence in social science research, the distinction between the micro and the macro lacks definitional precision. For attempts in illustrating the division see Krause (2013) for Sociology and Solomon & Steele (2016) for International Relations.

[17] Benjamin Muller (2009) also identified process of technologization in his research on risk management strategies at the border. However, he draws on Ceyhan's understanding without significantly altering it.

so, it reveals an understanding of technology as novel, high-tech or digital. This risks ignoring the often messy, discontinuous and locally contingent history of technologies as well as the effects of more mundane artifacts and techniques in global security (Amicelle, Aradau, and Jeandesboz 2015). Second, making the case for a global diffusion Ceyhan (2008) largely situates technologization at the societal or macro level. This suggests conceptual similarities to equally abstract phenomena such as globalization. Although they serve as useful catchphrases for complex large-scale developments, there are clear limitations for rigorous empirical analysis and inquiries into why, which and how specific security problems are technologized. Third, making technologization dependent on its perception as "absolute security provider" (Ceyhan 2008: 102) appears too rigid because it ignores the fundamental volatility of security governance assemblages. As will be argued below, security governance arrangements need to be performed constantly in order to function and thereby always carry the risk of producing new controversies and falling apart. Moreover, apart from the difficulties of measuring when a specific arrangement provides absolute security; Ceyhan understands technologization as a binary concept in that security governance is either technologized or not. This eschews the possibility of variance since security practices or mechanisms can be more or less dependent on technological input. Because in the end, technologies themselves are embedded in complex security governance networks and in turn are related to other human and material components in different degrees to adequately operate.

Kaufmann (2016) does not offer a concise definition of technologization. Similar to but not referencing Ceyhan, however, he describes it as a widespread phenomenon in security with a clear starting date – inviting similar critique. Particularly, he points to a post-9/11 environment that had not only seen a growing "reflection on the intrinsic vulnerability of liberal societies" (Kaufmann 2016: 77) but also the emergence of markets for security technologies. Unsurprisingly, then, Kaufmann limits the discussion to modern and mostly digital technology with a specific focus on surveillance. Different from Ceyhan and more in line with socio-material thinking, Kaufmann decidedly understands technology as embedded in human-material relations. As a consequence, technologization does not invariably determine security practices but he highlights the power of the individual to interpret and (re)act to technological affordances. Generally, his take on technologization is strongest when he summarizes various possible conceptualizations of security technology:

> *"Security devices function as a normative way to harden societies. At the same time, their use triggers the potential for action, bringing about opportunities to adjust, bend, and deactivate rules, and may have unintended consequences. Furthermore, we must consider that security*

devices can also be an essential component of group-specific self-understanding and external understanding and of radically changed practices" (Kaufmann 2016: 93).

He stops short of integrating the different perspectives but they remain next to each other as separate registers. In short, Kaufmann provides an overview of different modes of thinking about security technology that spans across scales and topics. As a result, instead of compiling an analytical framework for technologized security governance, his article serves as a useful starting point regardless whether one is interested in the micro or macro effects of technology, security practices, path dependencies or identity research.

3.3.2. Technologized Security Governance

Building on these contributions, technologized security governance places technology at the center of an assemblages of different kinds of security actors. As such, it is both conceivable in state-dominated as well as solely non-state settings that both enroll sophisticated technology or more mundane artifacts. In principle, the state-led U.S. drone campaign to fight global terror can be studied as an instance of technologized security governance just as the use of satellite imagery by civil society during humanitarian disasters or new filing systems and standardized medical techniques to determine the status of migrants in refugee camps.

Following the common proposition of Critical Security Studies (see chapter 2), this thesis understands security as an essentially contested concept. This is not to say that security can mean anything but that its meaning results from negotiation processes or controversies among different actors. Following Peer Schouten (2014a: 23) "[s]tudying security as controversy means refraining from making a priori assumptions about the ontology of (in)security, instead considering it as itself at stake in – and hence the outcome of – security governance efforts." Security as controversy implies that the very creation of a security threat, its problematization, is already a part of security governance. In this line of thought, security governance emerges from the bottom-up. Instead of a central authority – usually a government – that publicly declares a security threat, security governance can emerge out of decentralized assemblages of various types of (non-)state actors and things. As a result, multiple security governance assemblages might exist in parallel addressing the "same" problem through different practices such as monitoring and surveillance, knowledge production, public advocacy, naming-and-shaming, diplomatic statements, sanctions or positive incentives right up to the use of military force (Avant and Haufler 2012; Chandler 2016).

In all instances, the following framework provides the conceptual vocabulary to understand how technology problematizes a security threat, stabilizes assemblages and affects goals, and what effects this brings about.

3.4. Problematizations in Security Governance

3.4.1. What is Technology?

Although the definition of technology warrants a whole book by itself, it is useful to outline the thesis's understanding to further situate the conceptual framework between classic security governance and SMAS. The sub-section makes three contrasting moves against definitions that take technology as a neutral instrument, a determinist force and an unbounded assemblage of human-material relations that disintegrates in its environment. The goal is to arrive at a pragmatic take on technology that accepts its relationality in terms of rules, laws, discourses, institutions, other materials and human beings but does not unrecognizably conflate them. There is certainly no way of arguing that these heterogeneous elements are unimportant or do not partake in the design, use and effects of technology. But in socio-material thinking it is increasingly difficult to set technology apart from these very elements so that it is useful to retain the idea of technology as an object and material artifact. The strength of SMAS is the focus on relations that highlights the complexity and situatedness of technologies. "But," following Ian Hodder (2014: 25), "it is also the case that materials and objects have affordances that are continuous from context to context. These material possibilities (whether instantiated or not) create potentials and constraints."

Thus, technology is conceptualized as a material object that imbues its various relations with certain potentials and constraints which are actualized or not but at least exist as virtual possibilities. Acknowledging the materiality lifts it out of the heap of human-material relations. Moreover, the idea of potential is not a far cry from socio-material understandings that highlight the technological affordance inherent in assemblages (Dittmer 2014: 388; Kinsley 2014: 365): Speaking of potentials, capacities or offerings of technology removes the material determinism while the propensity of which potential is actualized remains empirically open (Dittmer 2014: 392). However, socio-material research seems to highlight the unlimited potential of relations in lieu of the material constraints that channel, order and fixate human actions (Hodder 2014: 33; Breu 2016: 21). Conceiving technology as a material object rectifies this imbalance to point out that technology both "enables some activities while rendering others difficult or impossible" (Jasanoff 2016: 8; see also Pouliot 2010: 299) which, for example, sets the boundaries of what is considered governable (Mayer and Acuto 2015: 672) or possible and legitimate in warfare (Shaw 2017: 459). At the same time, it opens the possibility of a goal-orientation or purpose of technology that stops short of instrumentalism. Instead, speaking of potentials and constraints recognizes that there are differing propensities of what is routinely and expectably actualized. Put simply, technology is more often used in certain ways than others (cf. Amicelle, Aradau, and Jeandesboz 2015). Lastly, although this thesis looks at a sophisticated technology, the definition is open enough to accommodate mundane artifacts such as manual record systems, folders, forms or paper maps.

3.4.2. Who Acts? Blurring Distinctions

The question of agency or who acts and who governs security often falls behind in poststructuralist research that rather focuses on rationales or how something is governed (Rothe 2015: 108). In contrast, both classic security governance and SMAS put a great emphasis on the actors agreeing with Bruno Latour (2005: 72) who makes it the essential starting point of any "science of the social." Moreover, they share a tendency – albeit in different degrees – to not only extend the circle of involved actors far beyond the nation-state but to blur the relations between the public and the private and the human and the material (see chapter 2). Security governance scholars come to the conclusion that preconceived notions of a public/private distinction are increasingly difficult to apply in the empirical world (e.g. Abrahamsen and Williams 2011). Anna Leander (2014: 201) even contends that the analytical distinction impedes research and blocks the view on hybrid networks of actors. SMAS go one step further and dissolve such distinctions, including the human/material divide, at the beginning and conceptualize them as effects of heterogeneous relations (e.g. Brandenburg 2017). In similar ways, both research programs are dissatisfied with the bad performance of those analytical distinctions and turn to empiricism to reach better and more nuanced accounts. Conceptually, there are various attempts at capturing this indivisibility and blurring such as heterogeneity, cyborg, hybrid or intra-action (e.g. Harraway 1991; Jasanoff 2004b; Latour 2005; Barad 2007; Feenberg 2017).

The efforts and goals of overcoming the human/material and public/private dualisms are understandable and laudable given the empirical complexity. However, the doing of research and writing about security governance renders it difficult to sustain the indivisibility, which warrants the question about its pragmatic benefits. Moreover, a disregard of bounded actors complicates issues of responsibility and accountability in security governance. Lastly, the very ideas of cyborgs or hybrids reify the distinction of at least two sides blending into one another (cf. Sørensen 2009: 60). It is important to keep in mind the intricate relationships across divides; but the conceptual divisions still make sense in order to not only talk about the empirical blurring of public/private and human/material distinctions themselves but also about their varying degrees in different cases. In short, there is still an analytical utility in distinguishing material and human factors as well as public and private actors.

3.4.3. Sacrificing Material Agency

Where does this leave material agency? It is a central pillar of SMAS that takes issue with conceptions of "[a]gency [..] as a residual category naming a natural inborn capacity of human responsible beings that enables them to resist the stubborn natural relations and the demands of structural forces" (Passoth, Peuker, and Schillmeier 2012: 1). Material agency as put forward by socio-material scholars in Security Studies and elsewhere question the assumed autonomy of

human action arguing that even everyday practices are entangled with objects. From the beginning, however, material agency was an unfortunate choice of words. It reifies the human-material distinction and too easily suggests a conflation with the common-sense understanding of human agency as intentional action (Sayes 2014: 143). Deliberately or not, this provocative and divisive formulation arguably prevents more differentiated discussions but forces socio-material scholars to consistently justify its use and clarify its actual meaning. Because "at its most basic, the insight is hardly a radical one. All it is saying is that matter exerts force and resistance. In short, matter matters. The fact that we can't see this as a relatively straightforward claim suggests the continuing power of correlationism and, even more, social construction as doxa" (Breu 2016: 13). In this sense, material agency is already thought in a distributive manner being the effect of a human-material assemblage. It is difficult to consistently sustain a human-material simultaneity when agency is adjourned to the empirical analysis and only cryptically comprehensible as "a relational, ever-changing outcome of its enactment" (Passoth et al. 2012: 4). With this in mind, material agency has perhaps been a necessary provocation to put the force of matter on the agenda of social scientists but has reached its limits of being analytically helpful. Other socio-material scholars or those sympathetic to its ideas have come to similar conclusions when they re-make distinctions between material and human agency to save a sense of reflexivity and intentionality (Coole 2013; Dittmer 2014: 389), voice fears of exaggerating the efficacy of matter (Squire 2015: 150) or contend that it "can easily be blamed for being a theoretical fiction or a rhetorical trick that does not lead to new insights" (Rammert 2012: 95).

Corresponding with the definition of technology, the force of matter is best understood as affordance. While the impact of materiality on relations and practices is maintained, it leaves human intention intact albeit it might be negligible in some situations. Thus, it is still useful to think of agency as distributed across assemblages of humans and things (Folkers 2013: 29). Instead of risking to dissolve human agency in an "ever tighter imbrication of human and machine in the global battlespace" (Bousquet 2017: 30), the framework emphasizes that agency is not equally distributed and that human beings tend to actualize potentials and resist constraints to varying degrees. In this way, there is no "agency ex nihilo" that "begins with a body moved by a mind" (Rammert 2012: 91) but human actors are always already meshed in various material relations that make offerings and impose requirements so that "[d]ifferent kinds and degrees of autonomy may therefore be found in relation to different areas of interdependency with the world" (Rammert 2012: 92; see also Barry 2001: 11).

3.4.4. Problematization: Co-Production of Security Threats

Based on these reflections, the first concept of the framework, problematization, captures the human-material co-production of insecurities. Central to technologized security governance is the

bottom-up creation of a security threat that requires attention by security actors and technologies. Problematization highlights the role of material objects in the shaping of security problems and how technologies enroll actors around it into a security governance assemblage.

Across theoretical schools, (security) governance scholars frequently assume that there is an agreed upon problem and then focus on how a solution is manufactured, which security practices or norms are promoted, and how effective they are (e.g. Bueger 2016; Carpenter 2016a; see also chapter 2). In short, the focus is on governance at the expense of security (Ceccorulli, Frappi, and Lucarelli 2017). Limiting security governance to solutions risks depoliticizing the emergence of security threats. Turning security governance on its head requires starting with the problematization of security. Three notable exceptions that propose a similar approach interestingly all focus on climate change as a governance problem in general (Allan 2017) or a security problem in particular (Mayer 2012; Rothe 2017). Variously drawing on concepts from STS they argue that the constitution of governance objects is fought over by different actors and technologies and shapes how they are governed. In short, security threats do not exist independently from the actors and technologies that choose to attend to them but they are actively constructed. In this regard, Michael Dillon and Julian Reid (2001: 52) provide a succinct and instructive definition of problematization:

> *"The emergence of a new, politically valent, security problematic is necessarily a complex phenomenon. It is not simply determined by the recognition of new needs by established political subjects whose structures and attributes are presumed to pre-exist the relations of force, knowledge and power that constitute them as the very specific subjects of power/knowledge that they are. Given the intimacy of the correlation of power and knowledge, the emergence of new problematisations is profoundly influenced by the complex interplay of epistemic invention and technological innovation, and by the relations of force, knowledge and power that define life and delimit populations."*

They clarify that security threats are not the result of negotiation processes among actors with preconceived norms and interests. Instead, security problematizations are better characterized as (1) complex human-material interactions that (2) involve the potentials and constraints offered by technologies and (3) dynamically assemble a group of actors. These three aspects are addressed in turn.

Co-Production: Complex Human-Material Interactions

Technology is no neutral instrument but "enables, limits, and redefines the ontological conditions for worlds" (Shaw 2017: 454). The concept of co-production is useful in this regard. It was coined

by Sheila Jasanoff (2004b) to argue that "the ways in which we know and represent the world (both nature and society) are inseparable from the ways in which we choose to live in it."[18] In this understanding, technologized governance and security threats co-produce each other as "a problematization already presupposes a solution or policy objective, a telos, in that it establishes a rationale regarding what is desirable or wrong in a particular situation" (Brandenburg 2017: 5; see also Allan 2017: 134). Drawing on the concept of co-production, Bentley Allan (2017) devises a three-step approach to show how the climate emerged as an object of global governance. First, what he calls designation describes the process of creating an object as distinct from others – in his case to distinguish climate from weather. Second, the object must be made intelligible not only to expert communities but governments and the (global) public. Third, drawing discursive-material connections to known threats and concerns problematizes the object and finally renders it in need of governance, e.g. linking climate change to food security, national security, biodiversity etc. (Allan 2017: 136-138). Although he focuses on climate governance, his approach is instructive for an analytics of problematizations in technologized security governance. However, his focus largely remains on the importance of science as knowledge production for the emergence of the climate as governance object. Therefore, the following paragraphs discuss the distinct role of technology in the co-production of security threats.

Technologies at the Center of Assemblages

The choice of technology also mediates the relations within a security governance assemblage: It impacts who becomes part of the assemblage, sketches out specific roles and affects the respective power distribution (Brandenburg 2017; Bueger and Gadinger 2014): An actor constellation surrounding surveillance drones likely differs from one focusing on surveillance satellites. Especially high technology might require a certain expertise, investment or technical support and, in doing so, elevates some actors to become obligatory for the assemblage to function. With that said, technologies become an analytically fruitful starting point for tracing the participants of technologized security governance (cf. Avant and Haufler 2012: 274). While many studies start with an assumed network of actors, looking at the initiation reveals how "agents actively shape their network position and the overall qualities of the networks they participate in" (Avant and Westerwinter 2016: 12). As a result, such an approach can depict early attempts at security governance that over time either fall apart or enroll new actors and technologies, stabilize and in

[18] Related concepts found in Security Studies are ontological politics or enactment. The former draws on Annemarie Mol's work (e.g. 2002) to denote the constitution of objects of governance as distinct from their discursive representation. In her balanced assessment of enactment, Vicki Squire (2015: 149) "conceives [enactment] as an onto-epistemological move of political significance, which implies a shift away from the epistemological concern with perspective in terms that allow an appreciation of boundary formations in terms of the co-constitution of 'subjects', 'objects' and 'environments.'"

the process re-constitute the security threats they address. In sum, problematization embraces the complex initiation of security governance assemblages as an ongoing controversy about the security threat itself as well as the practices, actors and technologies suitable for addressing them.

3.5. Stabilization of Security Governance

3.5.1. Of Relations and Assemblages

Relations form an essential component of how this thesis understands technologized security governance. They are distinct from connections. They describe a more distant, indirect and mediated contact while connections emphasize immediacy, locality and corporeality. As such relations are particularly apt in an analytics of technologized security governance. They grasp the abstract complexities of transnational norms, actors and practices without clearly delimited time or place (Feldman 2011: 379). However, relations are not a sufficient conceptual vocabulary to talk about wholes – such as technology, satellites, the nation-state or an NGO – no matter how fragile or temporary such entities might be. Up until this point, the assemblage terminology has been used relatively nonchalantly although the previous chapter pointed towards some differences to actor-networks. Therefore, it is necessary to re-assess and explain the thesis's choice of assemblages over actor-networks.

Arguments Against ANT…

While relationality is often highlighted as a central theme of both assemblage thinking and ANT (Breu 2016; McCourt 2016), this can be misleading. The difference is in ANT's rigorousness to accept entities as only defined by their relations; they exist through their relations in the network. As a result actors do not travel across networks and retain their identity, they effectively are different actors in different situations (Sørensen 2009: 53; Bueger and Gadinger 2014: 46). Moreover, Latour's extreme position on empiricism that only accepts traceable relations not only negates the option of virtual affordances that have not yet been realized but also complicates the importance of history, memory and path dependency as relations may only exist for a moment in their actuality (Baron and Gomez 2016: 141; Feenberg 2017: 645). These aspects contradict the definition of technology as well as the maintenance of human agency outlined above. Lastly, related to the uncompromising propositions of ANT and a vigilant followership, invoking actor-networks would put a considerable burden on a project that advances a flexible and eclectic analytics of technologized security governance.

…and For Assemblage Thinking

Assemblage thinking, on the other hand, has until now largely escaped ANT's fate and remained a rather versatile and pragmatic concept (e.g. Abrahamsen and Williams 2011; Berndtsson and Stern 2011; Sassen 2006). Moreover, it addresses the drawbacks outlined above since it retains

the idea of relatively independent entities that can be part of multiple assemblages at once. Certainly, actors are impacted by their participation in different networks, however, their very ontology is not limited to the relations in one given network (Harman 2014; Müller 2015):

> *"If assemblage theory wants to be a flat ontology, it cannot also be a relational holism, since it must grant autonomy to the various pieces of the cosmos rather than placing them amidst a harmonious whole. Nation-states, security guards, passports and citizens must not be defined by their relations, since they need to be able to enter and exit various relations at different times"* (Harman 2014: 122).

Since the single components of any assemblage are free to associate outside their existing relations, they retain a sense of substance, surplus or agency that cannot be explained by the sum of their current relations (Dittmer 2014; see also DeLanda 2009). Moreover, "the most significant gulf between ANT and assemblage thinking is thought to be ANT's preoccupation with the actual vis-à-vis the preference for the virtual in assemblage thinking" (Müller and Schurr 2016: 219). In short, assemblage thinking admits non-actualized potentials and capacities beyond the empirical tracing of relations, which is in sync with the definitions of technology and material agency. Maximilian Mayer and Michele Acuto (2015: 667) prefer the more haptic and tangible large technical systems (LTS) over assemblage thinking to introduce a technological sensitivity into global governance. However, despite LTS's benefits for thinking about critical infrastructure and similar transnational formations, assemblages remain open enough to accommodate smaller, more mundane groups of actors and technologies involved in security governance.

Stabilization: The Blind Spot of Assemblage Thinking

One shortcoming of assemblage thinking against ANT is the idea of stabilization. ANT mainly works through empirical case-studies[19] to develop various conceptual tools and make sense of the instability of facts, norms and other entities such as science, the nation-state or security threats. On the other hand, "[w]hen assemblage thinking is used to provide accounts of the stabilisation of relations, it faces one key shortcoming: its conceptual apparatus is underequipped to deal with the multifarious ways of assembling at anything else than a very general and descriptive level" (Müller and Schurr 2016: 220). Therefore, the remainder of this section deals with this shortcoming. In doing so, it outlines the thesis's understanding of instability and relations as a precursor of defining stabilization as the second central concept of the framework.

[19] In fact, one of its major proponents, John Law (2009: 141), argues that while it is possible to describe ANT in the abstract "this misses the point because it is not abstract but is grounded in empirical case-studies."

3.5.2. Reining in Performance and Instability of New Materialism

SMAS highlight that assemblages cannot be taken for granted but need to be actively performed to remain stable. Accepting security as essentially contested also implies some volatility concerning the constitution of threats and how they are addressed. As a consequence, security governance arrangements are only stable as long as actors agree on their position and practices in relation to the specific security problem (Avant and Westerwinter 2016: 16; Ceccorulli, Frappi, and Lucarelli 2017: 61). Performance as conceived here does not only pertain to the effects of a given assemblage (Sørensen 2009: 15) but how something is brought into being, or how relations of governance are kept in place (Bueger 2013: 340).

Instability Radicale

SMAS and especially ANT carry the idea of performance and instability to extremes where "assemblages last for only an instant, perishing in favour of a close successor that is not, strictly speaking, the *same* assemblage" (Harman 2014: 125; emphasis in original). Scholars are eager to emphasize that assemblages are fluid, in flux, contingent, mutable and characterized by flows, flexibility and instability (see chapter 2). This rests on the realization that stability is hard work. While we are used to continuity in the form of electricity in our office, coffee at every corner and lunch in the cafeteria such everyday expectations are the result of global assemblages of production, trade, transport, certification and so on. Similarly, some socio-material scholars draw on the natural sciences to show that Newtonian ideas of stable masses have long been amended: Mass is active in form of vibrant atoms, protons and electrons and, thereby, not stable but malleable (Hodder 2014: 21). ANT follows the core slogan of STS that "it could be otherwise" (Woolgar and Lezaun 2013: 322). It is only the relational practices that give the appearance of stability so that "realities only exist in the practices that materialize them" (Law 2010: 180).

Instability Normale

In principle, the thesis accepts the assumption of instability of assemblages but certain problems occur when it is taken too far. When reality is all-contingent and the result of fluid, unpredictable inter- or intra-actions, then it is not accessible through any theoretical abstraction or conceptual framework (cf. Chandler 2017). John Law (2009: 151; emphasis in original) declares the end of "*construction*, social or otherwise: there is no stable prime mover, social or individual, to construct anything, no builder, no puppeteer […] Rather, we are dealing with *enactment* or *performance*. In this heterogeneous world everything plays its part, relationally." Such an understanding usefully points to the situatedness of notions such as the market or security. But it conceals that (re-)construction is alive and well in the form of the researcher. The researcher remains in charge of tracing, categorizing and constructing while drawing on implicit theoretical notions of habit,

experience and practice. Assembling also means excluding stuff that is less relevant for the specific account. A conceptual framework is about making those choices more explicit which requires to accept a certain stability or endurance of things. This is possible because although it might require a lot of work, some entities are more stable than others. New materialism's repeated insistence on volatility and performance has

> *"yielded a great deal of stress on contingency and chance. Yet importantly, I think, this does not a priori rule out a quotient of inertia or more or less enduring continuities – such as patterns, path dependency, institutions, systemic logics – whose turgidity and congealing remain particularly important for the analysis of power. It is just that none of these more lasting forms are guaranteed, unassailable or as stable as they might appear. They need always to be reappraised within any particular context, along with their underlying ontological assumptions, lest they become reified or taken for granted"* (Coole 2013: 453).

Following Coole's assessment means to retain the assumption that stability is not the norm and be wary of reifying entities without recourse to its performance (see also Nexon and Pouliot 2013). But treating everything as equally in constant flux does not do justice to the hard work that keeps certain assemblages, practices and effects more durable than others.

In order to accommodate a view that some relations are more durable than others, it is useful to acknowledge varying degrees of stability of assemblages. The radical contingency of relations as proposed by ANT is criticized for being blind to the force of historical processes and large-scale phenomena such as race, class and gender inequalities (Bueger and Gadinger 2014; Nexon and Pouliot 2013). Arguably, these dimensions have been sacrificed for the mission of revealing the efficacy of matter in the study of the social. Having achieved this, it is time to move on from demonstrations of materiality to the study of the different ways this plays out (Baron and Gomez 2016; Grove 2016: 3).

3.5.3. Stabilization and Anchors

Once a problematization of security is established and actors assemble around a technology, it becomes important to ask why some assemblages prevail and others fall apart, or what stabilizes technologized security governance. Moving away from ideas of common interest of classic security governance, stabilization emphasizes the role technologies and routinized practices assume in the workings of an assemblage. Technologies are open to various usages but not indefinitely malleable according to the will of human actors. As a consequence, they impose a certain propensity and stability on specific relations and practices. They become anchors within a security governance assemblage. Those technological anchors invite repetitive practices that rather conform with habits, technical affordances or norms leading to routinized practices within

an assemblage. Taken together, stabilization locks in certain goals and responses of security governance assemblages that become resistant to change and bring about durable effects.

Objects as Anchors

Objects constitute the first analytical site of interest for stabilization processes. Building on the premise that "technology is society made durable" (Latour 1991), one could think of specific objects or material devices as cementing coordination practices among actors which become more difficult to change. Recalling that stability is not the normal state of assemblages, technology plays an important part in stabilizing and prescribing preferred relations and practices because "if order requires resisting inherent transformation, then ordering – stabilizing relations – is most effectively done exactly when the 'actors' are *not* human" (Schouten 2014b: 86; Callon and Latour 1981). This resistance to human agency is what Ian Hodder (2014: 19) calls the "darker side" of human-material relations as objects entrap human individuals – effectively limiting or even prescribing certain practices. Amending the neutral notion of relation, he argues, it is dependence that frequently characterizes human-material interactions "whether these be the victims of the AIDS virus, the work gang bound by chains, the women bound by child-rearing, or the populations bound by global agricultural systems" (Hodder 2014: 33). Thus, material objects or technologies become anchors in human-material assemblages that have a stabilizing function in that they are binding actors together and impose potentials and constraints on their relations.

Material anchors are stabilizing because they are themselves manifestations of historic relations, human interactions, inscribed norms, expectations and past uses. They are hardened practices and in this way "necessary stabilizers of the human collective" (Sayes 2014: 137; see also Nexon and Pouliot 2013: 344). Materials so to speak are the extension of practices in that they invoke the same practices, expectations and norms across contexts. This is related to what Latour (1987: 227; 2005: 223-227) calls "immutable mobiles" that retain their form in various settings. They can be scientific papers, NGO reports, ceasefire agreements or particular people as well as more sophisticated technologies or devices. Once they are enrolled into an assemblage they share the tendency to have patterning effects (Law 2010: 181). Moving beyond that, it would be misleading to assume that any material anchor has equal stabilizing effects. Rather, it is important to note the historical investment, relational baggage and complexity of a technology. For example, an ad-hoc paper-based registration system in a refugee camp might lead to a temporary stabilization of an assemblage as it requires some expertise and familiarity with the procedure. On other hand, a registration system based on biometric technology might draw in economic and scientific stakeholders, global biometric databases, intelligence and security agencies, certification programs etc. Different material anchors vary in their capacity to not only pattern specific

practices but also stabilize security governance assemblages by drawing in additional materials and actors that in turn bring with them additional authority, power and interests. As a rule of thumb, one might say that larger assemblages tend to be more stable.

Routinized Practices

Practices are the second analytical site in stabilization processes. In a sense, SMAS are as much about practices as they are about relations because "materiality cannot be prised apart from the enactment of relations or, more generally, the practices that do these relations" (Law 2010: 173). While their theoretical foundations might differ, this is also an interesting converging point that brings together classic security governance and practice theory. Deborah Avant and Virgina Haufler (2012: 274) argue that regular interaction among actors can contribute to form common goals and practices and, thereby, contribute to the stability of security governance. Practice theorists, on the other hand, accept this stability only as temporary or "an illusion created by the recursive nature of practice" (Adler and Pouliot 2011: 16). In sum, practices are constitutive of assemblages so that their repetition or routine becomes a useful indicator for their stability and goals.

To recapitulate, technology is defined as a material object that offers potentials and constraints for its usage. As actors actualize different potentials, technologies routinely and effectively serve varied goals and purposes. For example, some use drones more commonly for surveillance, others for targeted killing, and still others for package delivery. As a result, which technologies are enrolled in the problematization of security co-determines the goals. Absent preconceived interests and norms of security actors the choice of technology becomes an indicator for which goals the security governance assemblage pursues. Similarly, it is possible to identify various security governance assemblages that emerge around the same technology but highlight different potentials.

At the same time, the researcher needs to be wary of particular barriers to stabilization or even targeted destabilization moves. For example, while an expansion of public surveillance through CCTV cameras draws in a large amount of financial interest, experts and various technologies, civil society actors, national legislation and political parties might function as barriers to the stabilization of such a technologized security assemblage. In short, however, the enrollment of material objects and routinized practices frequently stabilizes the coordination of security governance assemblages and enables the locking in of particular security practices and goals.

3.6. Technologically Maximizing Goals

3.6.1. Legitimation Practices

Problematization captures parts of the ways in which technologized security governance is rendered desirable and legitimate. Before discussing the consequences of technologized security governance, the chapter deals with the notions of legitimacy and accountability both of which are considered effects rather than properties of security governance. For this, it is helpful to outline the overlap between classic security governance and SMAS.

In more classic accounts, legitimacy is frequently seen as a problem of security governance because it moves beyond the legal comfort of the (Western, liberal) nation-state where legitimacy is assumed to be almost naturally located (Bäckstrand and Kylsäter 2014: 332; Daase and Friesendorf 2010). The proliferation of (non-state) actors discards the idea of national democratic oversight so that privatized security governance draws its legitimacy from successful outcomes, i.e. output legitimacy (Bexell 2014: 292; Daase and Engert 2008). Although classic security governance, thereby, embraces legitimacy as performative, relational and contingent on results, it tends to retain measurements closely related to ideal-typical, state-like legitimacy that take it as a property of actors emanating from differing sources such as charisma, tradition, expertise etc. (Avant, Finnemore, and Sell 2010b; Barnett and Finnemore 2004; Weber 2002). In technologized security governance, this suggests adding another dimension of technological authority. However, this retains legitimacy as a property of technology. It does not register practices that appropriate science and technology for legitimating purposes.

SMAS also promote the ideas of performativity, relationality and contingency and focus on how technology infuses legitimacy into a security governance assemblage. More specifically, many socio-material studies take an interesting understanding of representation to denote how one specific actor or thing can authoritatively represent the whole assemblage (Bueger 2013). For example, how a visual image of a polar bear or a document like the assessment reports of the Intergovernmental Panel on Climate Change (IPCC) become the recognized spokespersons of global warming. Most importantly, SMAS turn legitimacy research into an empirical task and trace the various relations of how someone or something emanates as a representative of the assemblage. Surely, this is a useful approach for technologized security governance because it reveals the importance of science and technology for the perception of security practices as neutral, objective and unproblematic. Such analyses, however, usually take the effect of legitimacy as a starting point and then backtrack its emergence.

Both perspectives embrace process, relations and the distribution of actor relations within governance arrangements. The conceptual framework removes legitimacy as a categorical property as unhelpful and focuses on legitimation practices that stabilize governance structures.

Legitimation denotes the process by which certain actors or things seek legitimacy which can be studied by analyses of their legitimacy claims (Andonova and Carbonnier 2014: 352; Bäckstrand and Kylsäter 2014: 332; Olbrich and Shim 2019). In doing so, the approach is capable of capturing attempts at making a security governance assemblage appear legitimate including through reference to data (Leese 2014), science (Jasanoff 2017), visuality (Saugmann Andersen 2017: 5) or sheer materiality (Barry 2013a: 145-147). The approach reveals the "microfoundations of global politics" (Avant, Finnemore, and Sell 2010: 357) in order to account for the varied – potentially contradictory – sources of authority and how they come into being without pre-categorizing them. Moreover, it acknowledges the variation in degrees of authority that can be conferred by different audiences (Avant, Finnemore, and Sell 2010: 360). In doing so, it embodies the idea of controversy as various actors and things might issue legitimacy while others set out to challenge or delegitimate particular legitimacy relations.[20]

3.6.2. Dissolving the Accountability Trap

Accountability is a central feature of security governance in order to increase legitimacy and effectiveness. The diversification of actors beyond the nation-state does not necessarily increase acceptance of governance and can complicate questions of accountability. This is not only related to the sheer number of actors but also growing tendencies to include experts by virtue of their specialized and politically disinterested knowledge outside of democratic procedures (Barnett 2016: 135). In any case, classic security governance struggles to retain individual responsibility as a "necessary illusion" for the construction of legal accountability (Rammert 2012: 93).

SMAS do not accept the necessity of this illusion and instead emphasize how technologies are entangled with human actions. This gives rise to an accountability trap because material actors are influencing outcomes of security governance but do not hold particular intentions, aims or a purpose. However, if there is no intention or reflexivity involved in socio-material practices it becomes difficult to hold them accountable. It denotes a further fragmentation or dispersion of accountability across human non-human entities (see also Jasanoff 2016: 41). Established social organizations struggle with the human-material entanglement and its consequences for responsible action: For example, Derek Gregory (2011: 208) finds that singling out drone operators for undesired or even harmful consequences "obscures the structural effect of a military apparatus and political technology that viscerally immerses physically remote operators in combat and reinforces their sense of communion with troops on the ground." In relation to this accountability trap, two main themes are identified in socio-material studies. First, forms of

[20] Importantly, academic researchers can become a passive and active part in such legitimacy controversies of technologized security practices as they are either enrolled by security actors and technologies or actively deconstruct or critique forms of technological practices.

technologized security governance do not absolve the researcher from seeking out the distributed agencies at play.[21] Second, determining the distribution of accountability is an empirical question (Rammert 2012: 91; Dittmer 2014: 397) which among other things, however, is dependent on access to relevant stakeholders.

Socio-material scholars might also invoke that it is not their task to deliver concepts of accountability in sync with legal proceedings but to problematize the role of technology in security governance. Accountability, then, comes down to political judgment whether to acknowledge the socio-material entanglement or strategically ignore it for the benefit of having humans to blame (Bennett 2005: 464). However, given the high stakes involved in security governance, it is expedient to think about ways to avoid the accountability trap inherent in symmetrical concepts of agency and grasp individual responsibility. Moreover, in debates about global security but also climate change, the anthropocene and environmental destruction, it becomes ethically and politically important to not lose sight of human responsibility:

> *"Having rejected vertical or dualist ontologies, then – and this rejection may itself pave the way for a more bio-/eco-centric environmentalism – it is still important to hold human beings accountable, in a material if not in a moral sense, for the destructiveness they are wreaking on vulnerable eco-systems and to acknowledge the importance of cultivating agency – ethical or political, individual and collective – to tackle it"* (Coole 2013: 461).

The quote shows, Diana Coole (2013) goes further than other socio-material scholars (e.g. Bennett 2010; Latour 2005) in retaining a sense of human uniqueness. Here, it is again analytically useful to retain the human/material distinction. One central distinctive feature lies in the reflexive capacity of human beings who are – in contrast to material objects – not indifferent to the results of their actions (Coole 2013: 460). This way acknowledges the important contribution of new materialism for re-centering analytical attention to technology in security governance, the imbrication of human and material agents and the distribution of agency while not abandoning the political responsibility of reflexive, human beings altogether.

Retaining reflexivity as a meaningful distinction between human and material actors undermines the accountability trap. In more pragmatic and instructive terms, Bennett (2005: 464) wonders whether "the responsibility of individual humans may reside most significantly in one's response

[21] Although Rune Saugmann Andersen (2017) argues with respect to the role of video algorithms in securitization that it might be preferable to hold whole assemblages accountable. In particular, he points towards the broader conditions and power distributions that make certain practices possible. However, although this is a useful proposition, it does not solve the accountability trap and excuses individual responsibility.

to the assemblages in which one finds oneself participating – do I attempt to extricate myself from assemblages whose trajectory is likely to do harm?" (see also Bennett 2010). Doing so accepts the reflexive capacities of human beings while acknowledging the role of material objects and technologies they are entangled with. It cautions against unidimensional, simplistic accusations and stresses the importance of responsible and reflective human behavior. Lastly, it is a call to accept, or endure, contingency, complexity and ambiguity when it comes to assigning political responsibility.

3.6.3. Durable Effects of Technologized Security Governance

The conceptual framework theorizes not only how to grasp the effectiveness of security practices in reaching pre-set goals but also the potential fallout of technologized security governance. Echoing famous contributions to STS (Winner 1980), SMAS excel in the analysis of hidden material ordering practices that affect social and political governance (cf. Marres and Lezaun 2011: 494-495). The materiality of security governance locks in security practices that become difficult to change but easy to transfer across contexts. A growing entanglement of security governance with material objects and technologies not only increases complexity but also makes it harder to roll back (Hodder 2014: 31). The realization that security practices are durable does not immediately explain the effects; they are not a stable cause that leads to always the same effects (Law 2010: 178). However, it is clear, that even in ANT stabilized assemblages facilitate the approximation of explanations although they still require in-depth empirical analysis (Latour 1991: 130): Stable, routinized security practices at least create the appearance of cause-effect relations which provide a useful analytical starting point to trace the durable effects of technologized security governance.

For this, three interrelated implications are theorized for the conceptual framework: First, technologized security governance is limited to the management of effects of insecurities and does not tackle their root causes. Second, technologized security practices often involve the objectification and quantification of those governed. Third, technologization is prone to maximize the goals of security governance leading to an expansion of security practices.

Security Governance as Effect Management

Technologized security practices are frequently directed at the material or bodily manifestations of insecurity as they are more susceptible to the detection, observation and treatment through technical devices. Body scanners at airports might deter and limit the number of dangerous goods on airplanes but do not tackle the motivations of doing so, just as CCTV cameras or radar traps only locally manage deviant behavior. This is congruent with the decentralized and bottom-up view of security governance: Technologized security governance copes with security threats instead of tackling the causes of insecurities and imposes governance on allegedly passive objects

instead of engaging them as part of a solution (Chandler 2016: 9-10 drawing on Lederach 1998; see also Kaufmann 2016).

Objectification of the Governed

In classic security governance, correlation of security practices and quantifiable change are employed to measure the effectiveness of security measures (e.g. Kirchner and Dominguez 2014; Webber 2014): This can take the form of assessing the number of kidnappings, troop movements, civilian deaths, reported misconduct etc. before and after the implementation of security governance. Parts of the rationale of technologized security governance are not too dissimilar from such assessments because of the important role of quantification and objectification in the governance through technologies. However, the framework goes beyond this narrow view in important ways and more flexibly includes unexpected reactions of those governed and additionally reflects on their very quantification and objectification itself. Technologization is about reducing difference (cf. Jeandesboz 2016). In this way, technology is akin to technocracy that works on the premise of generalizable, simplified knowledge of experts who apply it across a range of diverse circumstances without much democratic oversight (Barnett 2016: 140; Jasanoff 2016). Similarly, technologized security practices render the relation between the governors and the governed unidirectional, abstract and technical. Technologized security governance is indifferent to the feedback of the humans and things it is directed at. While human interaction is characterized by the expectation of reaction, "[t]echnical action represents a partial escape from the human condition" (Feenberg 2005: 48). This indifference originates from an objectification and quantification that has technologized practices not acting on the actual human being but on their virtual, non-human proxies. In doing so, security threats are framed in a particular way so that those aspects are neglected which are more difficult to quantify regardless of their significance for successfully promoting security (cf. Jasanoff 2016: 53). In sum, technologized security governance promotes the quantification and objectification of insecurities and thereby taps into discussions of (de)politicization (cf. Hegemann and Kahl 2016). In doing so, it renders the involved humans and things into passive recipients of governance, blocks alternative practices and viewpoints and potentially prevents the very solution of the security threat at hand.

Cycle of Technologization

Another effect of technologized security governance is the ongoing maximization of security. As technology stabilizes and locks in goals and security practices, there is a tendency to continually pursue further security by repeating the same practices. In this logic, ever more data is being collected for security reasons, CCTV cameras become increasingly spread in public and private places, the use of surveillance and attack drones is expanded to other geographic areas, and

biometric identification has moved from high-security facilities to smart phones. James Der Derian (2009: 199-200) captures this process when security (or democracy, human rights etc.) is technologically maximized in his notion of virtuous war:

> *"It is always double-edged: converting political issues into virtual imperatives that can be technologically enforced, the imposed solutions inevitably give rise to new political problems. When technological inertia trumps political constraint, it poses even greater dangers; as the political philosopher Jean Bethke Elshtain puts it, 'Virtue without limits becomes terror.'*[22] *Virtuous war presents a paradox: the more we resort to virtual means to resolve political problems, the more we undermine the very ground upon which our political virtues rest."*

So, expansion and transfer of technologized security practices create new problems and threats that are again addressed by way of technologies (cf. Beck 1986). The governed, for example, might use the inertia or stickiness of technologized security practices to establish tactics of resistance and deception, which then need to be addressed by technological adaptation. In other cases, security threats are merely transferred to different groups such as when the bunkerization and remote management in humanitarian action increasingly expose local staff while protecting foreign NGO workers (Andersson and Weigand 2015). More of the same or new technological fixes are then fielded in order to address newly emergent security threats feeding a cycle of technologization of security. By definition, escaping this cycle is difficult; also due to the intricate human-material entanglement in technologized security governance: Too many resources, i.e. money, time, networks etc., have been invested and "unraveling one part of an entanglement often involves disentangling too many other parts" (Hodder 2014: 32). However, recalling the essential instability of security governance assemblages does not make it impossible and opens space for political intervention, change and alternative security practices.

3.7. Conclusion

By developing a conceptual framework that draws on both socio-material and more classic security governance research, this chapter diverges from much socio-material thinking that rejects preconceived analytical notions as too restrictive to account for a complex socio-material reality. In fact, even critics of ANT challenge attempts at marrying some of its insights with complementary analytics as incompatible because of ANT's "intended, totalizing, and evolving thrust" (Fine 2005: 92). The framework rejects this criticism in favor of an analytical eclecticism (cf. Bleiker 2015). This allows reining in some of the most extreme positions of SMAS that exacerbate dialogue with classic security governance scholars and make it a useful starting point

[22] Jean Bethke Elshtain (1995), *Democracy on Trial.* New York: Basic Books, 123.

for understanding why and how technologies are enrolled into security governance and to what effects.

In various approaches to security governance, security threats are already assumed to independently exist, selected and responded to. In contrast, the notion of problematization highlights that security threats are a result of the interactions among different actors, technologies and their imagined responses. More specifically, technologies co-produce the security threat they are directed at. By nature of their materiality and the specific potentials and constraints they impose on human-material relations they render particular security practices more likely than others. In doing so they also impact who participates in technologized security governance, define roles, expectations and affect the power distribution: Technology becomes an analytical starting point to assemble the governance constellation. In doing so, problematization understands the creation of security threats and suitable responses as a controversy among multiple actors and technologies.

Once security is problematized and actors assemble around a technology, the concept of stabilization looks at how assemblages prevail while others vanish. For this the framework mainly identifies two analytical sites. Technologies and material objects in assemblages function as anchors of relations as they invoke repetitive practices reminiscent of habits or norms and in sync with the technological potentials and constraints. They bind or entrap other actors and have patterning effects on the practices between them. As a result, routinized practices are another useful indicator for stabilization and the goals of governance assemblages. Moreover, assuming that larger assemblages become more stable, different types of technologies exercise varying degrees of stabilization by virtue of their history and complexity depending on the amount of additional actors and technologies they introduce to the assemblage.

Concerning the consequences of technologized security governance, the conceptual framework focuses on effects as a result of locked in security practices that are resistant to change by virtue of their materiality. More specifically, three connected implications are theorized. First, technologized security practices turn insecurities into technical and material proxies. As a result, technologized security governance is concerned with the management of and coping with security threats instead of dealing with their root causes. Second, the objectification and quantification of the governed actors and things render technologized security governance into a one-way street that acts on passive agents and is indifferent to their feedback. This additionally exacerbates attempts at the formulation of alternative practices and inclusion of the governed. Third, technologized security governance promotes the maximization of the purpose of locked in security practices. This comes in two variants. On the one hand, technology drives the illusion of

absolute security in that technologized security practices only need to be expanded to eliminate remaining insecurities. On the other hand, technological solutions create further insecurities that are addressed by yet other technological fixes. This leads to a cycle that is encouraged by large investments of resources into technologization and difficult to escape.

Again, the conceptual framework is no strict scheme that can be applied to empirical data. However, it provides conceptual markers which inform data collection and analysis. The following chapter turns to the research design, data collection and analysis in order to illustrate a pragmatic and reproducible way to investigate technologized security governance.

4 Research Design, Data and Methods

4.1. Introduction

Socio-material approaches to security, including new materialism or actor-network theory, keep emphasizing empiricism and trace actual relations between entities without imposing conceptual templates. They are understood as "flexible research tools that facilitate empirical investigation" (Bueger and Stockbruegger 2018: 49). However, large parts of research remain rather silent on data collection and analysis. In order to fill this gap, the chapter draws on a grounded theory methodology. In this line of thinking, the conceptual framework provides useful sensitizing concepts that guide the research practice. The notions of problematization, stabilization and durable effects structure the thesis's data collection and analysis.

Grounded theory was developed by Barney Glaser and Anselm Strauss (1967) to defend and empower qualitative methods as legitimate and systematic ways of knowledge production in the social sciences. It provides guidelines for recursive data collection and analysis, where initial interpretations are repeatedly refined based on new empirical material until theoretical categories and relationships emerge that are closely aligned with the available data. This leads to a constant back-and-forth between theoretical concepts and empirical material. In doing so, the framework is instructive in posing specific questions to the data: How do actors use technology in the construction of security threats? How are controversies over threats settled? What kind of problematizations can be identified? Which roles do technologies play in the stabilization of security governance? How are more actors and objects enrolled into the assemblage? What kinds of effects are imagined by the security actors? What effects are observable? After various cycles of data collection and interpretation, the empirical analysis substantiates how threats are problematized, what differences exist in the role and use of technologies and what governance effects become locked in.

In the following, this chapter outlines the research design of the thesis and reflects on the merits of grounded theory methods to explore non-governmental remote sensing. For this, the origin, development and central characteristics of grounded theory are presented. Next, it will be argued how the conceptual framework fits into the research design and how the analysis takes into account practices and material objects. Then, the theoretical and practical reasoning is pointed out for selecting non-governmental remote sensing as a case study. Section 3 more specifically delineates the process of data collection and data analysis before the chapter closes with some reflections on epistemology.

4.2. Research Design

The thesis follows a descriptive-explorative research design (cf. Mayring 2014: 12). This choice is informed by two analytical objectives: First, to empirically investigate the growing phenomenon of non-governmental remote sensing. To this end, the analysis works through the empirical data to register the fit and occurrence of the notions of the framework. Second, to theoretically and methodologically refine the understanding of the role of technology in security governance. For this it is necessary to abstract from and substantiate new conceptual links out of the empirical material. Put briefly, the in-depth analysis of non-governmental remote sensing is coupled with the task of theoretical refinement. The objectives correspond with the pragmatic approach to the micro-macro distinction outlined in the previous chapters. A restriction to sole empirical description would risk adopting the views of research subjects and losing sight of less visible forces at work that affect their actions. Moreover, further development of conceptual approaches applicable across different cases is considered one of the hallmarks of social science (Pouliot 2016: 278).

To accomplish this, the thesis draws on grounded theory methods for five reasons. (1) The thesis offers a conceptual framework because it serves as a useful starting point to guide data collection and analysis. It is acknowledged that further refinement is necessary based on empirical analysis. This excludes many quantitative and qualitative approaches that rather focus on hypothesis testing than theory refinement or generation (Tucker 2016: 427-428). (2) The focus of grounded theory methods on the analysis of specific agencies, relations, processes and practices corresponds well with the conceptual framework. More specifically, grounded theory analyses are concerned with uncovering and theorizing patterned processes (Charmaz 2006: 181). (3) The dual objective of empirical case study and theoretical abstraction is inherent in grounded theory methods' combination of inductive and deductive reasoning (Kelle 2005; Tucker 2016; Charmaz 2017). (4) While socio-material studies are attributed a theoretical, generative potential in close examination of empirical material (e.g. Bueger 2013: 340) the procedure often remains quite idiosyncratic and disorderly. This not only misses the chance of promoting tested techniques of theory generation but also hampers both advancing on resulting theoretical categories as well as integrating them into a common pool of existing theories. Grounded theory offers a way to engage the task of theory generation more systematically and transparently (Tucker 2016: 428). (5) Lastly, the 50-plus years of development and active usage across disciplines have left grounded theory methods adjustable enough to be deployed beyond its orthodoxy and allow for conceptual frameworks as starting points of analysis as well as the consideration of diverse empirical data beyond written text (Charmaz 2006; Hülst 2010).

After having summarized the rationale for choosing a grounded-theory-inspired approach, the following section briefly outlines its historical origins to address the unconventional choice of devising a conceptual framework to guide the analysis.

4.2.1. The Origins of Grounded Theory

Grounded theory of the 1960s was developed to turn qualitative research into a scientific approach equally accepted by its peers as its quantitative counterpart (Charmaz 2000: 509). In doing so, it allows to diverge from the testing of overarching sociological theories to focus on theory generation which brings hitherto under-theorized phenomena into the purview of social scientists (Tucker 2016: 428). Grounded theory is often characterized as a data-driven approach. This means it does not necessarily start with a literature review or theoretical framework. Instead, the researcher first collects an initial set of empirical data concerning the phenomenon of interest, e.g. by way of interviews, archives, ethnographies etc. Then, constant comparison of data, coding and renewed data collection help to identify clusters and patterns which make sense of the data.

After their foundational, co-authored publication of *The Discovery of Grounded Theory* (Glaser and Strauss 1967), Glaser and Strauss have moved in somewhat different directions (Charmaz 2000; Charmaz 2006; Berterö 2012). Glaser (1992) emphasizes grounded theory as a method of theoretical discovery. The researcher directly attends to the empirical data untainted by preconceptions and discipline-specific literature: Theoretical frameworks unnecessarily force the data into ex-ante categorizations and contradict the purpose of data-driven theory generation. As a consequence, he does not leave many starting points except that theory somehow emerges from working through the empirical material, or as Glaser (1992: 43) puts it: "Categories emerge upon comparison and properties emerge upon more comparison. And that is all there is to it." Strauss, on the other hand, worked together with Juliet Corbin to develop a set of guidelines for researchers to make sense of the empirical material (Strauss and Corbin 1998 [1990]). This results in prescriptions that are more systematic, accessible and easier to handle. Unsurprisingly, it is their version of grounded theory that has become more popular. Some of their elaborate technical procedures are picked up below in the data analysis section.

Despite their differences, both versions are criticized for cleaving to positivism and assuming an external, objective reality that are accessible by a neutral observer (Charmaz 2000: 510). As a response, Kathy Charmaz (e.g. 2000; 2006; 2017) has formulated a constructivist grounded theory that retains most of its original premises but recognizes the position of the researcher who interacts with the data (see also Bryman 2008; Berterö 2012). In accordance with constructivist principles, *the* objectively given reality is replaced by *a* reality enacted by the things and people that live in it. Consequently, theoretical categories are not inherent in the data but are also a product of the researcher's theoretical knowledge, questions and biases (Charmaz 2000: 522-

523). Given this emphasis on reflexivity, the thesis is closer to constructivist grounded theory than its positivist precursors.

Despite their differences, grounded theorists generally agree that theoretical abstraction is achieved through a form of detailed coding of empirical data that is subsequently condensed into conceptual, interrelated categories. In doing so, they jointly and repeatedly caution against forcing the data through preceding literature reviews or theoretical discussions. This has led to a complicated and at times inconsistent relationship to extant theories, concepts and frameworks (cf. Charmaz 2006: 67, 163-166). From the outset, grounded theory has struggled with the problematic idea of approaching data neutrally without preconceptions (Glaser and Strauss 1967: 3, 37). The constructivist version at least acknowledges the contradiction when it explicitly calls for reflexivity during data collection and analysis. Building on this acknowledgement, the following subsection argues that the open conceptual framework is well-suited to mitigate the problem while retaining core benefits of grounded theory methods.

4.2.2. Grounded Theory, Conceptual Frameworks and Materiality

Challenging the proposition that ex-ante literature reviews and theoretical concepts only hamper the analysis, it is argued that the conceptual framework can be usefully integrated with grounded theory methods. More specifically, such a combination (1) rediscovers and takes seriously early concerns of grounded theorists who have wrestled with a lack of orientation in the heap of data; (2) relates to already existing proposals to data analysis such as sensitizing concepts or the coding paradigm; (3) taps into the potential of grounded theory to flexibly accommodate cognate approaches and (4) turns grounded theory methods into valuable tools for a systematic analysis of practices, processes and material objects to guide socio-material approaches to security.

On Implicit and Explicit Frameworks

The commonplace proposition in grounded theory literature to commence the initial data collection and analysis without preconceptions is virtually untenable in practice. Glaser and Strauss (1967: 3, fn. 3; emphasis in original) already admit in their founding text that "the researcher does not approach reality as a *tabula rasa*." They introduce the auxiliary notion of "theoretical sensitivity" as the ability to see what is relevant in the data (Glaser and Strauss 1967: 46; Hülst 2010). However, they do not further specify how researchers should incorporate theoretical concepts or formalize pre-existing knowledge and experience (see also Kelle 2005: 5). Later developments of grounded theory increasingly take into account the role of theoretical literature even in the early project stages (Strauss and Corbin 1998). In most cases, social scientists usually hold an array of theoretical and discipline-specific knowledge that is unlikely to be suppressed at the beginning of a research project (Bryman 2008: 548-549). Putting the

conceptual framework before the analysis recognizes that any empirical investigation follows explicit or implicit theoretical inclinations to begin with (Kelle 2005: 3). Furthermore, it acknowledges and builds on the theoretical contributions of others, provides orientation for data collection, and a focused analysis.

Building on Existing Approaches to Structured Data Analysis

There are various accepted approaches in the grounded theory literature, which mimic analytical frameworks in their function to guide initial analysis and further support the choice in favor of a literature review and conceptual framework. Herbert Blumer's (1969) notion of sensitizing concepts – popular among grounded theorists – steers analyses in particular directions in line with the research interest and discipline-specific vantage points. In contrast to definitive concepts, they are starting points for analysis that can be adapted, discarded or broadened in response to the empirical data. Even Glaserian grounded theory, which might be described as the "most data-driven" form, cannot cope completely without a theoretical guiding structure. Glaser (1978) provides a general list of 18 coding families corresponding with general notions from sociology which are supposed to help the researcher in their analysis.[23] With respect to both ideas, however, the researcher is again left alone how exactly they are to support empirical analysis and link substantive with theoretical categories (cf. Kelle 2005). This problem is tackled by the so-called coding paradigm. Strauss and Corbin (1998) develop this scheme to make sense of and describe connections among codes and categories. In a straightforward fashion they define three different components: Conditions denote the structure and circumstances of a phenomenon; actions/interactions identify the agents and their practices; consequences concern the outcomes of their actions (Strauss and Corbin 1998: 127-134). Interestingly, the components correspond to some degree with the central notions of the conceptual framework problematization, stabilization and durable effects as outlined in the previous chapter. As these three examples show, there are already tendencies in classic grounded theory that pre-structure the data and point towards apparent points of connection for the technologization framework. Of course, the framework goes a bit further as it is rooted in the sedimented knowledge of security governance and socio-material approaches to security.

Flexibility of Grounded Theory

[23] Two examples should suffice: Under the header "identity-self" Glaser (1978) lists the theoretical codes of self-image, self-concept, self-worth, self-evaluation, identity, social worth, self-realization, transformation of self and conversions of identity. When referring to parts or characteristics of a phenomenon, possible codes in the "dimension" family are dimensions, elements, divisions, piece of, properties of, facet, slice, sector, portion, segment, part, aspect and section.

Grounded theory methods should not be confused with unalterable and fixed instructions but rather understood as a pool of useful guidelines and techniques that can be adapted according to the research interest and disciplinary requirements (Hülst 2010: 284). In this sense, it is combinable with other approaches of qualitative and even quantitative analysis (Charmaz 2006: 9; Hülst 2010). Given this mutability and elasticity, it is not necessary to devise an elaborate and complicated adaptation of grounded theory. Charmaz (2000: 510) locates constructivist grounded theory methods in-between postmodernism and positivism to harness its power to make sense of empirical data. It is not bound to a single epistemological tradition but allows for varied combinations of allegedly incompatible methods (Charmaz 2006; for an argument on combinatory methodologies see Bleiker 2015). In this light, a conceptual framework complemented by grounded theory methods to elaborate and substantiate its central theoretical categories and relations only amounts to a minor modification.

Materiality, Practice and Process in Grounded Theory

Grounded theory methods are useful in detecting the role of material objects in relations and processes by virtue of their detailed sorting and sifting through empirical data that is responsive to the conditions, patterns and consequences of practices. This is unsurprising considering grounded theory's roots in pragmatism: Accordingly, "[s]table social structures depend on the processes that constitute them. These processes largely occur through people's actions although scholars now also take into account the environment and nonhuman actors" (Charmaz 2017: 38). This corresponds well with the theoretical foundations of the conceptual framework. Materiality becomes visible in practice, i.e. when technologies and objects are used (Law 2017: 31). The iterative mode of data collection and analysis in grounded theory inductively discovers the patterned ways of doing (Bueger and Gadinger 2015: 457; Pouliot 2016: 272). At times, this calls for some creativity in deciphering the role of materials and putting it into words; one useful strategy is to attend to material relations and uses invoked by human agents (Schouten and Mayer 2017: 310-311).

Taken together, it has been shown that grounded theory can serve as a valuable complement to the conceptual framework. Charmaz (2006: 164-169) even outrightly states the possibility of bringing together theoretical frameworks with grounded theory methods. The framework, then, serves a useful source to guide the analysis and "to demonstrate how [..] grounded theory *refines, extends, challenges* or *supersedes* extant concepts" (Charmaz 2006: 168-169; emphasis in original). As a result, grounded theory methods move beyond detailed empirical accounts and a collection of vignettes and enable theoretical generalizations (see also Wedeen 2010; MacKay and Levin 2015).

4.2.3. Case Selection: Non-Governmental Remote Sensing of Security

The case selection is first and foremost guided by the objective to substantiate the conceptual framework so that it becomes better anchored in empirical data and extendable across other forms and instances of technologized security governance. For this purpose, non-governmental remote sensing of security is selected as a case in particular due to three significant characteristics.

First, as an emerging technology it promises considerable variance on key aspects of interest including which security threats are problematized and addressed; which and how actors and things are brought together and coordinated in a stable fashion; and what kind of goals are pursued and with which lasting effects. This expected variance is conducive for the theoretical engagement because patterns are established based on similarity, frequency, difference, sequence, correspondence and causality. In this way, theoretical concepts and their relations move from real to abstract or from particular to general while the constant comparison of codes and categories ensures well-sourced theorizing (Tucker 2016: 430). The long Cold War history of remote sensing and the 1999 launch of IKONOS as the first commercial high-resolution Earth observation satellite raise questions whether non-governmental satellite observation can still be considered an emerging technology. However, only recent changes in the availability, pricing and usability of commercial satellite imagery due to increasing digitalization and economic competition prompted a surge of non-state actors such as non-governmental organizations (NGO), universities, think tanks and companies to lastingly integrate satellite imagery in their operations. This provides an abundant source of different strategies, problems, roadblocks, actors and effects that can be analyzed. Grounded theory methods provide valuable tools to grasp such a moving target (Hülst 2010: 281).

Second, non-governmental remote sensing of security is on the rise and a focus on this setting alleviates problems with data collection and analysis often associated with ethnographic or grounded theory methods in International Relations and Security Studies (MacKay and Levin 2015). From the beginning, satellite imagery has been a tool of the intelligence and military community. As a result, research of relevant actors, practices and assemblages of governmental satellite observation would require access to classified material and members of the respective government agencies (e.g. National Geospatial Intelligence Agency (NGA)). Focusing on the non-governmental side removes this obstacle – despite remaining overlaps between private, non-profit and government actors (see chapter 5). The role of non-state actors in security governance has grown considerably. This also pertains to non-violent non-state actors such as NGOs or multinational corporations. Their immediate and remote interventions affect the security

environment and "their responses to violence draw them into the fabric of security governance" (D. D. Avant and Haufler 2012: 258).

Lastly, non-governmental satellite observation cuts across a number of policy-relevant topics beyond the technologization of security governance and the role of non-state actors. This also pertains to the consequences of increasing transparency for global politics and diplomacy, the benchmarks of assured knowledge and evidence in international decision-making as well as the role of technology in alleviating human and non-human suffering. Up to this point the commercialization of satellite imagery has removed a number of legal, technical and economic barriers. Plans for further satellite launches, new business start-ups and technological developments indicate that the role of commercial satellite observation in security governance is set to grow even further. In 2017, the number of commercial rocket launches has surpassed government launches for the first time in history. In 2014, the overall revenue of the space-based satellite observation market was estimated at around 1.5 billion U.S. dollars and the total number of Earth Observation satellites is set to double by 2021 to more than 300 with the by far biggest share made up of non-military remote sensing capabilities (OECD 2014; SIA 2015). Despite the importance of Earth observation across issue areas and the growing availability of satellite imagery in the open domain, research on how this affects practices and consequences of security governance is rather limited: Extant studies on non-governmental remote sensing are rather outdated (Florini 1988; Litfin 1997; Litfin 1998; Dehqanzada and Florini 2000; Baker, Williamson, and O'Connell 2001), limited to instrumental understandings of technology (Livingston and Robinson 2003; Baker and Williamson 2006; Aday and Livingston 2009; Wang et al. 2013), are limited in scope and issue area (Parks 2009; Shim 2014; Olbrich and Witjes 2016; Rothe 2017) or, most importantly, lack sufficient empirical data including interviews that substantiate their claims (Herscher 2014; Hasian 2016).

In sum, non-governmental remote sensing serves as a valuable case study to further illuminate the growing impact of an emerging technology across an array of issue areas in security governance.

4.3. Data Collection and Analysis

This section details the methodological reasoning and process of data collection and analysis. Although grounded theory decidedly pronounces an iterative process, each aspect will be attended to in turn. The following sub-section provides reasons for choosing interviews as the primary data collection method, describes the procedure and collected data. Then, the data analysis is explicated with recourse to central coding methods of grounded theory.

4.3.1. Getting Rich Empirical Data

Qualitative interviewing has been chosen as the primary data collection method. The resulting interview material constitutes the basis of the empirical investigation of non-governmental remote sensing and is supplemented with additional sources. Qualitative interviews correspond well with grounded theory since both are "open-ended yet directed, shaped yet emergent, and paced yet unrestricted" (Charmaz 2006: 28). The credibility and quality of a grounded theory analysis rests on rich, targeted and reliable data, which is achievable by way of extensive interviews with experts, practitioners and regulators of non-governmental remote sensing (Charmaz 2006: 18). Surely, direct access to the inside views of informants is impossible but interviews provide an otherwise unobtainable perspective on the phenomenon that significantly surpasses the study of reports, press commentaries and marketing-guided messaging of satellite imagery companies. The extensive interview base is another aspect that stands out from other accounts of satellite observation in the literature. Interviews do not only allow for tentative access to motivations and experiences of individuals but also for reconstructing the pertaining social structure, practices and processes (Pouliot 2016: 277). Lastly, the geographical distribution of informants, descriptive-explorative objectives of the thesis and probable variance of the phenomenon advise to conduct multi-sited qualitative interviews instead of extensive ethnographies that would unequally emphasize particular practices, geographies and perspectives.

Selection of Informants

Based on the conceptual framework that puts technologies at the center, initial sampling starts with non-governmental satellite imagery analysts as the primary users of the technology. Then, and in accordance with grounded theory, informants are mainly selected based on theoretical sampling (for an overview see table 1). Emphasizing the iteration of data collection and analysis, informants are interviewed in order to further develop theoretical categories. This can be achieved by talking to people who are likely to provide contrasting, complementary or deepening accounts of the phenomenon in order to satisfy conceptual demands (Charmaz 2000: 519). The central notions of problematization, stabilization and durable effects allowed for a strategic and systematic selection of interview partners (Charmaz 2006: 102). From there, further sampling is guided by exploring variation of the initially found practices, events and experiences (Charmaz 2006: 109). Most of the informants were easy to approach as they publish satellite imagery analyses and/or are related to NGOs, research and government institutions. Additionally, some have been identified and contacted with the help of previous informants. Usually, initial contact was established via e-mail that explained the background of the project. Overall, a great majority of informants responded positively to interview requests.

Conduct of Interviews and Topic Guides

The mentioned geographical dispersion of informants involved in satellite observation renders it impossible to conduct only face-to-face interviews due to time and economic restrictions. As a result, a mixed strategy is chosen that combines personal interviews in locations with a high concentration of potential informants, i.e. Washington, D.C. and the Bay Area in California, with voice-over-IP (VoIP) interviews. In both cases, researchers need to be aware that they are effectively co-creating the accounts by way of their questions, responses and sheer presence (Charmaz 2006: 26). The great majority of face-to-face interviews were conducted during working hours at the informants' offices. A smaller share took place at conferences or in public places such as cafés or restaurants. Most interviewees agreed to be recorded and conversations lasted between 40 minutes and four hours while commonly it took about one hour per interview.

The topic guides follow a conceptual logic which reflects the three central notions of the conceptual framework. According to a warm-up and cool-down approach, interviews usually start with a biographical question asking for the initial involvement with commercial satellite imagery that ensures an easy and comfortable entry into the conversation and ends with a more speculative, future-oriented question. In line with the explorative-descriptive research design, three different main sections of the topic guide account for the diversity of people in the satellite observation community: One emphasizes the procedure of satellite imagery analysis, another one the commercialization of satellite imagery and a last one the ultimate utilization of satellite imagery in public advocacy, research or monitoring. Furthermore, questions are adapted according to the conversation trajectory and answers given in previous interviews in order to not "force" but remain open to unanticipated responses (Gusterson 2008: 104; Leander 2016a: 5-6).

Preparation of Data

Recorded interviews are transferred into smooth verbatim transcripts that represent the original wording but leave out fillers such as "uhm," "ah" etc. (Mayring 2014: 45). Full transcriptions not only allow for more detailed coding and analysis but the process of transcribing already is conducive to think oneself back to the interview situation and potentially brings about ideas that otherwise go by the board (Charmaz 2006: 70). In the few instances, where recording is not possible detailed notes are produced immediately after the end of the conversation that includes a recollection of what has been said including early reflections and observations. All interviews are anonymized and assigned a number that relates to a master list with identifying information. The only copies of the list as well as the transcripts and original audio files are stored on a university server.

Supporting Material

In order to increase the reliability and substance of interview data, the thesis makes extensive use of supporting material such as satellite imagery reports, government and policy documents such as laws and regulations, media archives, press releases, commercial documents, third-party interviews, academic and grey literature. In several cases, informants themselves provided supplementary material. Where possible, supporting material is linked to informants, e.g. satellite imagery analysts to their specific reports, company or NGO representatives to corresponding press releases etc. The extensive use of secondary material is in line with the grounded theory dictum that "all is data", although the relevance for the analysis differs based on research interest (Glaser 2001; see also Hülst 2010: 283; Charmaz 2006: 16). In this way, however, theoretical sampling (see above) also applies to additional sources beyond interviews: Supporting material is referred to and included when it aids coding and theoretical refinement (Charmaz 2006: 107).

Theoretical Saturation

The grounded theory concept of theoretical saturation defines the end of data collection and solves a persistent problem of some socio-material studies that strive for full description and, therefore, can always collect more data. Saturation is achieved when new interviews or other data points do not yield further refinement of theoretical concepts or typologies (Charmaz 2000: 520). In this sense, it is inherently linked to data analysis as sufficiently substantiated theoretical categories already cover newly collected data (Bryman 2008: 542). As a result, there is no numerical threshold saying how many interviews are enough but data is produced successively in the process of analysis (Hülst 2010: 290).

Description of Data

Generally, data is divided into two broad categories. First, primary data in form of interview transcripts are the basis for detailed coding. They are constitutive of the development of codes and theoretical categories. A full list of interviewee including a brief description is produced with Atlas.ti and provided in the appendix. Second, background material and secondary literature are referenced in the running text where appropriate. For the sake of clarity, a condensed overview of the interviews is provided in table 1.

Table 1: Overview of Interview Material

Time and Place	**Description**
Aug to Dec 2014, VoIP & Spain	Six interviews with non-governmental satellite imagery analysts and an EU government expert. Data was collected in the

	context of an earlier project focused on satellite observation of North Korea. The data is particularly useful given the detailed background information and description of the process of satellite imagery analysis.
May to Jul 2015, VoIP & Boston	Three interviews with a satellite imagery expert, a company representative of a satellite imagery provider and a NGO representative. Data was collected to devise and refine the initial project proposal of the thesis.
Feb to Mar 2017, VoIP, Germany & Washington, D.C. area	Series of 27 interviews. Based on the topic guides outlined above interviews focused on the practice of satellite imagery analysis, the commercial dimension and the role of satellite observation in advocacy and other non-governmental applications.
April to June 2018, VoIP, Bay Area, California	Series of 14 interviews. Interviews dealt with the commercial and political dimension of satellite imagery and touched upon the practice of satellite imagery analysis. Additionally, two events were attended including a satellite data hackathon and a research and training session on satellite imagery analysis at a university.

In total, 50 interviews were conducted with 57 individual informants; 36 in person, one via messenger chat and 13 via VoIP. Most of the interviewees were based in the United States, or more specifically the D.C. and Bay Area (see appendix for further details). The U.S. as the main site of field research is not chosen deliberately or on methodological grounds but emerged in the process of data collection. Moreover, the repeated interviews over the course of several years allow for successive theoretical development and cover the techno-political development of satellite imagery in the non-governmental domain and the corresponding practices.

4.3.2. Data Analysis

Data analysis in grounded theory essentially relies on several interrelated processes. The initial immersion into the empirical data is handled by way of open coding and the comparative method. Memo writing, from the beginning, urges the researcher to register early interpretations, patterns and relationship among categories. The memos, then, are often instructive for focused coding that subsumes codes into theoretical categories and establishes how they are related – increasing the degree of abstraction. These processes are attended to in turn although they regularly iterate and intersect in the actual research process.

Open Coding

In a first step of analysis, the researcher immerses in the data by reading all available interview transcripts and sifting through the empirical material. In the process, open coding is used to define and categorize the data. The conceptual framework and its individual components function as sensitizing concepts. Open coding takes segments of data, e.g. excerpts from a text or a snippet of an image, and assigns a label to it that is a primary interpretive abstraction of the concrete statement. A code does not only denote what is happening in the data but also attempts to grasp what it means. In this sense, open coding is guided by the search for data fragments of potential theoretical relevance so that "data are treated as potential indicators of concepts" (Bryman 2008: 542). Importantly, however, open codes are only provisional and subject to change as the coding proceeds. Therefore, it is essential to at once not shy away from interpretation but keep an open mind (Charmaz 2006: 43-48; Bryman 2008: 542-543). The process of open coding extracts portions of data out of their context of origin; it fractures the data so that the analysis moves beyond the experiences of individual informants but makes visible similarities, patterns and trajectories among them (Tucker 2016: 429). For the active labeling of open codes, the researcher addresses various questions to the data inquiring about the actors, their roles, which practices are central, what reasons are given or what consequences are anticipated (Hülst 2010: fn. 6). Moreover, it can be helpful to use gerunds instead of nouns for open codes in order to stay close to the data, emphasize process and not close off meaning too early (Charmaz 2006: 49). This is further reinforced by the use of in-vivo codes which are taken directly from the utterances of informants (Charmaz 2006: 55). Taken together, open coding gives access to explicit statements as well as implicit meanings. The closeness to the empirical material ensures that initial abstractions have a strong footing in the lifeworld of informants.

Comparative Method

The constant comparative method is a valuable tool in the development and refinement of codes. In principle, comparing codes starts as soon as the second code is established and continues at every level of analysis (Charmaz 2006: 54). This procedure clarifies the relationship of codes: Do they belong to the same phenomenon? Do they contradict or resemble each other? Is one a reason, condition or consequences of the other? The comparative method is also applied to different informants, points of time, incidents, practices and, later on, theoretical categories (Charmaz 2000: 515). As a result, codes are re-labeled, merged or discarded which enables building clusters that are separated by theoretical distinctions but remain empirically grounded (Bryman 2008: 542; Tucker 2016: 429).

Memos

Writing memos from the beginning of the research process is a useful practice to reflect on the definition of codes, their connection and overall to keep track of the thinking process during data collection and analysis (Bryman 2008: 547). They are written in an ad-hoc and informal manner, can include direct quotations or diagrams and often constitute the building blocks of first drafts of whole sections. Charmaz (2000: 517-518) summarizes the advantages of early memo writing as a useful way "(a) to grapple with ideas about the data, (b) to set an analytic course, (c) to refine categories, (d) to define the relationships among various categories, and (e) to gain a sense of confidence and competence in their ability to analyze data." From this it becomes clear that memo writing is a cumulative process in which initial thoughts revolve around specific codes while later memos define patterns, theoretical categories and their connections (Charmaz 2006: 72).

Focused Coding: Clustering and Relating

Open coding transitions into focused coding. At this stage, various open codes are dropped or synthesized into larger units of meaning, which is both theory-guided and data-driven. This means the conceptual framework starts carrying more weight at this point. Drawing on the open codes and memos, clusters are created, broken down and related. In some sense, open coding partitions the data while focused coding reassembles it into theoretical, sensible constructs (Bryman 2008: 543). The emerging categories are chosen based on "which initial codes make the most analytic sense to categorize your data incisively and completely" (Charmaz 2006: 58). To avoid confusion, it should have become clear by now that there is a hierarchy of abstraction when talking about codes and categories: Codes are the result of open coding while categories are more theoretically elaborate and subsume a number of codes. There are a few procedures that help with selecting the most relevant codes for further analysis although, in the end, it is up to individual interpretation.

The frequency of codes across the empirical material, for example, can be an indicator of analytic importance. Another tool to arrive at more focused codes and relationships is the coding paradigm mentioned earlier (Strauss and Corbin 1998). It zooms in on a particular phenomenon by specifically urging the researcher to explore the structures and conditions that make it possible, the patterns of action related to it as well as the consequences. In this way, it is close to what Charmaz (2006: 92) proposes for her constructivist grounded theory methods: Drawing on memos the building of theoretical categories requires to "define the category; explicate the properties of the category; specify the conditions under which the category arises, is maintained, and changes; describe its consequences; show how this category relates to other categories." Most importantly, the central concepts of problematization, stabilization and durable effects are useful in the process of focused coding as they offer a frame or trajectory of action that can sort emerging

categories. Diagrams might instructively provide a visual representation of how theoretical categories are connected. They give points of reference and orientation in the development of a narrative that explores the phenomenon in a systematic and coherent fashion (Charmaz 2006: 118). For this purpose, the drafting of sections and chapters alternates with revisiting the data; writing becomes part of the analysis (Charmaz 2000: 526). The integration of the analysis into the conceptual framework is a result of linking the emerging theoretical categories to the conceptual framework. As a result, it is conceptually refined and illuminates non-governmental remote sensing as a recent phenomenon in security governance.

Software-Assisted Analysis

During the whole research process Atlas.ti (version 8.2.4 (559) for MacOS) is used to assist with the data analysis. It is considered a valuable tool to manage and structure the amount of interview data. Moreover, it offers useful functions that are in sync with grounded theory methods such as the creation of quotations, codes of differing hierarchies and memos. Moreover, most of these components can be linked, grouped into clusters and drawn onto a visual map or network. Lastly, the software facilities reporting of intermediate results and reports as an integrated function of the program.

4.4. Conclusion

As grounded theory was developed in a positivist tradition that assumes an external reality accessible by a neutral observer (Glaser and Strauss 1967), postmodernism can serve as a useful corrective that highlights the intricate relationship of the researcher with the research subject (Charmaz 2000: 528). The position of the researcher as actively co-constructing the empirical material during data collection as well as analysis discards strong notions of neutral objectivity but accepts it as being incomplete and partial (Hülst 2010: 284; see also Pouliot 2016: 277-278). Albeit this should instill an amount of humility during the analysis, this is no reason to refrain from theorizing and interpretation. Rather this openly acknowledges that "interpretation requires both a theory and a healthy skepticism about its explanatory efficacy. By navigating between concrete details and conceptual abstractions, we can refine and undermine, negate and create novel explanations about politics" (Wedeen 2010: 264). This corresponds well with the tools of grounded theory including open coding constant comparison, memo writing and focused coding.

In line with the descriptive-explorative research objectives, grounded theory methods serve as a valuable complementary to the conceptual framework outlined in the previous chapter. Despite repeated affirmations of the necessity of empiricism to trace socio-material relations in security governance, new materialism, assemblage thinking or actor-network theory rarely provide detailed descriptions of methods, data collection or analysis. Grounded theory provides the

methods to substantiate the conceptual framework and investigate the case of non-governmental remote sensing of security. For this purpose, the interview material serves as the primary empirical foundation of the following analysis. The remaining thesis is structured along the central notions of the framework starting with problematization to stabilization to durable effects. Each of the following chapters deals with one of the three central concepts to address one research question.

Part II

5 Satellites and the Co-Production of Security Threats

5.1. Introduction

When reports about an oil spill, human rights violations, illegal deforestation, natural disasters or nuclear tests appear in the media, non-governmental actors turn to commercial satellite imagery providers. They search the provider's imagery archive for an image that matches both their time and area of interest. The responsible satellite imagery analyst examines the visual data with regard to additional information. A written report including the satellite image is then disseminated to verify, refute or complement public media reports. Less frequently, analysts discover relevant developments on the satellite imagery itself that have not been reported yet such as missile test preparations, military movements or illegal fires. In both cases, satellite imagery analysts methodically analyze standardized remote sensing data to record and problematize threats to human, national, economic or environmental security. The use of satellite imagery gives additional credibility to the analysis as the security threat is allegedly presented for everyone to see. This chapter seeks to distort common-sense understandings about the use of non-governmental remote sensing for security purposes. First, it challenges the taken-for-granted human control over remote sensing in the construction of security threats. Second, it scrutinizes how satellite technology renders those constructions valid and credible. For doing so, the chapter asks: How do human and technological factors interact in non-governmental remote sensing to credibly problematize and create security threats? The structure follows the standard procedure of satellite imagery analysis from imagery acquisition to interpretation to report dissemination in order to trace the co-production of security threats. More specifically, the chapter looks at the techno-political conditions that define what satellite data is collected, what imagery non-state actors pull from the archive, how they interpret it and, lastly, how satellite imagery is translated into the public.

The first section identifies various political, economic and material constraints that qualify claims of an unbiased, global coverage of commercial satellite imagery. Effectively, it counters human-centric arguments that the satellite imagery that is acquired by non-governmental actors are determined by the problems they seek to address. In contrast, the section argues that security problematizations are indeed co-produced by remote sensing technologies themselves. The following section undermines the notion of seeing security threats on satellite imagery. The analysis of satellite imagery is difficult and ambiguous. Here it is shown how different coping strategies of non-governmental actors can give rise to flawed, overbearing and militarized forms of interpretation. Most importantly, the section argues that satellite imagery analysis essentially translates matter into security threats. Security threats are reduced to expressions of material

change or material proxies. This complicates desecuritization of problems, predefines the space of possibility and risks to simplify or even misrepresent security threats. Lastly, the chapter traces the practices and processes that render non-governmental remote sensing a functional and legitimate method to create security problematizations. More specifically, the visual and material dimensions of satellite imagery, at once, emotionalize and rationalize security threats. Despite indications to the contrary, they suggest an obviousness and scientific validity of the findings. This is further reinforced when established and trusted institutions integrate commercial satellite imagery into their work and endorse non-governmental remote sensing as a legitimate means to create security threats. Taken together, the chapter makes clear how the potentials and constraints of satellite imagery co-produce the problematizations of security and render them valid and credible threats.

5.2. Imagery Acquisition: Socio-Material Potentials and Constraints

Regardless of political, security or environmental circumstances, a commercial camera circling the planet at first promises unfiltered, global imagery of even the most inaccessible areas. Before the commercialization of satellite imagery, think tanks and security watchdogs had to rely on leaks or input from former intelligence personnel. The new transparency suggests unprecedented, direct access to information that was previously restricted to small groups inside governments. Putting this glossy vision to the test, this section traces the socio-material conditions and practices of how commercial satellite imagery is produced and how non-governmental actors access it. This is important for the problematization of security. Because non-governmental actors can only point to security threats on satellite imagery that is actually collected by an Earth observation (EO) satellite and is subsequently acquired for analysis.

5.2.1. Laws of Orbits

When it comes to international regulations in space, commercial remote sensing has found an encouraging legal regime since day one. The 1957 launch of Sputnik led to much celebration in the Soviet Union and an equivalent of hysteria in the United States and its allied nations. Apart from the so-called Sputnik shock, the first artificial satellite set an important precedent: Inserted in an elliptical orbit around Earth, Sputnik crossed multiple national borders of hostile countries within minutes – unimaginable for an airplane, civilian or otherwise. It effectively created a de-facto permission of orbital overflight. Just like Sputnik, present-day commercial EO satellites orbit the planet largely unhindered by claims of national sovereignty, airspace regulations and political borders. Non-governmental satellite imagery analysts are well aware of the great leeway they enjoy due to the low regulation of outer space in general: “Well, the thing about satellites is that they are in space. So, really, they are only controlled under treaties that regard space. So that’s quite nice because I’m [legally] not infringing someone’s sovereignty. I’m not going into their

territory" (Informant #42). This freedom is confirmed by international agreements. The 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, more commonly known as the Outer Space Treaty, guarantees the freedom of use of outer space. More specifically, the Principles Relating to Remote Sensing of the Earth from Outer Space of 1986 have concretized the right of satellites to fly over any part of the Earth (UN Office for Outer Space Affairs 2007). Interestingly, sovereignty and concerns of national security were major drivers of the formulation of these principles. Yet, they are not explicitly covered in the text. Instead, the principles only address those activities that deal with remote sensing of natural resources management, land use and the protection of the environment. The agreement does not deal with the original concerns but formalizes the practice of observing any place at any time as long as it can be guaranteed that the sensed state has equal access to the imagery that is captured. Effectively, no prior permission is needed, which was a central demand of a couple of states in the negotiations but which was trumped by the principle of "freedom of use of outer space" of the Outer Space Treaty that was brought forward by mainly developed nations including the Soviet Union and the U.S. (Soucek 2011: 370). In short, the thin international regulation of space in general and Earth observation in particular put few constraints on non-governmental remote sensing.

Regulatory Power of the Government

More significant regulation is taking place on the national level where governments retain considerable leeway over commercial remote sensing operations. In case of the U.S., the commercialization of satellite imagery was met with some internal resistance from parts of the military and intelligence communities (Olbrich 2019c). Although proponents prevailed, the U.S. government maintains significant control and influence over the production and sale of satellite imagery. All launches of EO satellites require government approval so that unwanted technologies can effectively be barred from orbit. In any case, the U.S. government restricts the maximum resolution of electro-optical satellite imagery to .25m – down from .5m in 2014. Additional legislation also forces U.S. providers to further reduce the resolution of commercial satellite imagery over Israel: The Kyl-Bingaman amendment prohibits the dissemination of U.S. satellite imagery of Israel at higher resolution than available from international sources. Moreover, the so-called shutter control policy allows the government to stop sales and end operations for reasons of national security (Witjes and Olbrich 2017). While the policy was never officially executed, the U.S. government bought exclusive rights of all available commercial satellite imagery in preparation of the war in Afghanistan. In doing so, it denied access to anyone but government actors – a practice called checkbook shutter control. The few international competitors of U.S.

providers of high-resolution imagery face similar national restrictions when it comes to imagery collection and sale.

The German 2007 *Satellitendatensicherheitsgesetz* (Satellite Data Security Act) includes similar restrictions on commercial high-resolution EO satellites. Any company requires prior approval to operate such a spacecraft. In addition to specific technical and data security regulations, one requirement rather broadly states that the operator or imagery provider possesses the needed reliability (*Zuverlässigkeit*) – a stipulation that arguably allows for considerable interpretation. All customer requests for imagery are subject to a prescribed sensitivity check. This check reviews the identity of the customer, imagery data properties and, most importantly, potential harm to German security interests before the sale takes place. Lastly, any provider needs to give priority to the imagery needs of the German government in situations of national emergency or defense. In light of these restrictions, multiple U.S.-based NGOs reported problems when trying to acquire satellite imagery from German satellites.

There is a general expectation that growing international competition will somewhat ease those national regulations. As of now, however, non-governmental actors mostly draw on U.S. or European satellites companies that pay close attention to existing regulations in the respective jurisdiction: For example, when a U.S. NGO seeks to buy Airbus imagery of Gaza, Airbus complies with the Kyl-Bingaman Amendment and degrades the satellite data to comply with U.S. laws. In any case, most countries' commercial remote sensing programs are intertwined with their government and military domains and subject to diverse limitations. Consequently, the designation of satellite imagery as commercial is at least in some cases to be taken with a grain of salt. They are "all commercial but not created equal" as one expert put it (Informant #47).

Orbital Powers

Commercial or not, orbital forces that apply to EO satellites prevent constant and uninterrupted observation. In fact, various material constraints affect high-resolution imaging from space. Remote sensing satellites that carry optical cameras depend on reflected sunlight to operate so they do not work at night or during cloud cover. In order to keep their altitudes of between 500km and 800km, EO satellites usually circle the Earth about every 90 minutes at 27,000 km/h in polar, north-south orbits. This way, they are in a favorable position in relation to the sun and avoid haze that can reduce image quality. Satellite images are preferably taken sometime between 10 am and 2 pm. Each satellite can focus on a particular region for only a few moments during an overpass. When doing so, high-resolution satellites capture smaller areas per collection than lower-resolution satellites. They collect imagery strips or multiple point targets with a width of a few kilometers. When a high-resolution satellite is over North Korea it does not capture an image of

the whole country but only a predetermined selection it was programmed to collect. For this, the satellites are built agile enough to slew and turn their sensors towards these areas of interests. In this case, they take images off-nadir, which are side-on shots. This can provide additional information because instead of only looking at the roof, analysts can discern details such as the number of stories or entrances of buildings.

In total, operators of high-resolution imaging satellites usually build constellations of a few spacecrafts. For example, industry leader DigitalGlobe operates four satellites at a time. This amounts to a daily image capacity of about 3 million square kilometers or circa 2 percent of the whole landmass – far away from constant surveillance. As these orbital constraints illustrate, commercial high-resolution satellite constellations do not offer 24-hour refresh rates. The limited frequency of imagery collections has significant implications for which and how security threats are highlighted: "If I go to Airbus' or DigitalGlobe's archives I see it happening maybe once a month or once every 3 weeks. That's very good, every 3 weeks is significant. But if I truly want to understand pattern-of-life type of information, I need to have imagery taken even more frequently – everyday would be nice" (Informant #43). The limited number of visits of high-resolution satellites influences the depth of analysis possible. More fundamentally, it excludes a significant number of security threats as there is no satellite imagery of the area and time of interest to begin with.

This can also become a problem when the satellite attempts to collect an area of interest that is covered in clouds. Electro-optical sensors cannot see through clouds, which usually cover two thirds of our planet (International Satellite Cloud Climatology Project 2016). Unsurprisingly, many non-governmental actors report negative experiences with cloud cover affecting their work. When satellites are over the area of interest only once or twice a week and cannot capture any useful imagery because of clouds, this leads to long stretches without any new information. This is a particular challenge when observing deforestation in the tropics, damage assessments after hurricanes or security developments in areas with a rainy or typhoon season: "so really what you're doing is, you're detecting forest loss in Brazil in the dry season and then you might not see the forest for several months until you get a clear view again" (Informant #32). When it comes to large-scale security issues such as ballistic missile programs or nuclear programs, particular activities are even timed to occur during the night or cloud cover in order to avoid observation (see chapter 7).

Overall, the legal and orbital conditions of commercial remote sensing affect the problematization of certain security threats. Drawing mainly on U.S. and European assets introduces a particular bias because their operations are governed with the respective national security concerns in

mind. Imagery providers need to follow national regulations and anticipate the interest of their regulators and major customers that "are very wary of publishing satellite imagery over military action or of NATO, U.S., European allies" (Informant #18). So, restrictions to release imagery over areas where NATO troops are active constraints the possibility of non-governmental analysts to select their areas of interest. Effectively, it will be easier to monitor areas of non-Western military activity, their actions and potential wrongdoings. Additionally, the technical limitations of focused sensors, brief overflights at certain times of day and environmental constraints such as nighttime and clouds further limit the depth of analysis possible as well as the frequency and areas of possible observations.

5.2.2. Different Sensors and Spectral Bands

Issues with light and cloud conditions mainly pertain to passive sensors such as electro-optical remote sensing which in principle work like common smartphone cameras. It is the most widely used sensor by non-governmental actors.[24] Yet, technical alternatives are available that offer a different spectral resolution, i.e. make use of the non-visible spectrum, but come with their own potentials and constraints.

As an active sensor, synthetic aperture radar (SAR) collects imagery at night as well as during cloud cover. The satellite transmits successive radio waves and records their echo to produce a high-resolution image. Given their all-weather capability, they are in high demand in military and intelligence circles. Until recently, commercial SAR imagery was unavailable from U.S. sources. In contrast to Canada or Europe, the U.S. company Capella Space has received the first license to launch and operate SAR satellites only in spring 2018. SAR and electro-optical products differ from each other and enable different kinds of analysis.

The different, non-natural appearance of objects in a SAR image require substantial experience and training. Consequently, non-governmental analysts without an intelligence history have a difficult time making use of SAR. Various informants have mentioned that they experiment with SAR imagery. Across the board, they highlight the usefulness of being independent from clear skies and daylight. Yet, most of them have not found a suitable problematization for this kind of imagery. Tentatively, it is very useful to detect vessels on the open sea that have switched off their automatic identification systems (AIS) or oil pollution given the distinctive way of reflectivity. The high prices and long revisit times, however, render its continuous use unpractical. Similarly, some NGOs have experimented with different kinds of infrared imagery. Usually, infrared satellite data is used in combination with electro-optical imagery. The use of thermal infrared to better locate forest fires is rather well-known. However, it can also be employed to ascertain whether factories

[24] Consequently, I speak of electro-optical satellite imagery if not indicated otherwise.

or nuclear reactors are operating in which case they show a higher temperature than the immediate environment. Near-infrared, on the other hand, is particularly useful to review plant health. That's why large agricultural companies use it to monitor their farmland. In the security sector, it helps to make damage assessments or validate missile tests by way of highlighting disturbed and burnt plants that is surrounded by healthy vegetation. The quite specialized areas of application make infrared imagery a sporadic source in non-governmental remote sensing. Although some think tanks and NGOs experiment with alternative sensors, electro-optical satellite imagery is the by far mostly used data.

As has been hinted at already, non-governmental actors usually draw on high-resolution satellite imagery. Commonly, resolution refers to the spatial resolution, which describes the detail discernible in an image. Arguably, the commercialization of remote sensing has attracted a number of non-governmental actors because it goes hand in hand with a substantial improvement of resolution. Civil remote sensing missions have operated since the 1970s and produced satellite imagery with 80m and later 30m resolution. The U.S. launch of IKONOS in 1999 was the first commercial imaging satellite with sub-meter, or high, resolution.

Spatial resolution plays an important role in the ability to identify features without special analysis tools. Because of this, only few non-governmental actors regularly draw on low-resolution satellite imagery. Similar to SAR and infrared imagery, there are few security problematizations that can be addressed with low-resolution images:

> *"We're somewhat – I don't wanna say unique – but more so than most other places we tend to sort of dabble in kind of experimental uses of some of the lower resolution sensors. Just trying to find applications for those. Many of the other NGOs that we've worked with haven't done as much with that because it doesn't have quite the same visual punch for advocacy efforts. We're dealing with strictly scientific data sets. They can still be useful"* (Informant #3)

The technology in some sense drives the security threats that are identified. When it comes to medium resolution imagery of about 3m to 5m, it can be useful as an additional source that helps to clarify timelines. In other words, it helps answering simple questions in particular contexts such as when has construction started or what is the monthly activity level over time. The company Planet has a constellation of about 150 satellites that produce daily imagery of 3-5m resolution. Given the continuous archives of low- and mid-resolution satellite imagery, it is useful for observations of large-scale and long-term developments. Essentially, the repeated collection of satellite imagery of the same area is an important feature in itself. This so-called temporal resolution denotes the time necessary for a satellite or a constellation to revisit the same area of interest. Given the smaller area size collected by high-resolution satellites and the high prices to

build and launch such sophisticated spacecraft, they have a lower temporal resolution. It is a trade-off between frequency and image quality. That said, there are limits to the degree that some satellites can be "used for the prevention of war crimes, crimes against humanity and genocide due to the low resolution" (Informant #49).

The spectral, spatial and temporal resolution of Earth observation satellites play an important role in the co-production of security threats. Their specific potentials and constraints co-determine which object can be made visible on a satellite image and, thereby, affect the possibility space of which security threats can be problematized. In some cases, non-governmental actors pick up alternative imagery products to experiment and find suitable applications. In this sense, the sensors drive the kind of problems that are addressed. For examples, NGOs might have difficulties to recognize activity at nuclear power plants at 30m spatial resolution. However, the sensor might be sufficient to observe deforestation over longer periods of time.

5.2.3. Power Context: Government-Industry Relations and Non-Governmental Remote Sensing

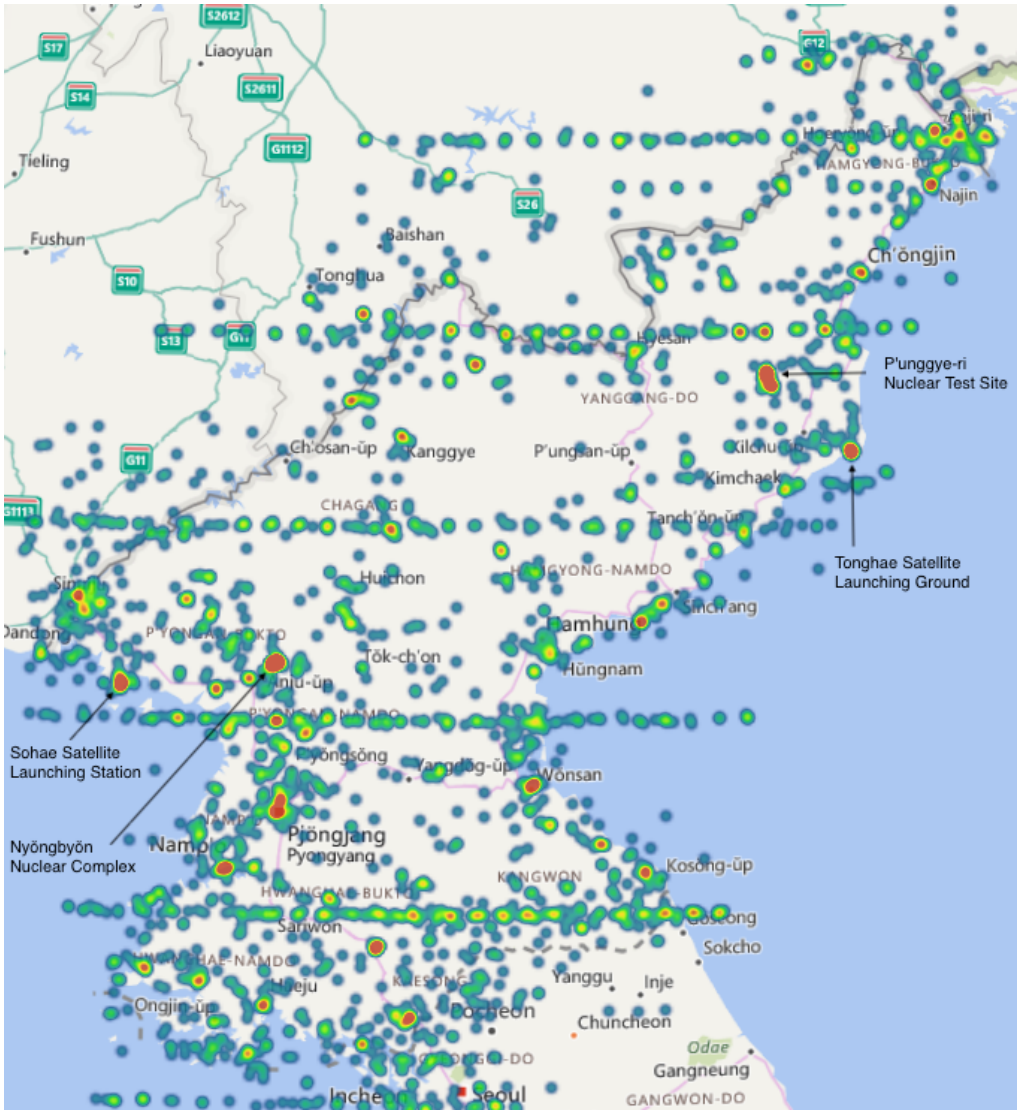
In addition to the regulator role of national governments, they also count among the largest buyers of commercial satellite imagery. In fact, the U.S. government has for years accounted for more than 60 percent of overall revenue of global industry leader and U.S. company DigitalGlobe, which continues to intensify its government involvement (Erwin 2018). Another significant share is other defense and intelligence business as well as foreign governments. The demand by NGOs and think tanks is negligible. They do not "move the needle for these companies whatsoever other than it's good for employee morale," as one informant put it. "Even if the Gates Foundation or the Clinton Foundation integrate this technology into everything they're doing. It's still not going to be enough" (Informant #5). DigitalGlobe sells most of its satellite imagery to the National Geospatial-Intelligence Agency (NGA) whose mission is to support the national security efforts of the Department of Defense and the U.S. intelligence community.[25] The demand for satellite imagery in the government is immense and cannot be satisfied by classified remote sensing assets alone. They already run at capacity to cover high-priority areas of interest. The commercial industry provides extra capacity to fill the somewhat lower-priority needs. The NGA's relations with DigitalGlobe are defined in service level agreements. According to these long-term agreements, the agency pays a fixed price for access to archival imagery data and tasking capacity, i.e. what images the satellites are going to collect. Consequently, the U.S. government has great influence over the parts of the world that are being imaged by DigitalGlobe. As a commercial company it largely follows requests by its largest customer, regulator and benefactor. The non-

[25] In 2018, the National Reconnaissance Office (NRO) has assumed responsibility of the contract with DigitalGlobe.

governmental community, on the other hand, has very limited power over what areas are collected, what goes into the archive and which areas are problematized.

Fundamentally, the economic importance of the defense and intelligence community for the remote sensing industry is reflected in the imagery archive. In the case of DigitalGlobe, the U.S. government heavily influences the satellite tasking and, thereby, determines what finds its way into the archive. Non-governmental actors usually cannot afford to task satellites themselves. Even if they do, waiting for the right orbit, appropriate cloud conditions and a free slot in the tasking capacity can create long waiting times. So instead of paying several thousand U.S. dollars, non-governmental actors routinely fall back on archival imagery. This comes at a cost of a few hundred U.S. dollars per image depending on the quality, area, and time of acquisition. Taking the archive as "the law of what can be said" (Foucault 1972: 129; see also Stoler 2002), the imagery archive further constrains the space of possible security problematizations because it lays the foundation for the problems and questions non-governmental users are able to address. In the case of DigitalGlobe, NGOs draw on a pool of imagery that from the beginning is biased towards U.S. government interests. In effect, it is easier to persistently monitor security threats that are in sync with U.S. government interests. Figure 1 illustrates the uneven concentration of high-resolution satellite imagery using the example of North Korea. The heatmap plots DigitalGlobe's commercial imagery archive over North Korea from 2002 through 2017. Thus, it shows which areas were more frequently imaged and are available for purchase. The four marked locations indicate particularly high concentrations of satellite imagery that match security hotspots of exceptional relevance for the U.S. government (Olbrich 2019b).

Figure 1: Heatmap of DigitalGlobe Satellite Imagery over North Korea, 2002-2017



Source: Olbrich (2019b)

In this view, commercial satellite imagery is no neutral instrument or transmission belt of the goals and values of non-governmental actors – or anyone that draws on the archive. Instead, it already contains the national security interests of governments, affects the range of questions non-governmental actors can raise and, and co-defines the political agenda. This is not to say that the U.S. government or others censor commercial satellite imagery. However, in their role as regulators and by far most important customers they predefine what is available for anyone else and increase the likelihood of non-governmental actors focusing on security situations that are in line with government interests. Coincidentally, then, the techno-political conditions nudge non-governmental remote sensing to copy and complement governmental intelligence rather than challenge it.

5.2.4. International Satellite Imagery Market

To some extent, non-governmental satellite imagery analysts are aware of the biased imagery archives. However, they hope that the ongoing commercialization of satellite imagery leads to additional and competing constellations of EO satellites. As a matter of fact, although DigitalGlobe and Airbus are the largest commercial satellite imagery provider, they are not alone anymore. For example, Planet also sells mid- and high-resolution satellite imagery to non-governmental actors. It operates the largest fleet of about 150 EO satellites including a dozen high-resolution satellites. Based on that, it can offer daily coverage of the whole landmass. However, this daily imagery is limited to 3-5m resolution, which is insufficient for many purposes of non-governmental remote sensing. Planet started off on a rather idealist platform to work towards global transparency, engage non-governmental actors and promote a humanitarian mission (Olbrich and Witjes 2016: 118-119). By now, it also works with old-time, institutional players including the NGA and Defense Intelligence Agency. Airbus is similarly involved with European governments and emerging start-ups openly aim to cater to the needs of government and intelligence communities. On a global scale, defense and intelligence actors accounted for about 65% of the 1.3 billion commercial satellite imagery market in 2017 (Euroconsult 2018). As of now, satellite imagery providers from China do not play a major role for non-governmental users because it is difficult to acquire their imagery. In any case, informants commonly report to restrict themselves to the large U.S. and European imagery providers. With that said, the term commercial satellite imagery comes with a number of qualifiers. Governments occupy prominent roles in the setup, regulation and business of Earth observation companies. So much so, that industry experts contend that, indeed, "it would be a major shift if commercial providers could operate completely free from government considerations" (Informant #47).

Moreover, there are a number of announced, planned and early-phase remote sensing start-ups, which would increase the availability of satellite data and drive down prices. As of now, however, their chances of success are up for debate. In order to pluralize and diversify the archives of high-resolution satellite imagery, it would be particularly critical to decrease the dependence on the government and defense sector. However, especially the ability of start-ups to create a more competitive market that is less reliant on government demand remains controversial. The costs to develop and launch satellites of any kind have fallen significantly over the past years due to growing competition in the launch market and the miniaturization of (EO) satellites. Yet, lower barriers to entry and technological innovation have not yet resulted in a sustainable commercial market for satellite imagery independent from governments. The uncertain future of commercial satellite imagery upsets non-governmental users because "the kind of work that we do is definitely contingent on how the satellite imagery industry is changing" (Informant #1).

5.2.5. Data Scarcity, Data Abundance, Data Democracy?

Still, optimists in the remote sensing industry contend that additional satellite constellations already diminish government influence. The expectation of an abundant and accessible supply of satellite imagery is encapsulated in the peculiar notion to "democratize access to data" (Marshall 2018a). Surely, large-scale projects such as Planet's deliver a lot of mid-resolution data. As of yet, though, the democratization terminology is misleading. The remaining high prices and government involvement differentiate between haves and have-nots. "First and foremost, it is an industry euphemism that highlights the exuberance and enthusiasm underlying the commercialization of satellite imagery" (Olbrich 2019c: 113). In any case, the global coverage of high-resolution satellite imagery that is necessary for many security-related analyses remains uneven. If nobody paid to task the satellite to collect a certain area of interest, NGOs will not have imagery: "So you've got an issue that all the time the imagery that you would like to have isn't available because nobody asked for it" (Informant #39). Overall, the governments and their defense and intelligence agencies assume an ambiguous role. Because of their sway over tasking decisions they predetermine what satellite imagery non-governmental actors draw on and, ultimately, what security threats are problematized. At the same time, by way of their continuous investment, they guarantee the existence and sustainability of commercial satellite imagery to begin with.

The fast-paced development of EO satellites and the uncertainty about its future find expression in contrasting assessments of non-governmental access to commercial satellite imagery. On the one hand, there is still not enough satellite imagery: "All my biggest frustrations come from the lack – every day it gets better – but there is still a lack of availability" (Informant #42). This relates to the dilemma of a biased imagery archive and obviously limits the possible problem set of non-governmental remote sensing. On the other hand, some anticipate that they do not have enough analysts to cope with the growing amount of satellite data they are dealing with. If non-governmental users "get flooded with information" (Informant #20), they face the additional task of filtering out what is relevant. Although availability has clearly improved over the past two decades, non-governmental remote sensing still oscillates between data scarcity and data abundance. This is largely sensor- and location-dependent. Especially actors whose work demands high-resolution imagery are still confronted with availability gaps. Moreover, the biased nature of imagery archives leads to different concentrations in terms of availability (see figure 1). As a result, there is more recent high-resolution imagery of Raqqa or Luhansk than Groningen or Paderborn. However, if you specifically require satellite imagery of Groningen and "nobody else pays for it or [satellite imagery providers] get it of their own volition you are not gonna see it, because it's not in the catalogue, because they didn't shoot it" (Informant #39). Despite high expectations that the commercialization of satellite imagery will democratize access, issues

associated with the data scarcity-abundance problematique affect which security threats non-governmental actors are able to tackle.

5.2.6. The Most Economical Security Threat

As elaborated earlier, non-governmental actors rely on the imagery archive because tasking a satellite to image an area of interest is prohibitively expensive and de facto reserved for government or large commercial customers. Having said that, even archival imagery strains the often tight budgets of NGOs and think tanks. In fact, NGOs and think tanks consistently raise budgetary and price problems when it comes to commercial remote sensing: "It's usually a tool that is too expensive for normal people to do outside of government" (Informant #1). Especially smaller groups cannot afford to regularly pay a couple of hundred U.S. dollars on satellite imagery. Consequently, they scan free and open sources for satellite imagery. Yet, drawing on GoogleEarth and foreign map services to pluck holes in their timelines also means to accept lower quality and virtually unpredictable image updates. The middle-ground is settling for cheaper mid-resolution imagery. However, the trade-off is that some problems simply cannot be addressed with anything else but high-resolution imagery. Moreover, non-governmental actors still face other cost positions that are not reduced by drawing on free or less expensive imagery sources. Because they still require the necessary hardware and software to deal with satellite imagery and, most importantly, a skilled workforce to analyze it.

Once, non-governmental actors have some experience in dealing with satellite imagery or even an institutional point person they develop rather idiosyncratic acquisition practices. These differ across organizations and across projects. Universities and other non-profits can hope on discounts on some commercial satellite imagery. DigitalGlobe, Airbus and others have established points of contact to take care of development, humanitarian and human rights customers – in effect anything non-commercial or non-governmental. Over time, non-governmental analysts establish good relationships with individual imagery providers so that a phone call or e-mail can go a long way in acquiring the right image. In doing so, U.S. companies in particular offer rather flexible pricing and acquisition models to non-governmental actors. This is possible because of the very specific interest of some advocacy groups or think tanks in a particular region or issue such as small islands in the South China Sea or deforestation in Indonesia. In the event of emergencies imagery providers regularly provide imagery free of charge to help relief efforts. Taken together, non-governmental users are often dependent on the good will or marketing prospects of imagery providers when they cannot put up the same funds as government or business clients.

Consequently, decisions to spend money on satellite imagery are made on a case-by-case basis. The economic pressure has peculiar implications for how security is problematized via

commercial satellite imagery. Because of the relatively high purchase costs, non-governmental actors cannot afford to not find anything on the satellite image. They are forced into an economical decision whether the anticipated value of the satellite image analysis justifies the costs. Consequently, non-governmental remote sensing defines areas of interest where there is high confidence in finding a potential threat: "Before we buy the shot, we have a pretty good idea of where it's gonna be. That's why we buy the shot. We're not buying a shot of random desert; that's a lot of desert to buy" (Informant #14). In this sense, it is safer to buy a high-resolution image of known security threats such as North Korea's Nyŏngbyŏn nuclear complex that shows some activity rather than spending hundreds of U.S. dollars and risk buying an image of an empty desert. This renders commercial satellite imagery not so much a tool to discover rather than corroborate, confirm and stabilize known security threats. Whereas "nothing to report" might be a valuable finding in the intelligence community as it gives an update on an ongoing security situation, it is less acceptable for NGOs that are dependent on donors, limited project funding and, by extension, publicity.

While most informants would say that the method of analysis follows the problem they are trying to tackle, this section argues that the problem set is co-produced by the potentials and constraints of satellite technology. It debunks repeated claims of unbiased, global coverage of commercial satellites. Tracing the politico-orbital conditions of non-governmental remote sensing highlights how satellite technology affects the way NGOs and think tanks problematize security. The commercialization of satellite imagery has been a boon for non-governmental access that is sustained by government and military demand. However, the central role of governments as regulators and major customers of commercial satellite imagery providers introduce a bias into which areas are most frequently imaged. This bias is implicitly perpetuated by availability and economic constraints that affect non-governmental users.

5.3. Imagery Interpretation: Translating Matter into Security Threats

Once the satellite imagery is acquired, non-governmental actors start analyzing it. Working with imagery creates the illusion of straightforward and easy analysis. After all, one can allegedly see what is happening, see the security threat. Scrutinizing the aspirations for visual and scientific accuracy, the following section focuses on the interpretive process of translating satellite data and the objects it depicts into security threats.

5.3.1. Lack of Expertise

The initial complication is a lack of awareness and expertise in the non-governmental sector when it comes to satellite imagery analysis. In fact, when an NGO decides to buy commercial satellite imagery, this is already a big step. The relatively small number of non-governmental users is a testament to this condition. Despite high expectations since the commercialization of satellite

imagery, non-governmental remote sensing is far from an established and stabilized practice (Olbrich 2019c). Instead, users develop customized practices of imagery acquisition and analysis. Generally, there is still a widespread lack of awareness concerning the capabilities and requirements of the technology. One industry expert explains that "it doesn't even occur to them that there might be value in it. And even when it does, the actual process of trying to acquire it, is really frustrating, so that can turn off a lot of people. […] So even if you got the image, do you really know what to do with it?" (Informant #21). This especially applies to smaller NGOs that remain oblivious to the potential benefits of Earth observation or are discouraged by an uncertainty about the costs and necessary know-how. At the same time, active users of the technology are often limited to their very niche of expertise. They do not follow ongoing developments in the satellite imagery business and miss to acknowledge the availability of different sensors, new solutions by start-ups or government programs promoting free access to satellite imagery.

As a result, the largest share of non-governmental remote sensing sticks to electro-optical satellite imagery as the analysis of SAR or infrared imagery requires additional expertise. The advent of high-resolution satellite imagery has made the identification of objects and activities much easier. However, satellite imagery analysts agree that their work remains an interpretive process that is liable to human and technical errors. They describe it as a "sophisticated art and science" (Informant #46) because satellite imagery "can be misleading or if not misleading then just ambiguous" (Informant #13). Put simply, security threats are neither visible nor immediately apparent. Still less do overhead images convey the dangers or horrors they are to depict such as unlawful detention, torture, excessive labor and executions in North Korea's political prison camp system (see e.g., UN Commission of Inquiry on Human Rights in the Democratic People's Republic of Korea 2014).

Although vision suggests validity, satellite imagery is far from self-evident. Satellite imagery analyses are the result of human interpretation and easily result in different or contradictory assessments. This becomes problematic for research-intensive non-profits because they are dependent on their reputation for social impact and successful fundraising. They cannot afford to be wrong because it undermines their credibility. However, the number of people who have the capabilities to analyze satellite imagery in the NGO community is rather low. Organizations are staffed with policy analysts, human rights or security experts. As such, they are more familiar with survey and interview data but the "skill set for interpreting satellite imagery […] is a big challenge, of course, in the branch of the NGO community" (Informant #15). The remainder of this section presents how the non-governmental sector deals with the difficulties of EO technologies and satellite imagery interpretation and what this means for the problematization of security.

5.3.2. Learning-by-Doing and Its Limits

The first intuitive way of dealing with commercial satellite imagery has been to just conduct a visual analysis with the limited knowledge available. In the early 2000s, the expertise to properly analyze satellite imagery was – even more than now – tied down in government agencies and large companies. As a result early satellite imagery analysts have drawn on academic literature, which obviously focused on low-resolution sensors, as well as unclassified handbooks originally written for intelligence analysts, e.g. at the Defense Mapping Agency (1996). Some NGOs also have geographers on staff who are familiar with geographic information systems (GIS) software. Apart from that, non-governmental analysts go through a self-schooling process and slowly become familiar with overhead images of buildings, vehicles or environmental change. Over time, this learning-by-doing approach could be complemented by online courses that emerged in areas such as remote sensing technologies or geospatial analysis. Because imagery remains expensive for NGOs and think tanks, it is bought on an ad-hoc basis and discourages investments in the education of dedicated imagery analysts. This, of course, cripples any learning-by-doing efforts because it limits overall practice opportunities. The hard-earned knowledge and experience are passed on to new staff members in an apprentice-style manner in which new hires learn from self-taught employees.

Professional satellite imagery analysts acknowledge the importance of hands-on experience. At the same time, they highlight the necessary specialized training in order to get a proper understanding of the on-the-ground situation. This means, just looking at satellite imagery will not help analysts develop an understanding of what it looks like if a coalmine, fertilizer processing plant or chicken farm is operational or what conclusions can be drawn from a smoke plume or specific vehicle activity at a nuclear complex. Without a broader understanding of what can be seen from above, missile specialists might mistake regular transport trucks for transporter erector launchers. This is particularly true when a cognitive bias is triggered because an analyst has received information that something is happening in a particular area of interest. Overall, self-taught non-governmental remote sensing is at risk of overstretching interpretations. The latter is reinforced when analysts turn to more complex analyses and become complacent with their skills. Multiple non-governmental analysts report to have become too bold with an analysis or give in to the temptation of scoring a coup.

The commercialization of satellite imagery creates a vulnerability for people who jump to conclusions. Despite the danger of losing credibility, expert analysts complain that “some of the interpretation out there is incredibly horrible. It is not holistic, it does not use any real depth of knowledge on local culture, society, industrial procedures or anything like that. Quite often I laugh at what I see” (Informant #43). In fact, non-governmental remote sensing repeatedly leads to

controversial assertions about security threats. The Satellite Sentinel Project (SSP) observed the security situation in Sudan and South Sudan starting in early 2011. Comprised of different organizations including the Enough Project, UN organizations and DigitalGlobe, they relied on satellite imagery analysis by young researchers at the Harvard Humanitarian Initiative. While the inexperienced team could count on the support of DigitalGlobe's analysis team, it did not prevent eventual misinterpretations that required later corrections (Informant #13; see also Harvard Humanitarian Initiative 2011a; Harvard Humanitarian Initiative 2011b).

The visuality and apparent accuracy of satellite imagery further embolden analysts unfamiliar with its limitations. The Beyond Parallel program of the Center for Strategic and International Studies (CSIS) aims to provide objective information and clarity to decision-makers concerning Korean unification – albeit much of their analysis is focused on North Korea's economic and security situation. After North Korea's fourth nuclear test in early January 2016, Beyond Parallel issued a report that claims a significant reduction of economic activity on the Chinese-North Korean border (Beyond Parallel 2016). To arrive at this assessment, they count trucks, trains and boats in two satellite images from early 2015 to establish a baseline. They compare this to a third image from February 14, 2016 and find substantially less vehicles and activity. The think tank interprets this as "independent Chinese actions" to reduce trade in response to the nuclear test (Beyond Parallel 2016). The report does not indicate who conducted the analysis but the interpretation moves far beyond what can be derived from the imagery. At the outset, calculating a baseline of economic activity based on two images is at least carless. Any follow-up image might randomly indicate more or less activity. On top of that, Beyond Parallel compares the "baseline" to only one post-nuclear test image that has been taken one day after Spring Festival – a prominent, week-long public holiday in China – and would presumably suggest reduced economic activity by itself. Although the general methodology of comparing before and after imagery works in principle, the limited amount of data, inadequate timing and carless interpretation do not support the reported findings. Nonetheless, the report does not hold back to commend the power of satellite imagery in bringing the "on-the-ground reality into clearer focus" (Beyond Parallel 2016). This incident corresponds with the assessment of another experienced satellite imagery analyst who observes that public reports repeatedly rely on a handful of satellite images. He or she admonishes that many NGOs simply aren't aware of all of the things that they need to take into account and that they need to conduct satellite imagery analysis on a large scale and over a large amount of time. While SSP has publicly corrected its erroneous interpretation, Beyond Parallel has refrained from doing so. Instead, they have hired a well-known satellite imagery analyst of North Korea with decades of experience in the intelligence domain; conceivably, to avoid further errors.

Arguably, they are honest mistakes by large NGOs that strive for accurate and diligent interpretation. The growing availability of commercial satellite imagery, however, also invites individual amateurs to publish quick and sensationalist analyses on social media channels. In light of this development, several non-governmental analysts note that people "get a little overly excited about the abilities. Everybody thinks they're an imagery analyst" (Informant #4). The repercussions of this development are kept within reasonable limits if they focus on obvious change detection. However, they endanger the credibility of non-governmental remote sensing as a whole when venturing too far into a distorted interpretation. As satellite data and information gets more ubiquitous and more available to the public, it empowers more non-governmental players to weigh in on issues of significance to global security. But it also empowers amateur analysts who do not have any expertise to kind of muddy the waters.

The learning-by-doing approach of non-governmental actors introduces various uncertainties to the interpretation of satellite imagery. The great majority of NGOs and think tanks err on the side of caution because they are dependent on maintaining a good reputation and credibility. They only publish interpretation when they have high confidence in the findings or add an appropriate caveat. Still, a lack of expertise risks entirely missing or misrepresenting security threats. That is why some non-governmental organizations turn to professional imagery analysts who are trained to squeeze the smallest detail out of satellite imagery.

5.3.3. The Militarization of Non-Governmental Remote Sensing

Outsourcing the satellite imagery analysis to professionals enables more complicated interpretations that otherwise are beyond the skills of NGOs and think tanks. It enables non-governmental actors to actualize more potentials of commercial satellite imagery. Expert analysts can deduce more information from the way infrastructure is organized and what vehicle activity means in the larger context of the situation. In short, they potentially extract more value out of each satellite image. Therefore, even larger organizations like Amnesty International that had already established a dedicated GIS analytical unit moved on to hire a full-time, professional satellite imagery analyst. In addition to the more detailed and certain identification of objects on high-resolution satellite imagery, external analysts are also more likely to bring in knowledge about other spectral bands such as thermal, near-infrared or SAR imagery that would be inaccessible for NGOs.

Data collection for this thesis suggests that there is a very limited pool of professional imagery analysts offering their services to the non-governmental community. The rest of the much sought-after workforce is bound up with the government and commercial sectors. As a result, the costs of hiring professional analysts are rather high and add to the expenses for the commercial satellite imagery. Given the project-based funding of many, especially smaller, non-profits, it is more

sensible to spend a larger amount once than adding a permanent analyst to the staff. Unsurprisingly, then, DigitalGlobe also houses an analytics team and offers customers to buy satellite imagery including the analysis, which of course drives up the price. In that case, chances are that the NGO receives a report drafted by a satellite imagery analyst with intelligence experience. Following various mergers and as a consequence of its close cooperation with the government, DigitalGlobe has attracted various former intelligence and military analysts to offer their skills in the private sector.

Similarly, the freelance imagery analysts that provide their services to the NGO community often have a military or intelligence background. Especially when it comes to granular analysis of high-resolution satellite imagery, human rights groups as well as security think tanks rely on the same analysts. In the environmental and humanitarian areas, academics and university researchers also engage NGOs to support their imagery analysis. Moreover, there are a number of start-ups that develop automatic change detection of large amounts of satellite data. However, only rarely does this approach match with the analytical needs and limited budgets of NGOs. In contrast, being trained as an imagery analyst for one of the military services or intelligence agencies involves poring over image after image to identify military infrastructure. This detailed knowledge about the appearance of objects and activities on overhead imagery is closely related to non-governmental remote sensing.

The analytical expertise gives authority to external analysts when working with NGOs. This is reinforced by the inexperience with remote sensing in the non-governmental sector. In the end, NGOs trust the interpretation of the analysts. Buying external expertise for training or analysis purposes often means cooperating with former government analysts that work directly for the imagery providers, as freelancers or other analytics companies. The analytical products and services are tailor-made for the regular customers from the defense and intelligence sector. They cannot be directly transferred to the needs of NGOs: “Sometimes, when the organization pays the imagery provider to do the analysis, it comes out more like a military analysis rather than a human rights analysis. Because they don’t have their human rights glasses on” (Informant #4). This is unsurprising since the government training most likely did not cover human rights or environmental degradation but rather military activities and national security. It produces experts in identifying weapon systems or hidden infrastructure and interpreting the capabilities of armed forces. This way, external analysts carry their expertise into the non-governmental domain without the special training or a proper understanding of the political situation on the ground. While at least larger NGOs increasingly build up in-house expertise, it proves generally difficult to appropriately transfer the former military practices into the development, humanitarian and human rights area:

Some of them are professionals, who have been doing this for decades in some cases. Now obviously, their focus has been different. They have been focusing on defense related issues. This is a very interesting angle and we discover interesting things to say the least, when these very same experts sit down with us and realize that they have been looking for other things and they haven't been necessarily focusing on those details that might be more relevant to the work that we do (Informant #38).

These professionals are experts at feature identification and easily make out conventional military facilities, copper mines or missile factories. However, it risks overlooking essential details for a human rights or humanitarian analysis. Moreover, the unfamiliarity with certain civilian infrastructure might lead to interpretations that take it as military-related. Naturally, this improves over time as the limited number of professional analysts available for the non-governmental community grows increasingly versatile. Instead of staring at the same area or conflict for months, they are hired for a variety of jobs across issue areas and geographic locations. Nonetheless, drawing on analysts that are deeply ingrained in military work locks non-governmental remote sensing into a particular way of analysis that searches for insecurity, damage or misbehavior. In doing so, NGOs and think tanks are prevented from moving towards other, more constructive directions that take into focus how to improve agricultural management or civil infrastructure planning and highlight shortcomings to local decision-makers or, more generally, offer support in the pursuit of the sustainable development goals (see chapter 8).

Instead, the skills of a military-inspired way of seeing are transferred to the non-governmental sector. As inexperienced users of remote sensing, NGOs and think tanks tend to adopt military-intelligence methods of analysis. This includes the language, annotations and, arguably, what is problematized on an image. In the course of this, military parlance has crept into NGO reports despite efforts by NGOs to amend the often sober, descriptive and technical language. As a result, the Committee for Human Rights in North Korea (HRNK) finds that prisoner housing and other buildings "appear to be moderately well maintained and in a moderate state of repair" (Bermudez, Dinville, and Eley 2016: 33). In their report about the actions of Myanmar Security Forces against the Rohingya, Amnesty International repeatedly assures that "analysis of satellite imagery corroborated witness accounts" (Amnesty International 2018: 106). Lastly, SSP does not directly name objects in satellite imagery but limits itself to technical descriptions that they are "consistent with" tanks, airplanes or other things (e.g. Satellite Sentinel Project 2013: 6). Interestingly, this practice has quickly taken hold in non-governmental remote sensing. Beyond the linguistic changes, the skill transfer introduces a military dimension into non-governmental remote sensing. Human rights experts learn to identify tanks and artillery, which produces gaps when it comes to more civilian-centric perspectives on, for instance, IDPs in refugee camps. This bias towards a

military analysis distracts from the human rights focus, as one imagery analyst reports: "I've seen that in some cases where people start off trying to document human rights violations but then get sidetracked into only like 'we tracked this tank and then we saw it over here.' And I was like, 'guys, a tank is not a human rights violations'" (Informant #4). In doing so, it does not stop at awkward linguistic descriptions. Instead, military-focused problematizations themselves creep into human rights analyses by way of satellite imagery. In other words, the military roots of remote sensing technologies have outlived the commercialization of satellite imagery and influence the analytical practices of non-governmental users.

5.3.4. The Materiality of Security Threats

The holdover of those military roots finds expression in the satellite imagery analysis. This sub-section argues that the interpretation of satellite imagery is about the translation of matter into security threats. Imagery analysts merely perceive visible objects on the satellite image which are constructed as proxies or indicators of suspicious events. This process risks simplifying or even misrepresenting security threats.

Imagery analysts are limited to what they actually see. In this sense, materiality constitutes a sine-qua-non for security threats. When satellite imagery analysts have ordered an image for analysis they are looking for unusual objects or material change. They note all remarkable features and compare them to another image. Only then follows the next step of trying to figure out the meaning of those features in the broader picture of the area of interest. It follows that materiality defines the space of potential security problematizations. Some things are clearly identifiable. Runways that also show a number of airplanes parked on the side are straightforward to recognize even for laypeople. However, it requires more information to determine what it means and what is happening in the buildings around it. Moreover, given the orbital and technological constraints (see section 5.2.), it is virtually impossible to continuously track security threats in a satellite live feed or even identify individual persons on a satellite image. Accordingly, high-resolution satellite imagery is believed to hold more information, to be more convincing and to require less training (cf. Olbrich 2019a). In contrast, low-resolution satellite imagery produces less security threats. So when the European Union implements its civil remote sensing program Copernicus, it limits the kind and depth of identifiable security threats by restricting the resolution to 10m.

As such, the image never has the whole story. Because of the limitations of satellite imagery in terms of material security threats, analysts draw on additional information and supplementary data. Virtually all informants agree that satellite imagery works best in conjunction with other sources: "Satellite imagery is not that helpful on its own. This is an insular discipline but not a useless one – obviously. But if you don't have context, if you don't have the on-the-ground imagery, there's not a lot of problems you can solve alone with it" (Informant #14). What many analysts

describe as context is quite broadly conceived. This could be information that initiates the analysis. For example, satellite imagery can be used to verify or refute media reports about the deployment of weapon systems, spontaneous settlements of refugees or the clearing of woodland. Additionally, the analyst can move beyond the materiality of the image and complement their analysis with information from academic and media sources. Satellite imagery also helps with geolocating where and when an event took place. If a video claims to show aerial bombing in Syria, particular features in that video such as a large building or a mountain range indicate a location that can be confirmed with overhead imagery. If the large building is severely damaged in the video, satellite imagery even allows narrowing down the timeline of events. Similarly, context could mean witness testimony about the location of mass graves or illegal waste disposal. In one remarkable instance, satellite imagery analysts collaborated with North Korean escapees from political prison camps. They printed out satellite images on large paper rolls and collectively analyzed them. As the camps can look like regular villages in North Korea, the context information provided by the refugees has been essential to confirm the existence and location of the camps and even determine the function of particular buildings. Because of the overall importance of context information for the analysis of satellite imagery, non-governmental actors are increasingly interested in foreign language skills to be able to mine additional sources. By the same token, this suggests that the reliance on satellite imagery increases in inaccessible and low-information landscapes such as North Korea's nuclear complex. Regardless of the available context information, many NGOs and think tanks have established informal peer-review processes. In order to diminish the impact of cognitive biases and speculation, fellow analysts or area specialists review written imagery analyses.

However, this does not mitigate the limitation that material security threats are rarely obvious on the satellite image. The satellite image does not depict the nuclear bomb on the test stand or catches human rights violators in the act. Analyses of North Korea's nuclear test site are rather restricted to observing vehicle activity or changes in the spoil pile from digging test tunnels. Similarly, disturbed earth or burnt villages potentially correlate with reports of the discovery of mass graves or militia violence but they usually do not capture how the event is taking place. In short, satellite imagery analysts need to rely on a number of signatures that indicate the existence of a particular security threat. Signatures are highly-context dependent in that they are derived from additional background information. If analysts are familiar with the operations of a uranium mine or the nuclear fuel cycle, they come up with a number of signatures that approximate the current activity level on the ground. In other instances, fallow or overgrown agricultural fields might indicate forced migration. Lastly, because it is difficult to find military forces deployed in the field, observing known military bases for visible changes could be an indicator of conflict or general military activity. In addition to these optical signatures, thermal signatures can be used to

determine if a power plant or nuclear reactor is operating. Given the importance of material change for the analysis of satellite imagery, analysts keep libraries of signatures that contain shots of different kinds of vehicles, weapon systems or civil infrastructure as a baseline for later comparison. Despite the context dependence, there are particular technical necessities that facilitate the development of signatures. For instance, ballistic missile storage sites share some common features across contexts as one analyst explains:

> *Because I've done this before, I know off hand that ballistic missiles are fairly dangerous to store. Solid-fuel ballistic missiles are fairly dangerous to store, because if someone lights a fire near them, they tend to go off. That's bad. So, they tend to have special storage techniques. I am not off hand familiar with those special storage techniques. However, I know a whole host of countries that build both solid fuel ballistic missiles, solid-propellant space launch vehicles […] Now I understand that the ones in the EU and the U.S. have been doing this for decades, so they're gonna do it a little differently than someone who's been doing it for half a decade. […] So, I understand it's not gonna be a perfect match. But there are certain things you can't avoid. So, I try to answer the question what is the core visual signature of this that I can derive purely from visuals and some supporting data that I can then apply elsewhere (Informant #14).*

In essence, more open countries are used as reference points to establish global signatures for other countries. The intelligence community has similar guides and handbooks that explain in detail how developments on the ground appear on satellite imagery (e.g. Defense Mapping Agency 1996). Effectively, these signatures serve as stand-ins or material proxies for security threats. In this understanding, satellite imagery keeps moving further away from the idea that security threats can be seen with your own eyes. Rather, security threats are the result of an elaborate translation from the materiality a satellite image depicts. In doing so, satellite imagery moves closer to statistical indicators that compile various measures to approximate or represent reality. This entails various implications for the problematization of security via satellite imagery analysis.

First, focusing on the materiality facilitates the construction of security threat. Satellite imagery emphasizes the materiality of security threats whereas alternative sources usually rely on interpretation of public statements, presumed intentions and political strategies. In these cases, the material focus of satellite imagery spearheads the hierarchy of evidence. In this vein, when satellite imagery detects the construction of new runways, analysts are quick to compare their length to the minimum distances required by military airplanes for take-off and landing despite verbal assertions of their peaceful purpose. This risks militarizing the meaning of those runways whose actual use cannot be derived from their materiality alone. Similarly, increased

vehicle activity or emissions from a ventilation stack of a nuclear reactor become tantamount to a restarted nuclear weapons program. In doing so, material explanations of insecurity are pitted against discourse analyses or verbal assertions of a peaceful agenda. In this sense, non-governmental remote sensing risks complicating the desecuritization of material observations.

Second, and relatedly, the materiality of security threats predefines the problem space of non-governmental efforts. To put it crudely, since immaterial changes cannot be captured by satellite imagery, they do not appear on the agenda of NGOs and think tanks. Using satellite imagery emphasizes large, material security problems over others: "if there were a way to detect if plantations were using illegal labor or child labor with satellite images, we would be interested" (Informant #32). In this example, the potentials and constraints of remote sensing, however, only allow for monitoring illegal land burning so that the technology prescribes the problematization. Surely, NGOs have a variety of reasons to choose different objectives and areas of focus. However, the point is rather to recognize the bias technology introduces into these decisions. In this sense, satellite imagery co-produces the mission if its affordances dictate the most promising issue "just because it's very visible" (Informant #24). This technological bias also comes in after those objectives have been set. For example, when NGOs seek to monitor and document human rights violations, the sheer materiality of tanks, artillery and airplanes easily distracts from this mission because they are more easily identifiable on satellite imagery, nudging the mission into a conflict analysis.

Third, satellite remote sensing risks simplifying or even misrepresenting security threats. Reducing threats to material proxies fades out important contextual factors. With respect to the case of North Korea's nuclear program and human rights record, I have argued elsewhere:

> *The satellites' targeted and unidirectional gaze absolves others from accountability for existing insecurities as their material origins are limited to North Korean territory. In doing so, the hierarchy of evidence risks reducing the complexity of the insecurities to material manifestations and externalizing the sole responsibility to North Korea. Put differently, the continuous view from above is conducive to oversimplifications of security problems. The specific practices and relations that are in place to tackle the problematized uncertainty surrounding North Korea produce an authoritative knowledge account of the human rights and security situation at the risk of casting aside significant contextual factors. Only to name a few tangible examples, this arguably bears the danger of obscuring the relevance of UN sanctions, China's mixed track record of implementing them or its position towards North Korean refugees who are classified as economic migrants and repatriated to experience punishment at the hand of their own government. Similarly, this applies to the deployment of*

roughly 29,000 U.S. soldiers on the Korean peninsula, annual large military maneuvers of the U.S. and South Korea, and the role of China's military modernization in U.S. security strategy (Olbrich 2019a: 78-79).

As remote sensing emphasizes the materiality of security threats other dimensions lose significance. This problem is exacerbated by the use of material proxies that by definition are simplifications of a security situation. They concentrate on how the situation appears in its materiality rather than on how it came about and what other options were on the table. Because remote sensing is so fixated on the problematization, it is less surprising that analysts recognize that "there aren't a lot of compelling ways to use satellite imagery to explain the solution" (Informant #7). In fact, the material fetishism introduced by satellite imagery rather risks narrowing the zone of possible solutions because it emphasizes material change over change of use and meaning. Going further, the danger of misrepresentation of security threats has already been hinted at with the example of Beyond Parallel's analysis of vehicle activity as an indicator for the impact of sanctions on Sino-North Korean trade. In this case, it was rather easy to identify the shortcomings of the imagery analysis. However, it becomes more difficult with automated satellite imagery analysis that applies a once defined material proxy at scale because it is biased towards large, easy-to-detect material changes.

Overall, the section demystifies claims of straightforward, visual analysis of satellite imagery. Oftentimes, human rights violations, security threats or environmental crimes cannot be seen directly. Instead, the lack of expertise, military roots of and materiality focus involved in non-governmental remote sensing introduce various complications and biases. Still, remote sensing is referred to as a legitimate and almost scientific way to create knowledge about security threats. The following section looks at the processes that stabilize this reputation.

5.4. Reporting: Validating Effects of Vision and Matter

Security problematizations that depend on a few satellite images are accompanied by written reports. Oftentimes, the most pertinent image is introduced early in the report and further distributed on social media – usually annotated to highlight the findings. In contrast, more sophisticated analyses of a large number of perhaps low-resolution satellite images require a more elaborate presentation. They are embedded in interactive platforms in which the viewer can choose from and manipulate different variables such as the time period, data source etc. Such databases also build the foundation of more detailed reports that include additional satellite imagery for illustration. Despite the downsides and biases inherent in remote sensing, non-governmental actors count on the persuasive character in legitimizing and validating the construction of security threats. This section identifies three mechanisms that reinforce the credibility and legitimacy of non-governmental remote sensing.

5.4.1. Visual Legitimacy of Security Threats

First off, despite the fact that satellite imagery is rarely obvious, the visuality inherent in satellite imagery promotes a sense of validity and legitimacy. Although it is impossible for most people to analyze a satellite image or only recognize an alleged tunnel or vehicle, the imagery adds credibility to the report. Paradoxically, the security threat itself is virtually invisible to most people but they can see it on the image. As such, the visual dimension of satellite imagery, at once, emotionalizes and validates the security threat.

To some extent, remote sensing is like peeking through a keyhole.[26] Part of the power of EO satellites is that they collect imagery over otherwise denied areas. These are areas too large to monitor from the ground or too dangerous or even forbidden to go to. It creates a fascination of seeing hidden places that is difficult to grasp without figurative language: "Satellite photos have this extra thing that they are always sort of…There is something spying about them. You almost get the sense that you're always looking in through a forbidden lens or something like that. It's looking over someone's shoulder" (Informant #15). Consequently, some of the first commercial satellite images acquired by non-governmental actors have been of sites such as Area 51 (Olbrich 2019c). Although the existence of this Air Force base was publicly known in the early 2000s, an overhead satellite image created strong interest because the location was still officially classified and virtually inaccessible. In this sense, it fits into a larger political narrative. It has a symbolic significance beyond the materiality it depicts: "A photo of Area 51 or a photo of a mass grave or a photo of Auschwitz has political significance because it demonstrates something that's happened. It makes a political point. It goes beyond just the technology or what the science says" (Informant #6). Despite the fact that imagery can be biased, impossible to decipher for a layperson or misrepresent a security threat, a report is still more convincing if it includes a satellite image. Essentially, its visuality rather appeals to an emotional impulse than a rational conviction. This effect is perhaps not well understood but recognized by non-governmental actors when they state:

i. *"A picture is worth a thousand words" (Informant #5);*
ii. *"For some reason it seems to amplify the veracity or the impact of the article" (Informant #18);*
iii. *"We still have the idea that seeing is believing" (Informant #32);*
iv. *"I don't have to believe your word if you can prove it to me with an image" (Informant #42);*
v. *"It is not just words" (Informant #50).*

[26] Tellingly, a prominent series of U.S. spy satellites has been designated Keyhole (KH).

Satellite imagery legitimizes reports about security threats because it suggests that anyone can see for themselves. Satellite imagery is perceived as external to or even above discourse; it is more than "just words". In doing so, the visual dimension reinforces the function of satellites imagery as a simplification tool (see section 5.3.4.). Reducing a security threat to its visuals makes it seemingly easier to comprehend since the story unfolds in front of your eyes. As a result, it also becomes more attractive for different media outlets to pick up an NGO report that includes satellite imagery that at once encapsulates the complexity of a difficult security situation. This could be an image of the destruction of Raqqa (Lubin 2017), how a Ugandan village becomes the host of more than 250,000 refugees (Hodgson 2018) or hundreds of cars clustering around a crossing point at the Syrian-Turkish border (BBC 2014). In doing so, the visuality of remote sensing makes an effective tool to simplify, emotionalize and draw attention to otherwise less prominent issues.

At the same time, satellite imagery is imbued with credibility by way of visual markers. Satellite images of human rights violations, nuclear tests or environmental degradation are rather inconspicuous and unremarkable. In fact, a layperson would have difficulties to identify them at all. Satellite imagery of North Korea's nuclear test site appears almost dull, similar to an arbitrary mountain range or mining activities. Satellite imagery analysts need to know what they are looking for and translate their findings for the common viewer. This results in a number of arrows, annotations and captions that are added to the satellite image. Only then, the imagery becomes legible for everyone else. The objects are explained in their specific material and political context. Now, even unexperienced viewers confidently identify grey piles as spoil from nuclear test tunnels.

Effectively, analysts have to explain to the viewers what they are supposed to see in an image. Consequently, satellite imagery is usually embedded in a report that meticulously describes what can be derived from the visual evidence. In some instances, analysts could also convey their message without including the satellite image because it is impossible for most readers to match it with the written description anyways. However, the combination of the visual appeal and the allegedly obvious, descriptive annotations create a visual legitimacy that is effective across contexts. Once "the satellite data stream is transmitted to a ground station, computed, transformed into an image, perhaps pan-sharpened and made legible, it becomes a mobile thing that is neither purely knowledge nor material. Rather, it is part and result of an assemblage of cameras, rocket technology, government regulations, international law, GIS software, analysts and so on. This new mobile thing is then relatively stable in various contexts such as intelligence briefings, lecture rooms, television shows or newspapers" (Olbrich 2019a: 76; see also Rothe 2015). In this sense, the annotations of satellite imagery reinforce the visual appeal. Only when

security threats are represented by large material changes that can be easily detected on high-resolution imagery, annotations become expendable. Images of island reclamation activities by China, Vietnam and other nations in the South China Sea are a pertinent example. The emergence of new sandy islands against the contrast of a turquoise sea develop their very own aesthetics. The aesthetics of remote sensing nurture a common belief that "with imagery comes credibility and a certain amount of science" (Informant #5). In other words, the legitimacy of security threats is not only derived from the visual but also scientific appeal. It not only emotionalizes but also rationalizes security threats.

5.4.2. Material Authority of Satellite Imagery

Satellite imagery is imbued with a material authority. In addition to the visual dimension, non-governmental actors emphasize that it is objective, scientific data. Contrary to what has been argued in the preceding sections, they claim that it lacks political bias. Eyewitness testimony, on the other hand, is subjective, "often unreliable and by nature qualitative. Satellite imagery is quantitative, it's digital, it's here. You can put it out there" (Informant #3). Despite the necessity of human interpretation to make it legible, satellite imagery is presented as quantitative, objective data. It fits into a hierarchy of evidence that favors materiality over verbal testimony. The evidentiary character allegedly builds an impartial foundation of knowledge "so people can make their own choices about whether or not threats are worthwhile and whether or not they should be worrying about this" (Informant #14). Non-governmental actors nurture the alleged objectivity and evidentiary character of satellite imagery to legitimize the creation of security threats.

Further, they attempt to follow and associate themselves with scientific methods which reinforce the perception that security threats are backed by credible evidence. For doing so, reports present the different steps of satellite data acquisition and analysis in a transparent manner:

> *"what we strive to do is be very public and transparent about the data sources that we're using and the assumptions that we're making when we publish an analysis or an opinion that is based on imagery. So that other people, if they wanted to come up with their own opinion, could go back to the same sources we use and take a look for themselves"* (Informant #33).

Indeed, NGOs and think tanks consistently state the sources of satellite imagery to allow for replicability. However, as mentioned above: Even looking at the same image can lead to different results. Consequently, analysts stick as close to the data as possible. In doing so, they make distinctions between imagery analysts and political analysts. While the former errs on the side of caution, the latter is encouraged to make interpretive leaps that involves supplementary, speculative and theoretical information. Both, however, benefit from the additional credibility

satellite imagery adds to their claims. As a result, a satellite image is sometimes even included in reports if they only have an illustrative rather than argumentative function. Lastly, satellite imagery analyses tend to share a common way of speaking that expresses cautious pondering of potential findings. In addition to some military parlance (see section 5.3.3.), non-governmental actors make sure to refrain from absolute statements: "We would say this is probable or this is corroborated. We wouldn't insist that is the absolute truth, we would say this is what the evidence shows" (Informant #13). Staying as close as possible to scientific habitus, language and methodology further validates security threats found in commercial satellite imagery.

5.4.3. Adding Socio-Political Authority

The credibility of security threats and non-governmental remote sensing also grows when the satellite imagery is picked up by other socio-political authorities. When these authorities refer to or embed satellite imagery in their own work, concerns about biases of satellite imagery, that are introduced during the acquisition and interpretation process, increasingly fade out (Olbrich 2019a). As mentioned above, satellite imagery becomes highly mobile across contexts once it is analyzed and annotated. Consequently, it is easy for a host of institutions such as parliaments, governments, foundations or the media to pick it up and transfer it into the public. In doing so, remote sensing is rendered functional and legitimate as a method to identify global insecurities.

Newspapers, news agencies and TV stations regularly pick up satellite imagery analyses in their daily reporting. NGOs and think tanks have noticed the interest in the visualization of ongoing security hotspots. As a result, non-governmental actors often approach different major news outlets or agencies prior to publication to ensure ample media traction. Having said that, the visual appeal of satellite imagery alone does not suffice for a story in the New York Times. Journalists are sensitive to the newsworthiness of a story. This means that they are more interested in satellite imagery of Chinese activities in the South China Sea while Vietnam and other states receive less attention. As most NGOs and think tanks are dependent on donations and, by extension, publicity, the incentive structure favors those security threats that are deemed newsworthy. All the while, the tension between the difficulty of imagery interpretation and the persuasiveness of the visuality and materiality of satellite imagery also find expression in media reporting. Simply put, there is a risk of journalists misrepresenting security threats and not conveying the caveats related to satellite imagery analysis.

In March 2018, the New York Times reported that North Korea is "firing up a reactor" in Nyŏngbyŏn (Lai, Broad, and Sanger 2018). The journalists had drawn on a report of satellite imagery analysts at Stanford's Center for International Security and Cooperation (CISAC) which had identified emissions from the stack of North Korea's experimental light water reactor (ELWR). Only two days later, analysts at 38 North published a commentary that criticized both the original

analysts as well as the journalists. First, 38 North questioned the presence of emissions from the ELWR's ventilation stack which were adduced as the indicator for reactor activity. What was identified as vapor "may simply be a ground feature of a lighter color" (Pabian, Bermudez, and Liu 2018c). Second, they argued, the New York Times slanted the analysis. The journalists mislabeled satellite imagery and went too far by suggesting that the reactor is beginning operations. Because even if emissions were visible, this would merely indicate a checking of ventilation systems and by no means the initiation of operations. This example both illustrates the inherent difficulties of satellite imagery interpretation as well as how security threats can easily be misrepresented in public. In another case, the same New York Times journalists overstretched the findings of a satellite imagery analysis of North Korea's missile program. The reporting was subsequently criticized by other outlets and imagery analysts (Sanger and Broad 2018; Shorrok 2018). This form of medial misrepresentation is careless, if not dangerous, as the identification of security threats is related to and creates public expectations of government responses. In light of the activity at the ELWR in Nyŏngbyŏn, the New York Times journalists set the goal for the Trump administration to make Pyongyang give up its nuclear facilities. In the case of the missile program, they suggested that the North Korean government was deceiving the U.S. and its allies. The controversies about satellite imagery analyses, however, are confined to expert circles and are not addressed in the newspaper which stood by its story. The additional translation of material security threats from the imagery analysis into other formats bears the danger of further bias. Overall, however, the inclusion of commercial satellite imagery in familiar settings such as major press outlets normalizes and legitimizes non-governmental remote sensing as a practice to identify security threats.

Leading to a similar effect, satellite imagery analyses are also picked up by other socio-political authorities. A particular upside of commercial satellite imagery for governments is that it is not classified. It can be freely shared with allies and the public without disclosing the capabilities of government satellites. As a result, commercial satellite imagery is repeatedly used by government as part of their foreign policy – for example, NATO used commercial satellite imagery to show Russian military personnel on Ukrainian territory (North Atlantic Treaty Organization 2014; see also Shim 2018). Non-governmental remote sensing is also cited by the U.S. State Department in its human rights reports (e.g. U.S. Department of State 2017) and appears in other institutionalized processes such as testimony before committees of the U.S.-American Senate (e.g. Cha 2015) or House of Representatives (e.g. Scarlatoiu 2014). Lastly, the United Nations have begun to adopt non-governmental remote sensing in a similar form as human rights NGOs. One pertinent example is the UN Commission of Inquiry on Human Rights in the Democratic People's Republic of Korea (2014). In addition to extensive refugee testimony, the report frequently draws on commercial satellite imagery that was analyzed by non-governmental groups such as HRNK or

Amnesty International. In doing so, the UN commission promotes non-governmental remote sensing as an effective and legitimate means to monitor and document human rights violations.

As media outlets, national institutions, international organizations and other socio-political authorities increasingly endorse commercial satellite imagery, it is perceived as less unconventional, gains legitimacy as an observation tool and becomes more broadly accepted as evidence. Effectively, the problems and concerns about the identification of security threats via satellite imagery are not solved. However, they fade to the background during the conversion of satellite imagery "into a mobile thing and its introduction into public political processes" (Olbrich 2019a: 77). As a consequence, non-governmental remote sensing is rendered a functional and legitimate tool to create credible security problematizations.

5.5. Conclusion

The chapter shows the various ways in which human and technological factors interact in non-governmental remote sensing to create security problematizations from the bottom up. The potentials and constraints of satellite technology co-produce security threats and render them credible. More specifically, this addresses three myths or common misconceptions when it comes to the use of satellite imagery in security governance.

Myth #1: Commercial remote sensing produces a stockpile of global, universal and unbiased satellite imagery.

The first section focuses on the collection of satellite imagery and how non-governmental users acquire it. The material affordances of EO satellites already pre-define the possibility space of which security threats can be addressed. The spatial, spectral and temporal resolution of satellite imagery facilitates the identification of some threats while blocking others. Commercial EO meets a rather permissive international regulatory landscape. However, imagery providers remain closely intertwined with national governments and their defense apparatus. As major regulators and customers, governments hold substantial sway over national remote sensing so that the actual contents of the term "commercial" vary significantly across jurisdictions. More specifically, governments still affect what technologies and companies succeed and which areas of the globe are regularly visited by high-resolution satellites. In doing so, the defense and intelligence communities co-determine the ultimate content of imagery archives. They produce particular concentrations, silences and gaps in collections of satellite imagery providers. Price constraints force non-governmental actors to mainly fall back on this archival imagery. Conceptualizing the archive as "the law of what can be said" (Foucault 1972: 129), this constraints the selection and extent of problematizations non-governmental actors are able to address. Further, it introduces an inherent bias towards government interests, non-Western countries and security hotspots in

line with national policies. Taken together, the section reveals techno-political biases inherent in non-governmental remote sensing. Non-governmental users face an already skewed repository of satellite imagery that affects which and how they problematize security threats.

Myth #2: Non-governmental remote sensing enables seeing security threats.

Satellite imagery analysis is difficult and liable to human and technical errors. Security threats are not immediately apparent or visible as such on the image. As a consequence, NGOs and think tanks have developed idiosyncratic, customized ways of handling satellite imagery analysis. The learning-by-doing approach limits non-governmental actors to problematize obvious, large-scale security threats. As demonstrated, when inexperienced analysts tackle more complex security problems they risk overstretching or misinterpreting imagery. External analysts with military or intelligence experience introduce their own biases into non-governmental remote sensing. Effectively, they perpetuate the military roots of EO technologies and risk militarizing the mission and findings of NGOs that are usually many degrees removed from government or military interests. Regardless of the approach, satellite imagery analysis means the translation of matter into security threats. They are converted into material proxies. Although satellite imagery does not represent naval strategy, military planning or threat perceptions, an empty naval base might be rendered suspicious. The material fetish of non-governmental remote sensing prioritizes security over other dimensions, narrows the potential problem space and simplifies or even misrepresents security threats.

Myth #3: Remote sensing is an inherently legitimate and scientific technique.

The last section deconstructs how non-governmental remote sensing is rendered a legitimate surveillance practice to create valid security threats. This means legitimacy is not naturally given to satellite imagery but consistent efforts effectively maintain this understanding. Paradoxically, despite the uncertainties involved in satellite imagery analysis, the visuality itself serves to emotionalize and validate security threats on satellite imagery. Moreover, the translation into material proxies transports a sense of scientificity and objectivity. For this, analysts follow a scientific habitus, language and methodological demeanor that adds credibility to security threats. Lastly, the legitimacy of non-governmental remote sensing is reinforced when established and trusted institutions endorse its methods and findings.

Overall, the chapter has revealed the practices that elevate non-governmental remote sensing to a functional and legitimate way to problematize security. However, an uncritical acceptance of security threats that is driven by the trust in the objectivity of satellite imagery is misleading and hazardous. The analysis has shown how the potentials and constraints actively preselect, shape

and co-produce security threats. The following chapter raises the level of abstraction and looks at the coordination of non-governmental remote sensing. It identifies that different modes of non-governmental remote sensing have emerged and stabilized. Each of them emphasizes different potentials and constraints of satellite technology in accordance with their goals and capabilities.

6 A Typology of Non-Governmental Remote Sensing

6.1. Introduction

Since the U.S. commercialization of high-resolution satellite imagery in the late 1990s, NGOs, think tanks, universities and other non-state actors have gained access to a hitherto exclusive government resource. Starting in the 1970s the U.S. government has financed and operated the Landsat program to produce mid-resolution satellite imagery for Earth Science research. This has given the scientific community continuous access to civil remote sensing data to observe large-scale changes of the planet's environment. However, the resolution is too coarse to reliably identify smaller details such as vehicles, buildings, roads etc. Higher-resolution remote sensing remained a restricted practice limited to the military and intelligence community. Accordingly, government satellite imagery is classified and cannot be shared publicly to protect the satellites' technical abilities. The advent of commercial high-resolution satellite imagery, then, has raised expectations that non-governmental actors monitor government actions, security threats, the status of human rights and environmental changes on a global scale (Olbrich 2019c). The access to Earth observation satellites was to make journalists, NGOs, companies and academics "imagery activists" that would draw global attention to public policy issues (Baker 2001; Baker and Williamson 2006). Some have called it a geospatial revolution because they assume that commercial satellite imagery is broadly picked up by NGOs and makes a lasting impact across a great number of industries and government domains (Masback 2015; O'Connell 2017).

This chapter sets out to scrutinize these assumptions and expectations. For this, it poses the question how non-governmental actors adopt commercial satellite imagery. How do they integrate the technology into their regular operations? Taken together, what types of non-governmental remote sensing emerge and stabilize in terms of users, practices, goals and issue areas? The chapter argues that the uptake of commercial satellite imagery by the non-governmental sector has not been swift, universal or uniform. Instead, the analysis shows a more fragmented picture. A discussion of the initiation phase of non-governmental remote sensing makes clear how non-governmental actors come to pick up satellite imagery as a data source to begin with. Presented with this technology, they have developed and stabilized elaborate practices of enrolling remote sensing data in their operations. These practices differ significantly. Actors make use of different remote sensing products, analytical practices and tackle various problematizations for differing purposes. For tracing these emergent typologies, the chapter maps four modes of remote sensing that have become prevalent in the non-governmental domain. They are largely defined by two characteristics: Their emphasis of potentials of remote sensing products as visual imagery or data as well as their predominant goal they seek to address by way

of satellite imagery. All in all, the chapter argues that there is no uniform geospatial revolution in the non-governmental sectors. Instead, non-governmental actors have variously integrated commercial satellite imagery into their operations leading to four distinct modes of non-governmental remote sensing.

6.2. Initiation of Non-Governmental Remote Sensing

Given the military roots of remote sensing, one of the biggest obstacles for non-governmental actors to pick up satellite imagery remains a lack of awareness. This does not necessarily pertain to the general possibility to use satellite imagery. Rather, many non-governmental actors are oblivious to the acquisition process, costs, methods of analysis and, frankly, applications and problem sets. In the non-governmental domain, individual champions and proponents of remote sensing have promoted its benefits to the overall community – incidentally defining new problems that could be tackled by way of satellite imagery. In fact, the initiation of remote sensing projects can often be traced back to the efforts of a relatively small number of individuals. In the early 2000s, industry representatives, who were familiar with the defense applications of satellite imagery, promoted the value of remote sensing technology to NGOs and think tanks in the Washington, D.C. area. One of the early-adopters of commercial satellite imagery is the American Association for the Advancement of Science (AAAS). In 2007, it institutionalized the Geospatial Technologies and Human Rights Project to promote the use of satellite imagery for human rights. In this program, NGOs approach AAAS with an ongoing project – usually in the context of an active conflict or remote location. AAAS assesses how remote sensing technologies can be applied and delivers a satellite imagery analysis for free. The inquiring NGOs can then use it for their reporting or advocacy efforts. A collaboration of this kind also planted the seed for Amnesty International's use of satellite imagery. What started out as a joint effort with AAAS has turned into an in-house geospatial analysis team contributing satellite imagery as well as other geospatial analysis to Amnesty International projects. Similarly, Human Rights Watch worked together with AAAS before hiring full-time geospatial analysts to work with satellite imagery. In the more security-oriented think tank environment, former government employees provide the knowledge and personal relationships to introduce geospatial products. Overall, the initiation of non-governmental remote sensing – especially at the beginning – depends on personal contacts and face-to-face interaction that are able to present the technology's potential, explain its constraints and clarify misconceptions.

The personal interactions are the first step to initiate pilot projects. The AAAS program was successful because it tackled various shortcomings of NGOs at once including a lack of awareness, analytical skills and vision for how to apply commercial satellite imagery. Pilot projects temporarily suspend these barriers to show users the value of remote sensing for their immediate

operations, media feedback and donor relations (Olbrich 2019c). By definition, pilot projects are temporary and rather serve to demonstrate the potential of the technology than establishing stable and sustainable processes. Hiring geospatial analysts and regularly purchasing satellite imagery requires substantial investment and a long-term commitment. Consequently, many non-governmental users did not advance beyond a project-based approach in which the use of satellite imagery is dependent on dedicated funds, discounted contributions by imagery providers or time-limited program support. The importance of personal relations and short-term pilot projects lead to a broad but sparsely connected network of non-governmental remote sensing. Professional satellite imagery analysts and promoters of non-governmental remote sensing constitute the few nodes and bridges between NGOs and think tanks. As a result, human rights NGOs, environmental advocacy groups and security think tanks might work with the same analysts and imagery providers but do not know the work of their colleagues: "They have no idea about other projects that are going on. It might even be the same area that they are working on but everybody's just doing their thing" (Informant #4). Even within the same issue areas, only a few connecting individuals are aware of the extent, methods and geographical area of projects. NGO representatives collaborate with a small number of people and focus on responding to current events and problems. There is no formal, overarching expert community to discuss and establish best practices or institutional knowledge for non-governmental remote sensing despite some efforts in this direction. Instead, the different clusters of non-governmental actors have developed different approaches of using satellite imagery. The following sections lay out a typology of four distinct modes of non-governmental satellite observation.

6.3. Four Modes of Non-Governmental Remote Sensing

In order to characterize the different modes of non-governmental remote sensing, two defining dimensions have emerged from the data that are best understood as continua. On the one hand, the goals of non-governmental actors can be gleaned from how they use commercial satellite imagery. On the other hand, whether non-governmental actors rather actualize the imagery or data potential of remote sensing co-defines and stabilizes their practices. These differences are mapped onto respective continua instead of categories. This serves to emphasize that there are no clear-cut boundaries between different manifestations of those dimensions. Instead, seamless transitions and mixed cases are possible. However, the classification is helpful to understand why and how non-governmental actors actualize specific potentials of commercial satellite imagery while disregarding others.

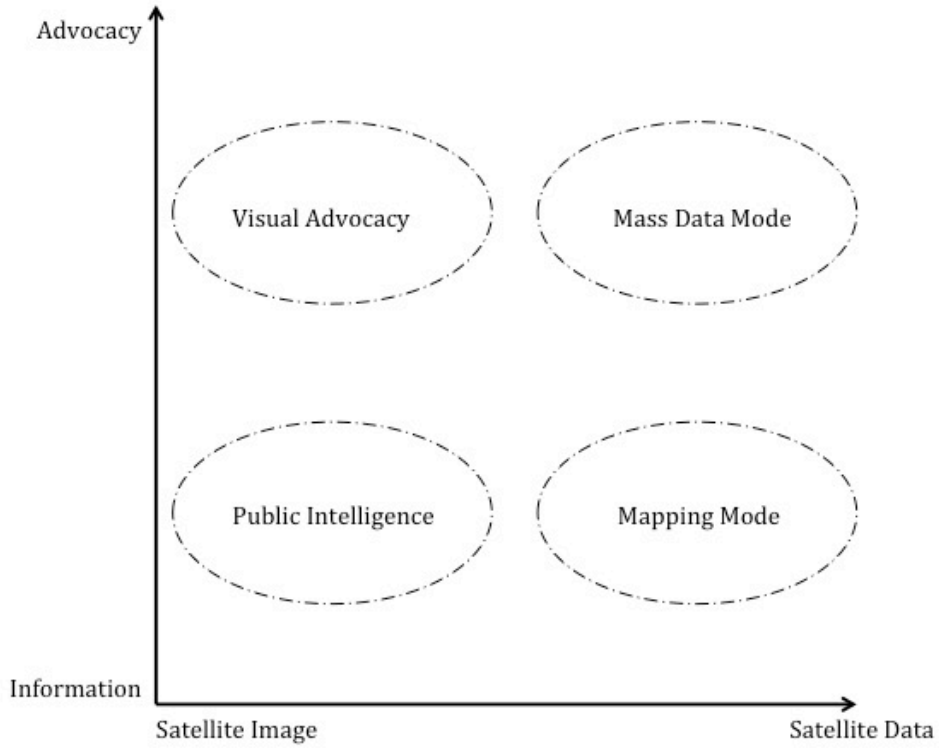
The first continuum deals with the goals of non-governmental users of satellite imagery. There is a broad consensus about the net benefits of transparency. A more detailed analysis reveals significant differences in the specific purposes non-governmental actors seek to achieve. More

specifically, the continuum runs from the provision of objective information to employing satellite imagery for advocacy purposes and creating political or legal accountability. Some non-state actors identify the lack of public information as the main problem to finding a solution to a security threat. In this line of thinking, it first and foremost requires more information to facilitate an evidence-based public debate and avoid that rumors and uninformed opinions lay the foundation of important policy decisions. Generally, such a lack of information can have various reasons from government secrecy, inaccessible and vast terrain or issue complexity. When it comes to questions of national security such as nuclear or other weapons programs, governments are usually reluctant to share information or even to verify or deny claims made in the public. Similarly, it is challenging to produce consistent and objective assessments of poverty, plant health and infrastructure such as pipelines, roads or power lines across large swaths of potentially inaccessible areas. Non-state actors then turn to commercial and open-source satellite imagery to produce allegedly objective, public information and assist a rational and sober policy debate devoid of rumors and politicized opinions. On the other end of the continuum, non-state actors seek to advocate a particular cause and, if possible, identify those politically or legally responsible for a security threat. Here, the problem is not necessarily a lack of information but rather a lack of awareness, public concern and the political will to act. Often aligned with the protection of international norms or global commons, satellite imagery is employed as evidence of norm violations – for everybody to see. Pertinent examples include the documentation and monitoring of human rights violations or environmental conservation efforts that can be seen from space in the form of razed villages or troop movement and decaying glaciers or deforestation, respectively. In short, moving beyond research and generating new information, some non-state actors employ remote sensing products in their pursuit for more immediate political impact and to create accountability for norm violations.

The second continuum differentiates which potentials of remote sensing is actualized: Are remote sensing products taken as satellite imagery or satellite data? In the face of a growing availability of remote sensing, it has become rather commonplace to assert that users do not care about an image but about the answer to their research problem (e.g. Pultarova 2017). Although this understanding can certainly be found in the interview material, it does not amount to a generalizable finding in the non-governmental domain. Instead, non-state actors equally highlight and make strategic use of the visual potential of satellite imagery. As a result, the continuum again has two poles. On the one hand, problematizations that largely emphasize the potential of satellite observation to visualize a security threat. On the other hand, problematizations that make use of it as a scientific data product alongside additional sources. This is not to say that satellite imagery alone suffices for any of those problematizations. To the contrary, across all uses it is usually employed in concert with further information such as media reports, witness testimony or ground

images. However, the potential of satellite data rather focuses on the information extracted from the data than an apparent visual change on an image. Accordingly, satellite data is usually associated with larger areas of interest at once while the spatial resolution plays a lesser role. Instead, satellite data is associated with the timely acquisition of data after a specific incident or temporal resolution that allows for more frequent images of the same area to create time series data. In contrast, problematizations that are less time-sensitive and depend on the visual appeal of satellite imagery even draw on GoogleEarth occasionally for inexpensive, easy-to-access and visual review of sequences of change and events. When visuality is key, non-state actors are not only interested in the answer to the research question but also in providing objective, readily understandable information, raising awareness or evoking an emotional response. All of this is rather facilitated by a photo-like visual representation than a computed table or big data analysis whose methodologies are less comprehensible for laypeople.

Figure 2: Four Modes of Non-Governmental Remote Sensing



Taken together, transparency is an overarching theme in how non-state actors respond to various problematizations. However, there are differences in the specific goals and actualized potentials of remote sensing (see figure 2). The public intelligence mode provides objective information to

the public about security threats and focuses on the visual dimension of satellite imagery. The mapping mode likewise focuses on objective information by extracting insights from satellite data. The visual advocacy mode builds on individual images to pursue goals of advocacy and accountability. Lastly, the mass data mode also seeks to raise awareness and advocate for a particular cause but turns to larger amounts of satellite data for doing so. In the following, I will present each mode of non-governmental satellite observation.

6.3.1. Public Intelligence Mode

Objective Information for Evidence-Based Policymaking

In the public intelligence mode, non-governmental actors employ satellite imagery to produce objective information and inject it into ongoing political controversies. They identify a lack of impartial information about security threats as major impediment to evidence-based policymaking. In doing so, non-governmental actors seek to mitigate the impact of rumors, uninformed opinions and conjecture. There is a strong belief that transparency in the form of better and more information does not only improve public debates but by extension political decision-making. As a result, they attempt to spread their analyses as widely as possible across conventional and social media channels. Consequently, some of the users work in close alignment with the news cycle in order to verify or refute reported claims about alleged security threats such as missile launches, weapon developments, deployment of military gear, or nuclear programs. Their goal is to educate the public about the relevance and seriousness of security issues and to dispel alarmist statements by providing satellite imagery-based information. Even though many of those non-governmental users closely follow the news and are regularly approached by journalists after significant events, they are reluctant to offer soundbites but favor accuracy of information over speed. In this function of publicly providing up-to-date information about ongoing security situations lies the crucial difference to government intelligence actors. In fact, many implicitly or explicitly dissociate themselves from governments in two fundamental ways. First, with the help of publicly accessible satellite imagery they act as reviewers of statements made by governments concerning particular security situations:

> *"In the past anyone could make a claim about something and that could affect the conversation in the public which again could trickle into the conversation behind closed doors in the government or something. And vice versa, if a government were to say, this is a picture of something and this is what's happening, we just had to take their word at it. And, you know, beat the drum we're marching to. But now that satellite imagery has just proliferated into all sorts of realms and people have more access to higher quality, more frequent satellite imagery, we're now for the first time able to look at things and question them"* (Informant #20).

When government officials contradict each other in their public announcements about contentious issues such as the conflicts in Eastern Ukraine or the South China Sea, this leads to open, irresolvable disagreements. Non-governmental actors use commercial satellite imagery to match government statements with actions on the ground. In that sense, they are less dependent on blindly trusting government sources but can see for themselves. Second, non-governmental users of satellite imagery dissociate themselves from the classified-by-default mindset of many governments when it comes to information on issues of national security. There is a general acknowledgement that some security-related information requires classification. However, commercial satellite imagery helps reducing the extent of classified information from the outside by working against and reducing the secrecy imposed by governments. In this way, non-governmental users in the public intelligence mode produce "open-source intelligence reports so we can start learning things faster than what the government would tell us" (Informant #14).

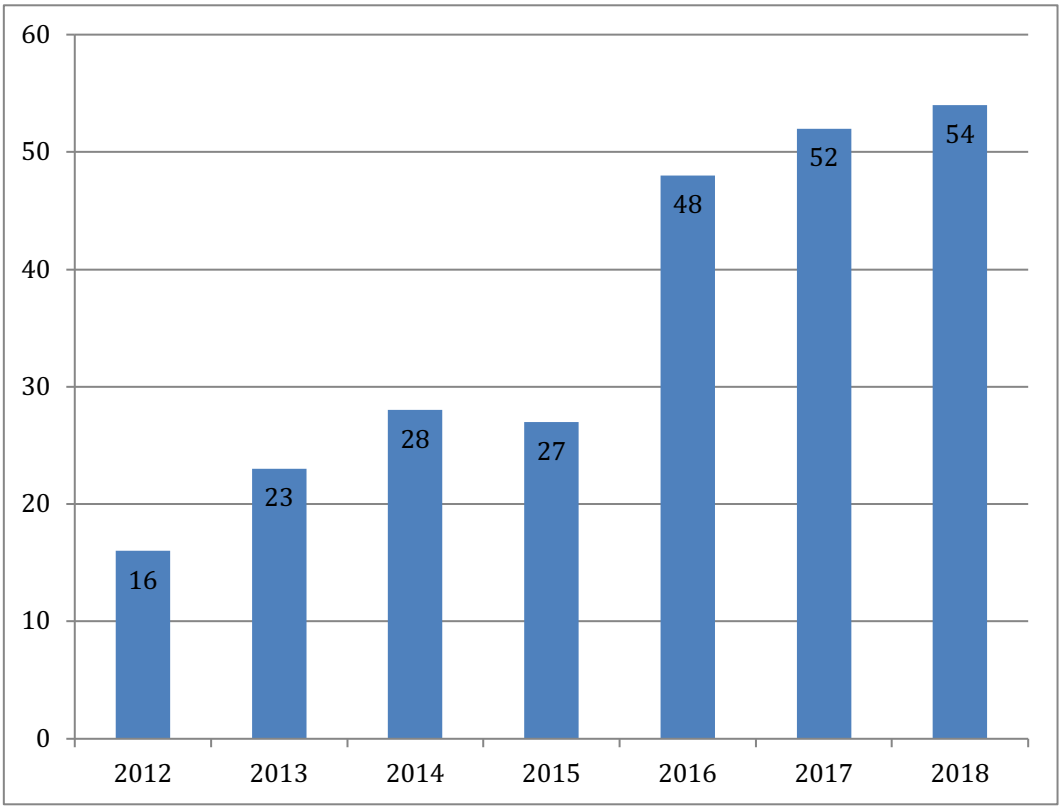
Similar to intelligence work, the knowledge practices are guided by a pursuit for unpoliticized, objective information. When writing the report of a satellite imagery analysis non-governmental actors in the public intelligence mode strive to "let the facts speak for themselves" (Informant #3) and not reflect their personal, political opinions in their reporting. They do not attempt to advocate for a particular cause, recommend policy or identify who is ultimately to be held accountable for an emergent security threat. Instead, they see their value in the allegedly impartial analysis that is conducted and presented in an as technical as possible manner. There is a firm belief in the scientific and almost apolitical nature of satellite imagery analysis. Analysts pride themselves for holding back their political views and make this a relevant dimension in defining the reputation of fellow colleagues. Somewhat counterintuitively, the reputation of non-governmental analysts among their peers is not primarily defined by the amount of traction they are able to generate in the media. Pandering to or giving in to the sensationalism of some media outlets is actually frowned upon. Satellite imagery analysts rather commend prudent, cautious and fine-grained technical analyses that are untainted by too far-reaching political positions.

Focus on Conventional Security Threats

As has already been hinted at, the public intelligence mode is predominantly applied to more conventional security issues that are characterized by poor information situations. One prime example is the non-governmental monitoring of North Korea's nuclear and other weapons programs by groups such as 38 North, the Institute for Science and International Security (ISIS), the James Martin Center for Nonproliferation Studies (CNS) or Stanford's Center for International Security and Cooperation (CISAC). The difficult access to and secretive nature of North Korea complicate non-governmental efforts to produce comprehensive assessments of security-related activities. In attempts to expand the availability of public information, those groups increasingly

use commercial satellite imagery to monitor known sites such as the Nyŏngbyŏn nuclear complex, the P'unggye-ri nuclear test site (e.g. Pabian, Bermudez, and Liu 2018a; Puccioni and Serbin 2018), the Tonghae satellite launching ground (also Musudan-ri) on the East coast and the Sohae satellite launching station on the West coast both of which are associated with the development of intercontinental ballistic missiles (ICBM) (Bermudez, Pabian, and Liu 2018; Hansen 2013), the Sinpo naval base which is related to North Korea's submarine-launched ballistic missile program (e.g. Cook 2017) or the Dandong-Sinŭiju area as a major hub for China-DPRK trade (e.g. LaFoy and Ahn 2017; Beyond Parallel 2016). In particular 38 North has increased its activity over the years producing roughly one report a week on average that includes satellite imagery in 2018 (see figure 3). Unsurprisingly, North Korea's nuclear program is a main focus of many groups. In doing so, they aim to provide a constant stream of information to enable civil society to weigh in on what is asserted to be a major security threat of global magnitude because "if you don't know what's going on and what the basic parameters are in terms of nuclear deterrence, then society can't have much of a say; it's all left to the privileged decision-makers with access to classified information" (Informant #40).

Figure 3: Number of Satellite Imagery Analyses by 38 North, per year



Similarly, the Asia Maritime Transparency Initiative (AMTI) at the Center for Strategic and International Studies (CSIS) has specialized on the South China Sea conflict in which various territorial claims overlap. Given this rivalry, governments regularly issue contradicting statements about recent developments in the remote location, which leads to a lack of clarity of what is actually happening on the ground. AMTI operates in a public intelligence mode when it uses commercial satellite imagery to check the substance of government statements (AMTI 2017) and to develop an "Island Tracker" feature that consistently monitors land reclamation or militarization activities of various nations (AMTI 2018). While conventional security issues make up the largest part of the public intelligence mode, it is also applied to other issues. This includes the Geospatial Technologies and Human Rights Project run by AAAS, which was mentioned above. AAAS provides a technical report to a non-governmental client about what observable information can be derived from satellite images concerning the client's area of interest; for example, Physicians for Human Rights approached them for an assessment of Syrian medical facilities after reported attacks (AAAS 2016). AAAS does not include extensive eye-witness testimony, add a political or legal analysis or assign responsibility for potential human rights violations. When the report is disseminated, however, the clients are free to integrate those findings, which are imbued with AAAS's impartial and scientific reputation, in their advocacy efforts.

Small Community of Satellite Imagery Analysts

While there are a number of non-state groups that work in the public intelligence mode, their level of institutionalization is rather low. Oftentimes, they are grant-funded projects with a low number of analysts attached to larger non-profit organizations in Washington, D.C. or the San Francisco Bay Area. At the same time, it is a small community in which analysts know each other across organizations although rarely across issue areas so that satellite imagery analysts focusing on nuclear issues are less aware of the work of their colleagues on human rights, environmental or humanitarian issues. As the monitoring of security programs is often confined to the observation of few specific sites such as missile test areas or nuclear facilities, the public intelligence mode is further characterized by a specific regional concentration as opposed to a global coverage. So even though non-governmental actors in this mode might be following developments in Iran, North Korea, Pakistan and Russia, they define limited areas of interest of several square kilometers.

Visual Analysis: Seeing a Security Threat

Despite the pitfalls and limitations mentioned in the previous chapter, the visual potential of satellite imagery takes center stage in the public intelligence mode. Analysts usually provide granular reports on what is visibly observable in one or a number of satellite images. Such reports

use captions, circles and arrows to identify buildings, vegetation, roads, fences, vehicles and note changes in before-and-after image comparisons. The public intelligence mode is essentially about seeing the security threats so that they need to be translated into observables. Generally, they are confined to larger, visible changes that are indicative but rarely conclusive proof of security developments on the ground. In this mode, vehicle activity, steam, smoke and cooling water discharge become suspicious telltale signs about the level of activity of North Korea's nuclear program while burnt vegetation shows recent missile engine tests. In short, the quality of a public intelligence report depends on if "what the satellite imagery analyst is telling you can actually be seen on the image" (Informant #43).

Very rarely, satellite imagery analysts accidentally hit upon a new, significant scoop in an image. Rather, they turn to satellite imagery to verify or refute media reports, eye-witness accounts or other sources that in beforehand indicate significant developments. In that case, analysts acquire imagery that fits the reported timeline to review whether something actually happened as reported or claimed. Moreover, they curate lists of relevant sites that are regularly monitored for changes. Oftentimes, conventional security threats constitute long-running issues that are tied to fixed locations because of necessary financial and structural investments. Analysts benefit from this fact and "monitor those as often as we can and as much as we can afford, too. Just to have a good sense of what's going on in these areas" (Informant #1). Over time, analysts become experts on a number of security-related locations and begin noticing patterns of activity that occur prior to or in association with meaningful events. Regardless of whether analysts seek to examine the substance of a particular media reports or check an item on their watch list, time is less of an issue than providing accurate and objective information.

Matching the visual emphasis and narrow areas of interest in the public intelligence mode, non-governmental actors mainly work with electro-optical imagery which comes closest to everyday photographs and is comparatively easy to relate to even for laypeople. Moreover, analysts prefer high-resolution imagery because it provides greater detail and allows for a more fine-grained analysis as it facilitates the identification of objects on the ground. While the visual analysis requires large amounts of training and experience, the public intelligence mode is technologically simple and straightforward. It does not involve the use of complex software tools and algorithms for automatic image detection nor does it usually combine different spectral bands such as thermal infrared, hyperspectral or radar imagery. Having said that, there is great variance of technical skillsets in the public intelligence mode. As a result, a few non-governmental actors still extensively use publicly accessible imagery sources like GoogleEarth and similar products to update running assessments of security programs. At the same time, there is a clear, observable development that has non-governmental actors increasingly turn to more technologically

sophisticated analyses involving different kinds of imagery while staying true to the focus on visuality.

Imitating Cold-War Intelligence Practices

The public intelligence mode seeks to promote a transparency that builds on allegedly objective information that is mainly derived from the visual dimension of satellite imagery. In doing so, it is reminiscent of Cold War-like intelligence practices. Incidentally, more often than others actors within this mode are familiar with and make use of governmental intelligence parlance such as open-source intelligence (OSINT), image intelligence (IMINT) or signal intelligence (SIGSINT). The overall defining difference to the intelligence community is that they ultimately provide information to the public instead of a select group of policymakers. Given the strong sense of objectivity, there is limited reflection on the selection of sites, i.e. which countries and issue areas are chosen, and the political context. In the public intelligence mode, analysts seem to agree that their responsibility lies in the truthful and objective presentation of facts that are observable in an image. However, this responsibility rarely extends beyond the publication of the report. So, whenever satellite imagery analyses of national weapons program or military activities "are leading people to see them as aggressive, that's not our fault for releasing the imagery" (Informant #7). This, however, neglects that this information is rarely released into a discursive vacuum but can become a powerful tool to reinforce existing biases and stereotypes (see chapter 7).

6.3.2. Mapping Mode

Actionable Intelligence for Humanitarians

The mapping mode is unified in its goal to acquire objective, actionable information across considerable space. Non-governmental actors in this mode attempt to support decision-making by charting a large geographic area according to predefined categories. This mode comes in two central manifestations that can be delineated by way of their temporal orientation.

First, the mapping mode is central to humanitarian action and crisis response. It is a tool to assess the impact of natural and man-made disasters, identify the severity of destruction and map out road networks to support crisis responders on the ground. In these cases, speed is of the essence. One of the major problems of crisis response in areas impacted by natural disasters such as earthquakes or flooding is to determine road accessibility. On the one hand, roads could be destroyed or blocked as a consequence of the disaster. In this case, satellite imagery of before and after the event can be compared to assess whether roads, tunnels and bridges are still passable to reach affected populations. On the other hand, when disasters strike in remote areas it is possible that roads are not well mapped at all so that satellite imagery is necessary to quickly create reliable ad-hoc maps of the affected area. In these cases, the public at large is not so much the

target audience as governments, humanitarian organizations and first responders that rely on this information to plan and coordinate their assistance. Moreover, satellite imagery is not so much employed to verify or refute claims but to generate a common baseline to facilitate action. In doing so, it supports where it does not replace ground surveys and accelerates the time necessary for damage assessment and planning from days to hours.

The time-sensitive mapping mode is characterized by a great diversity of actors: NGOs are joined by a number of international organizations, quasi-governmental institutions and commercial companies. The Humanitarian OpenStreetMap Team (HOT) is a non-profit organization that relies on donated satellite images and volunteers to create maps of buildings and road networks in the immediate aftermath of disasters. The maps are then provided to humanitarian organizations to facilitate relief efforts on the ground. Pursuing a similar mission, the International Charter "Space and Major Disasters" brings together national space agencies and national civil protection agencies. Registered government organizations can activate the charter in case of natural or man-made disasters. Once activated, there is a process in place that has remote sensing specialists analyze satellite data to provide maps including relevant information pertaining to emergency response to the affected country at no cost. If the country of concern has not registered an organization with the charter, the UN Office of Outer Space Affairs (UNOOSA) and UNITAR's Operational Satellite Applications Program (UNOSAT) can activate the charter on behalf of UN member states. Lastly, commercial satellite imagery providers produce their own analyses of natural and man-made disasters. As operators of the EO satellites they can quickly access and analyze relevant data. In addition to supporting emergency response, this is an opportunity for companies to demonstrate their corporate responsibility, showcase analytical capabilities and market analytical products to potential customers from the government and insurance sectors.

Country-Wide Analysis from Space

Second, the mapping mode is deployed for documentation and evaluation of phenomena across large geographic areas. This practice does not capitalize on the rapid response made possible by remote sensing but on the possibility of covering extensive areas at once using the same framework. Usually, different kinds of built and natural infrastructure are surveyed including road networks, electrical grids, refugee camps, pipelines, military garrisons, housing density, forests and water bodies. Especially when it becomes difficult to obtain reliable and internationally comparable data, remote sensing becomes a go-to source for non-governmental actors to produce an overview of the situation. In some cases, the goal is simply to create reference catalogues for unspecified later use. More often, however, the observed infrastructure is mapped as a proxy of geospatial distribution and regional concentration of military force, poverty, resource accessibility or logistical choke points to inform policy planning and decision-making.

Actors mainly comprise research and development organizations. Non-governmental actors have extensively mapped North Korea's energy, military, agriculture and other infrastructure (Melvin 2009) to more focused research articles on the development of markets in in the country (Cha and Collins 2018). Oftentimes, such initiatives draw on satellite imagery from GoogleEarth. The consequent trade-off between free data of extensive geographic areas and limited temporal and spatial resolution illustrates the different emphasis of issue-specific mapping projects in contrast to more time-sensitive crisis mapping. Moreover, actors like the World Bank use wide-area satellite imagery assessments to produce comparable accounts of economic well-being, housing in rural areas or other socio-economic indicators. Since thorough surveys to produce poverty statistics remain difficult and particularly rare in less developed countries, satellite imagery fills this gap in a cost-effective way. By way of an array of indicators including housing density, roof material and number of cars poverty estimates are produced that can be broken down by region (for an example of Sri Lanka, see Engstrom, Hersh, and Newhouse 2017). In response to the adoption of the 2030 Agenda for Sustainable Development, national space agencies as well as international and non-governmental organizations have drawn up plans to use Earth observation data for the achievement of the 17 Sustainable Development Goals (SDGs). In effect, they use research as in the example above to guide planning and operation of development activities. For example, the NGO GiveDirectly used a satellite-based poverty assessment to select the poorest villages for their unconditional cash transfer program in East Africa (Varshney et al. 2015).

Satellite Data for Decision-Making

Non-governmental users of the mapping mode embrace the objectivity and accuracy of satellite data. At the same time, they value how large areas can be surveyed quickly in an ad-hoc manner to produce actionable analyses. Similar to the public intelligence mode, they largely understand satellite data itself as apolitical and impartial so that they see their role "as just providing good information and people use it however they're gonna use it. […] I'm not trying to pass some new law or regulation. I'm not trying to put somebody out of business or in prison. I'm just trying…I think the information can speak for itself" (Informant #2). To be clear, this perspective represents the position of satellite imagery analysts themselves. The organizations they are affiliated with are arguably pushing specific agendas relying on their maps and information. For example, when an organization commissions them to work on the distribution of ballistic missile facilities in contrast to rural access to electricity already is the result of a political decision. Moreover, the mapping mode is focused on data that can directly contribute to decision-making, as one informant put it who monitored an oil spill in progress: "And we were strictly by the book when we were doing that work, in the hopes that it was actionable data that we were producing, not just imagery to wake up the public about the magnitude of the spill but actually stuff that would be

helpful to the agencies that were struggling to manage it" (Informant #33). In contrast to the public intelligence mode, the focus moves away from the visual dimension of satellite imagery. Instead, the data potential of remote sensing is used to construct an instructive end product that conveys the information believed to be necessary for quick and reasonable response. Mostly, this comes in the form of easy-to-read maps. Central findings are color-coded and individual observations are charted on an interactive map, e.g. on GoogleEarth, which the end user can navigate on her or his own. With this in mind, the satellite image itself becomes less important and sometimes merely figures as the background to the data displayed on top of it.

As has become clear by now, non-governmental actors are sharing this space with international organizations as well as government actors. This applies to the time-sensitive as well as issue-specific mapping mode. Both face different challenges when it comes to imagery access. When the World Bank or NGOs conduct country-wide assessments of infrastructure or poverty estimates, they usually concentrate on less developed countries lacking sufficient statistical data. As a result, they require significant amounts of satellite data so that non-governmental actors with their limited funds often draw on GoogleEarth. This means, non-governmental users "have to wait until it randomly appears" because commercial satellite imagery is so expensive that "you have to have an organization that supports you to do it" (Informant #2). The imagery needs for crisis or humanitarian mapping are less about exhaustive data for the whole country but up-to-date collections of before and after the event. The time-sensitive mapping efforts for emergency situations have a global scope but remain limited to the affected areas. Newly collected imagery as well as tasking is often too expensive for humanitarian NGOs. Consequently, they depend on the good will of commercial satellite imagery providers that "would release imagery to the public for a limited amount of time to enable crisis response and mapping" (Informant #37). The International Charter "Space and Major Disasters" counters this dependence with the institutionalized process that involves national space and civil protection agencies. In doing so, it guarantees satellite imagery access in most natural and man-made disasters for registered public agencies. Given the government involvement, politically sensitive situations are effectively excluded. In addition to civilian government assets, commercial imagery providers like DigitalGlobe or Planet are also part of the Charter and provide satellite imagery to registered members at pre-negotiated costs (Informant #48).

Crowdsourcing Geospatial Data

As the mapping mode usually covers large areas, the visual dimension of the satellite image fades into the background. Given the ambition to inform actions on the ground, the focus shifts towards data points that are either derived from the satellite data or marked on top of the image itself. If the main interest lies in the distribution and connection of energy infrastructure in a country, then

it is not necessary for the user to visually examine each power plant and transmission tower. However, when the network is mapped out relevant information can be derived such as bottlenecks, rural access or reliance on specific power sources. The mapping mode counts events or signatures across time and space and visualizes their relations on top of the satellite image. In doing so, they mainly focus on the satellite data itself only consulting additional sources when necessary. As such, the satellite data itself is usually the starting point for analysis. Nevertheless, there is no need for end users to zoom in on the visual details of the image itself. Instead they rely on differently colored areas to indicate poverty estimates, housing density or water access, captions to identify infrastructure types and pictograms to signify impassable roads or bridges. Going further, this mapping approach can also be translated into tables and graphs to allow for additional comparative analysis.

The time dimension is most critical for the mapping mode for crisis response. The process of the International Charter "Space and Major Disasters" delivers up-to-date satellite imagery to a remote sensing expert who conducts professional analysis of the situation at hand. In most cases, the analysis focuses on damage assessments after floods, forest fires or earthquakes. The analyses use various types of satellite images including electro-optical, thermal infrared as well as radar imagery. Usually, they provide a broad overview of flooded area and damaged buildings. In comparison, the strength of the non-governmental side of humanitarian mapping lies in more detailed analyses of large crisis areas by leveraging a greater number of volunteers. In the case of the 2015 Nepal earthquake more than 6,000 so-called community mappers participated in the post-disaster efforts of the Humanitarian OpenStreetMap Team. These lay mappers receive brief tutorials about how to map the features of interest before they independently select an area to map. Drawing on such a large group of people allows for more detailed mapping of roads and buildings as well as more extensive damage assessments. Commercial satellite company DigitalGlobe has further automated this approach of harnessing the crowd. Its Tomnod platform is regularly activated when disasters require mapping efforts. In such cases, DigitalGlobe provides before and after imagery on an easy-to-use community platform. Multiple users can tag flooded areas, destroyed buildings or blocked bridges at the same time. An algorithm identifies reliable tags and disregards outliers. In the Nepal example, Tomnod mapped the impacted areas in Nepal in less than 48 hours. This example also illustrates the complex web of relations. While DigitalGlobe itself is active in the Nepal disaster response via its Tomnod platform, it also provides satellite imagery to OpenStreetMap for the same event. When maps are crowdsourced by inexperienced analysts, it is effective to use high-resolution imagery because laypeople are less familiar with how vehicles or buildings look on 10m-resolution overhead imagery. Once the data is compiled, however, the imagery itself loses some of its importance while the colored tags become more relevant.

Automated Imagery Analysis

The same applies to issue-specific mapping across large geographic areas. As long as analysts manually work on the satellite imagery to tag and annotate, higher spatial resolution enables more accurate mapping. Even if an analysis is restricted to one issue, such as dams or power plants, mapping out a whole country manually is a laborious and time-intensive task even when satellite imagery is available. Moreover, in order to keep the map updated, one has to continuously follow recent developments and add them to the map. Therefore, actors like the World Bank and a few larger NGOs increasingly shift towards automated imagery analysis to facilitate mapping efforts of country-wide proportions. In these examples, algorithms are trained to automatically identify roof material, cars or waterways as indicators for economic well-being, fresh water access and so on. The Tomnod platform is also active in the area of less time-sensitive mapping. For example, when it comes to mapping rural settlements in remote areas, the algorithm presents its findings in the form of a satellite image with what it calculated to be houses or buildings. The users only have to decide whether the assessment is correct or wrong. They do not and actually cannot browse the imagery and tag by themselves. This way, DigitalGlobe receives the mapping data it needs while at the same time training its proprietary algorithms that are later used for commercial contracts.

The mapping mode draws on satellite data to provide geospatial information across large geographic areas. It seeks to provide actionable information to planners, decision-makers and actors on the ground. In this sense, it has a rather professional target audience with special needs. When maps are manually created, the visual dimension of satellite imagery remains crucial during the analysis. For automated analysis and the eventual presentation of the finished mapping product, however, the emphasis shift towards the tagged, colored or otherwise marked information drawn upon the satellite image. Non-governmental actors are part of a diverse assemblage of actors active in the mapping of country-wide assessments along different indicators as well as crisis response.

6.3.3. Visual Advocacy Mode

Satellite Imagery for Change

In the visual advocacy mode, non-governmental users employ satellite imagery to ultimately effect change on the ground. For this purpose, NGOs and think thanks use satellite imagery to document and monitor human rights violations and security threats in remote or hard-to-access places across the globe. In doing so, they seek to raise awareness, advocate a political program, affect policy decisions or hold people accountable. In a few instances, remote sensing is also employed to deter further illegal or harmful actions.

Human rights NGOs in particular harness the potentials of the commercialization of remote sensing since "satellite images can be very powerful in that regard because of the visual impact" (Informant #16). In this way, satellite imagery becomes a tool for non-governmental actors to communicate more effectively with the public as well as policymakers. In contrast to the public intelligence mode, adherents to visual advocacy go to great lengths to make themselves heard. More often than not, it is existing institutions that already count as experts on their respective issue area. Now, they integrate commercial satellite imagery into their operations. In doing so, they fill a gap left behind by governments, which cannot publish satellite imagery from their national security assets. In this way, it is seen as an effective storytelling device for advocacy purposes because "a lot of people take it as higher credibility" (Informant #21).

Accordingly, satellite imagery adds to efforts to create public pressure and public accountability for human rights offenses, ecological damage and other norm violations. In this domain, satellite imagery is understood as an additional layer of evidence to corroborate anonymous sources, and definitively validate denials or assertions of innocence. In this sense, NGOs become investigators that do not only produce evidence of a specific event. Instead, they seek to build a case, find motives and determine the people responsible. Going further, there have also been early efforts to use remote sensing for prediction and deterrence of insecurities as one informant revealed that "now we are shifting a little bit from being very reactive to more like active monitoring which we didn't do before because we didn't have the capacity. But now there is more imagery and there is more staff and it becomes easier" (Informant #16). This reorientation from retrospective analysis to future-oriented action takes different forms. On the one hand, satellite surveillance could serve as a cue to imminent acts of war or human rights violations. This would allow for shorter response times with respect to political action and international aid efforts. On the other hand, constant surveillance can be understood as exercising a deterrence effect for potential perpetrators who think twice before being caught in the act.

Exposing and Monitoring Human Rights Violations

The visual advocacy mode in the human rights domain usually boils down to more or less extensive reports. In addition to eye-witness testimony, policy statements and other sources, NGOs add commercial satellite imagery to make their case. Known for its early use of this technology, the Committee for Human Rights in North Korea (HRNK) has published multiple reports on North Korea's political prison camp system it dubbed *Hidden Gulag* (Hawk 2003). In this publication, HRNK worked together with former prisoners to identify the functions and relations of buildings in the camps and quite prophetically predicted that "in the coming years, this tool will be used to understand and expose the human rights and humanitarian situation in this still-closed society" (Hawk 2003: 88). Indeed, satellite imagery has become a go-to source for

human rights NGOs – not only for documenting atrocities in North Korea but also China, Iraq, Nigeria, Palestine, Sudan or Syria. In 2018, Amnesty made extensive use of commercial satellite imagery in the context of the Rohingya crisis. Satellite imagery served to corroborate or dispute testimony, reproduce timelines of actions and visualize the burning and razing of villages. In doing so, it substantiated accusations of ethnic cleansing by the Myanmar security forces in Rakhine State. While Human Rights Watch and other groups follow similar goals of producing evidence human rights violations, the Satellite Sentinel Projects (SSP) stands out. In anticipation of the independence referendum in South Sudan, SSP promoted the goal to use satellite imagery to monitor potential human rights and security hotspots in near real-time in order to deter human rights violations. That means the team acquired, analyzed and released satellite imagery within 48 hours. This was made possible by a dedicated investment of George Clooney and other celebrities, human rights experts at Harvard University, DigitalGlobe and the non-profit organization Enough Project. This unique setup even allowed SSP to task DigitalGlobe satellites to collect satellite imagery upon their request. In all cases, satellite imagery is not merely a tool to provide objective information but to promote human rights and create accountability.

This motivation is also prevalent in other fields such as non-proliferation, conservation or environmental protection. The National Defense and Research Council (NRDC), for example, is an apt user of remote sensing technologies to promote these goals. Some U.S. foreign policy think tanks also engage in the visual advocacy mode to influence decision-makers on matters of national security when it becomes obvious that their "policy is not working in the way that [they] want it to work. So, we do use imagery to help influence policy decisions" (Informant #1). At times, the approach of creating public transparency gets more traction and is deemed more effective than direct advocacy to the U.S. government. Lastly, non-governmental remote sensing is used to create public awareness of hitherto neglected issues such the destruction of cultural sites in the context of the war in Syria.

Geospatial Analysis Teams of NGOs

Similar to the public intelligence mode, this way of granular analysis of satellite imagery requires training and expertise. However, most human rights NGOs have not been familiar with the technology before its commercialization in the early 2000s. Consequently, the early days were characterized by experimentation and learning-by-doing. At the same time, some organizations have turned to external experts including AAAS, commercial or former government analysts. As a testament to the usefulness of satellite imagery for their operations, larger NGOs in particular have by now developed dedicated geospatial analysis teams who conduct satellite imagery analysis themselves including Amnesty International and Human Rights Watch. Volunteers, as in the case of the mapping mode, usually do not have the necessary expertise to help with identifying

imagery signatures of human rights violations. For human rights monitoring, satellite imagery is applied on a global scale. However, most of the time the analyses focus on developing countries in the context of civil conflicts. While NGOs are aware of this imbalance, the more egregious human rights violations in other contexts take place in ways that often are invisible to satellite imagery such as human trafficking or abuses in the prison system.

Becoming a Witness of Human Rights Violations

For the purposes of awareness, advocacy and accountability, the visual potential of satellite imagery plays a decisive role. The visual is taken as definitive proof of a political situation and believed to be instrumental in pushing for growing awareness and the will to respond. Consequently, advocacy efforts by way of satellite imagery are most powerful and effective when the event of concern is immediately visible without elaborate analysis and annotation. Such a strategy is, for example, applicable to razing campaigns, which leave behind burning homes, as well as island reclamation activities in the South China Sea. In most cases, however, the events on the ground are too complex and, frankly, too small to be recognized on satellite imagery by the uninitiated eye. The most common strategy of analysis in the visual advocacy mode is combining eye-witness testimony, photographs, videos or other sources with commercial satellite imagery. Oftentimes, the first job is to geolocate the event. When a photograph shows, even if only in the background, a church, mosque or temple in a city, satellite imagery can become instrumental in determining the precise location and angle from where the photograph was taken. For this to work, non-governmental actors favor a few high-resolution images over mid-resolution variants. As commercial satellite imagery also comes with an exact time stamp, it is possible to corroborate or dispute testimony and timelines. For example, when witnesses report of security forces moving heavy vehicles at a certain place and time of day. In this sense, it is similar to the public intelligence mode and, arguably, the intelligence agencies: "I suppose this is true for the intelligence community, too, but the best circumstance were when you had satellite imagery and ground information from people on the ground that you could validate" (Informant #8).

Much of the political clout of NGOs hinges upon their credibility in terms of methodological and ethical rigor. Conceivably, relying on crowdsourcing approaches and amateur analysts would jeopardize this resource to begin with. As mentioned, external analysts are a common way to introduce satellite imagery analysis into the repertoire of human rights NGOs. While former military analysts reliably identify weapon types or critical infrastructure, human rights analysis requires additional political context to properly make sense of the imagery:

> *"Where do we come in? Well, the satellite imagery is not enough. You'll also need the context, the political context, the human rights context, that enables you to understand why you see*

this infrastructure changes. Moreover, you need eyes and boots on the ground which is not always possible. But if it is possible, it is extraordinarily helpful because you can corroborate witness testimony with satellite imagery" (Informant #9).

So, bringing together this knowledge and close collaboration between human rights experts and satellite imagery analysts are key in the visual advocacy mode.

Transparent Methods of Analysis

Given the importance of credibility, the visual advocacy mode is characterized by a great amount of transparency when it comes to the methodological analysis of satellite imagery. The drafted reports usually contain an independent methodology section. Therein, the authors describe in detail the imagery sources as well as how it is analyzed. Inspired by scientific standards, the goal is to fight the impression of political bias and emphasize the unbiased, objective nature of the visual evidence. The diligence and accuracy in conducting the analysis is also connected to the goal of accountability in this mode of remote sensing. Several NGOs explore to or already work with courts including the International Criminal Court (ICC). This cooperation takes the form of education efforts where NGO would present to the court the current possibilities of commercial remote sensing for human rights work. Moreover, non-governmental actors attempt to create as useful information as possible for the Office of the Prosecutor: "We were gathering information to a forensic standard and to a scientific standard and to a legal standard where it would stand up in court for a war crimes investigation before the International Criminal Court or any other court of competent jurisdiction. So, our information was bulletproof" (Informant #13). Accordingly, they think about issues such as a chain of custody concerning the collection, processing and analysis of commercial satellite imagery as well as how it can be presented in court by way of an expert witness who usually is the analyst themself. Interestingly, the ICC is rather quick in picking up the advantages of open-source information including satellite imagery and hires dedicated staff in this area of expertise. The particular potential of satellite imagery is to become linkage evidence so that political accountability is tied to the high-level culprits and not those executing orders on the ground. For this,

"satellite imagery and remote sensing can really come into play. Because it can help you understand troop movements, you know, who is doing what, when, where and how, what were the trajectories, where did trucks originate, where did troops originate and what were basically these kind of patterns of movement that can really ultimately link different atrocities back to their source" (Informant #19).

In short, NGOs re-trace the chain of action to support the work of the court and perhaps even point to possible culprits.

Given this sense of potential of remote sensing for advocacy and accountability, human rights NGOs have become vocal about introducing ethical and methodological standards in the practice of satellite imagery analysis. They fear that sloppy, premature and eventually incorrect analyses damage the craft as a whole. Moreover, many analyses cover active conflicts. Consequently, releasing up-to-date satellite imagery of refugee camps, destroyed cultural sites or razed villages might risk harming vulnerable populations by providing crucial intelligence to parties to the conflict.

6.3.4. Mass Data Mode

Environmental Satellite Data on a Global Scale

A relatively small group of non-governmental actors actualizes the potential of satellite data for advocacy purposes in combination with other datasets. Commonly, this mode is applied to problematizations in the environmental and conservationist domain. The goal is to produce scientific data on a global scale to inform public advocacy and affect environmental protection policies. Considering the amounts of data necessary to produce global datasets based on satellite imagery, the commercialization has created the potential for the mass data mode to pursue its goals. In doing so, it assumes a global scope to advocacy and accountability and employs various methods to achieve its ends.

Environmentally-oriented organizations increasingly have the potential to create reliable data where governments and international organizations fail to do so. Accordingly, they become important players in constituting what counts as a threat to the environment, biodiversity and human welfare. Essentially, once deforestation or environmental pollution can be measured and visualized, it becomes more difficult for policymakers to neglect them as problems: Only then are they called upon to change policies or at least forced to justify inaction. This goes hand-in-hand with easier and cheaper ways to share this data with the public. While some NGOs have already been working with civilian, low-resolution Landsat satellite imagery since the 1970s, it was virtually impossible to share their data with the public. In fact, the analysts themselves received their satellite images by mail on hard drives and disks. After GoogleEarth it has become increasingly normal to launch interactive platforms of global datasets individual users can navigate by themselves. At first, this would be complete global datasets of a fixed point in time that would be updated irregularly, i.e. whenever new data is available and affordable. Thanks to the growing number of Earth observation satellites, new data can be dynamically added to the dataset. This allows NGOs – as curators of the data – to issue alerts when something is happening. This could be forest fires that after further analysis might turn out to be illegally started to create new land for plantations.

As should be clear by now, the mass data mode requires highly qualified staff, technological know-how and sufficient resources so that it is often larger NGOs engaging in this work. This also allows them to develop and field-test entirely new analytical methods. In this sense, these non-governmental actors do not only rise up against established government actors to act as watchdogs. Instead, they showcase how satellite data can be used in the public space by others including national agencies and international organizations:

> *"It's demonstrating what's possible to regulators and policymakers so that they can creatively develop newer, more effective policy and regulation that's based on the technical possibilities we presented. It takes public pressure though to ensure that government players act effectively and expeditiously once those opportunities present themselves. So, we're certainly reaching out to the public"* (Informant #33).

Consequently, the goal is to the public engaged and to understand the scope of the problem is an important step towards political action.

Monitoring Natural Resources

The Global Forest Watch program of the World Resources Institute (WRI) is an online forest monitoring tool that is consistently updated with new data. Users create customized maps on a global scale or go down to a more detailed level of analysis for their area of interest. At the same time, they can subscribe to receive notification in case of sudden tree cover loss in a specified area. For the largely automated analysis, WRI uses the Landsat dataset with a 30m resolution. This suffices given the large-scale changes visible on satellite imagery in case of deforestation. For another program that observes forest fires the NGO also employs high-resolution data. For doing so, it consistently monitors and detects fires from the high temperatures. When a hotspot illegally takes place in a known company concession, high-resolution satellite imagery is used to create additional evidence and link the fires to the responsible actors. The platform Global Fishing Watch, launched by a partnership between Google, Oceana and SkyTruth tackles the issue of illegal, unreported and unregulated (IUU) fishing. For doing so, it maps commercial fishing activities on an online platform by compiling the automatic identification systems (AIS) of ships. This way, anyone can follow individual vessel tracks in exclusive economic zones and marine protected areas. This global data also allows spotting possible transshipment, i.e. when a trawler transfers its catch to a refrigerated vessel far from port. This way illicit catch is mixed with legally caught fish without oversight. In addition to problems of sustainable fisheries management this illegal practice is also related to human rights violations like human trafficking and slavery. In a Pulitzer Prize-winning story, journalists of the Associated Press used high-resolution satellite imagery to

identify transshipment vessels that were crewed by illegal, forced labor (McDowell, Mendoza, and Mason 2015).

NGOs as Regular Customers of Satellite Imagery

Similar to the mapping mode, NGOs that tackle environmental or conservation problems on a global scale require large amounts of satellite data that cover areas at large or even global scales. At times, this also includes up-to-date imagery of emerging situations on the ground. Yet, it does not pertain to crisis and emergency situations per se. Consequently, commercial satellite imagery providers are reluctant to provide this data free of charge. In contrast, the larger NGOs that employ the mass data mode are seen as regular customers similar to other commercial entities. Given the sheer amount of data necessary to keep large datasets updated, these projects run into cost constraints especially when it comes to labor costs and high-resolution satellite imagery. It is still an expensive technology to work with relative to the data budgets of most environmental projects. At the same time, the technological sophistication of the mass data mode makes it interesting for commercial analytics companies. Algorithms that automatically monitor plant health and soil characteristics for big agriculture businesses might hold potential for observing global forests and plantations. Similarly, maritime surveillance for the government could produce spin-off techniques for fisheries monitoring and vice versa.

Scientific Approaches to Satellite Data

The mass data mode requires significant technological know-how. The large amounts of satellite imagery necessary to produce global datasets render the visual potential of remote sensing secondary to the information that can be pulled from it. Accordingly, the focus is on a constant and continuous stream of standardized satellite data that reliably recognizes changes over time. Spatial resolution, on the other hand, is less important. High-resolution satellite imagery rather serves as a visual illustration and validation of the scientific findings in the satellite data. In addition to the drive to automate the extraction of information from satellite data, the mass data mode seeks to integrate various kinds of data streams: “Now, how do we combine it with other datasets? There is a lot of information on how to look at statistics specifically but I think there is a lot more than just statistics that it can be cross-referenced with” (Informant #28). For doing so, the starting point of analysis is not individual images as with the public intelligence or visual advocacy mode. Instead, it is whole archives of satellite imagery providers. This also leads to different purchasing models. Instead of looking for new collections of a pre-selected number of locations and buy individual images, subscription models allow NGOs to tap into the wealth of archival data for a fixed price and run tests of their new products.

Ultimately, the goal is to further automate rudimentary data analysis such as feature identification and reduce the time human analysts have to manually sift through a lot of satellite imagery. While high-resolution satellite imagery holds great potential in that regard, it also remains very cost-intensive. The combination of automated imagery analysis with additional datasets could discover relevant geographic patterns and relationships related to environmental protection on a global scale. This would strengthen moves from reaction to prediction and fundamentally rearrange practices of advocacy and political accountability. As of now, near-real time alerts of changes happening on the ground come closest to this potential future. Some NGOs in the mass data mode attempt to form a rapid response network that is increasingly sensitive to the global data they produce and translate it into local action. They "are interested in working with groups that are on the ground; somebody who can actually investigate in the field and tell the bigger story. Because for us, sitting in our offices, we're just seeing pink pixels on the screen…"(32:51). Local journalists or NGOs are approached to tell the story behind what is happening, what are the social and political drivers and, perhaps most importantly, what is the impact on the population.

Integrating Commercial Satellite Imagery

The mass data mode is arguably the technologically most sophisticated non-governmental mode of remote sensing and pursued by remote sensing experts on a scientific level. As of now, many NGOs still draw on free but lower-resolution satellite data from the U.S. Landsat or EU Copernicus programs. They are still weighing the overall benefits of better-quality commercial imagery against its higher costs. Regardless of the imagery quality, however, the scientific approach to large and various datasets does not eliminate the need for interpretation of satellite data due to human, organizational and technological factors.

6.4. Conclusion

The narrative of a geospatial revolution instructively points to the overall potential of commercial satellite imagery for non-governmental actors. However, the chapter shows that the initiation and stabilized operational practices vary significantly across issue areas, goals and users.

First off, a lack of awareness, necessary funding and analytical skills in the non-governmental domain are lasting barriers to picking up commercial satellite imagery (see chapter 5). Contrary to early expectations, journalists and the media have not become everyday users of satellite imagery and turned into "imagery activists." However, the outreach activities of individual champions and proponents of commercial satellite imagery have helped bear a fragile non-governmental network of users. Pilot projects temporarily suspend existing barriers and let non-governmental actors experience the value of satellite imagery for their operations. While many NGOs and think tanks have not moved beyond single satellite imagery projects, some have

translated them into more institutionalized forms of stand-alone geospatial analysis teams. Still, the network is sparsely connected and characterized by few nodes and bridges – mostly external imagery analysts and imagery providers. As a result, there is limited exchange of experiences and methodologies. Not uncommonly, non-governmental actors even compete for the same funding to acquire satellite imagery.

In this light, it is not surprising that multiple modes of non-governmental remote sensing have emerged and stabilized next to each other. While there is a conviction about the benefits of transparency, the typology delineates four distinct ways and practices of how non-governmental actors have reacted to the so-called commercialization of satellite imagery (see table 2).

Table 2: Overview of the Four Modes of Non-Governmental Remote Sensing

	Public Intelligence Mode	**Mapping Mode**	**Visual Advocacy Mode**	**Mass Data Mode**
Goals	Producing objective, evidence-based information; contributing to public debates; resolving alarmist discussions; improving policy-making	Producing objective, actionable information; improving policy decision-making	Creating awareness and advocating a cause; seeking political/legal accountability for norm violations	Creating awareness and advocating a cause; building evidence-base for political/legal accountability for norm violations
Imagery vs. Data Potential	Visual analysis of satellite imagery	Satellite data for geospatial mapping	Visual analysis of satellite imagery	Combination of satellite data with additional sources
Area of Operation	Conventional security threats incl. WMDs, military conflict; human rights	Humanitarian and crisis response; development work; political and economic mapping	Human rights; conflict analysis; environmental protection	Environmental protection; conservation efforts
Type of Actor	Independent or small teams of analysts; usually affiliated with a think tank or university	Humanitarian and development NGOs; contributions from government actors	International human rights NGOs; universities and independent analysts	Large environmental NGOs; university programs

		and international organizations		
Geographic Focus	Small areas of interest; relatively stable list of security hotpots; mostly non-Western countries	Larger areas hit by disaster; global orientation; data-poor countries for issue-specific mapping	Small areas of interest; varying list of countries; Global South focus	Global approach of data collection and analysis
Target Audience	General public; stakeholders; policymakers	First responders; planners; decision-makers	General public; donors; policy-makers	General public; journalist; policymakers; scientists
Technological Sophistication	Low; focus on manual analysis of high-resolution electro-optical imagery; rare utilization of SAR or thermal infrared imagery	Low to middle; scientific analyses of disaster impact; use of different kinds of imagery types; still some manual mapping with GoogleEarth	Low; focus on manual analysis of high-resolution electro-optical imagery; virtually no use of other imagery types	High; integration of global datasets; extensive use of civilian mid-resolution imagery; elaborate presentation in scientific journal or dynamic online platforms

The above overview illustrates that mostly smaller NGOs and think tanks work on hard security issues or human rights and emphasize the visual dimension of satellite imagery. Actualizing the image potential of remote sensing stabilizes practices that emphasize the meticulous analysis of a few high-resolution images in concert with relevant on-the-ground information such as photographs, witness testimony or media reports. In doing so, they imitate Cold War intelligence practices of satellite imagery analysis. Actors in the humanitarian, development and environmental domain rather seize on different kinds and a greater quantity of satellite data. Notably, they are often part of more institutionalized networks that also include government actors, large donors and international organizations. While the commercialization of satellite imagery promised to equalize the playing field for non-governmental actors, the typology suggests a reversal of this trend when it comes to data-intensive analyses. Visual imagery analysis has well entered the reach of think tanks, journalists and universities. But the more elaborate, algorithm-driven methods are often tied to long-term funding, expertise and technical know-how that corporations, governments and to some extent larger NGOs have.

While the potential consequences have been illustrated in specific cases, the following chapter further raises the level of abstraction. It discusses the effects of non-governmental remote sensing as an emerging practice in global security. This chapter has already shown that the creation of transparency is a major motivator for non-governmental actors to work with commercial satellite imagery. The following chapter examines the consequences of this drive to maximize transparency of security threats.

7 Forced Transparency

7.1. Introduction

Concerning the effects and implications of non-governmental remote sensing, transparency emerges as the central category out of the analysis. The preceding pages have looked at the role of satellite technology in the construction of security threats and how a typology of four distinct modes of satellite observation have developed and stabilized. In the process of that, multiple cases were presented that clarify the value of commercial satellite imagery for NGOs and think tanks on an operational level. Moreover, the dearth of academic literature, news stories and op-eds on non-governmental remote sensing emphasizes the manifold benefits of commercial satellite imagery (e.g. Baker, Williamson, and O'Connell 2001; Aday and Livingston 2009; Marx and Goward 2013; Convergne and Snyder 2015; Sivanpillai, Jones, and Lamb 2017). While acknowledging the operational benefits, the chapter takes a more critical stance that balances the assessment of non-governmental remote sensing as a security practice. This serves to identify more abstract implications and risks when looking at the use of satellite imagery by non-state actors. To be clear, it does not constitute an attempt to disband the opportunities of commercial EO technologies or to discredit non-governmental remote sensing. Rather, the purpose is to bring attention to political effects that frequently remain hidden. In accordance with the conceptual framework, the chapter focuses on how the effects of insecurities are managed, how the observed are affected and how technologized security practices seek to continuously increase their goals. Moving beyond that, the data analysis has produced further risks and effects that add to the initially theorized implications. As such, the exercise sensitizes academics, users and policymakers for the potential fallout from non-governmental remote sensing and offers avenues to further improve on understanding, programming and regulating the security practice.

More concretely, the chapter develops the notion of forced transparency. It results from the interaction of the virtuous pursuit of non-governmental remote sensing to achieve complete transparency and the technological potentials and constraints of commercial satellite imagery. Despite the apparent popularity and significance of transparency in the satellite imagery community, it often serves as a mere buzzword with positive connotations. The lack of definitional clarity, however, prevents discerning the term's content and underlying assumptions. As a result, it becomes impossible to analyze the durable effects of non-governmental remote sensing. Against this background, two questions are of particular interest here. What is the nature of transparency that non-governmental remote sensing promotes and how is it shaped by commercial satellite imagery? Once this is established, a second question asks about the risks and implications of transparency brought about by non-governmental remote sensing. The first section argues that

non-governmental users of satellite imagery understand transparency as the amount of publicly available information about a security threat. It is a quantitative measure they seek to maximize. Moreover, transparency is perceived as a virtue in itself and serves as a ubiquitous justification to intensify satellite observation. In doing so, creating transparency becomes technologized: The pursuit of transparency is continuously reinforced by the technological potentials of satellite observation. The goal but impossibility of complete transparency fuels a cycle of technologization that demands ever more and better satellite imagery. In the process, non-governmental remote sensing keeps forcing transparency. In a nutshell, the chapter argues that the socio-materiality of non-governmental remote sensing forces transparency. The second part of the chapter then focuses on six implications of forced transparency that for the most part remain hidden in case-study based analyses of non-governmental remote sensing focusing on the operational level.

7.2. The Illusion of Complete Transparency

7.2.1. Forced Transparency

Transparency is Information

From the beginning, the commercialization of satellite imagery has been tightly linked to notions of transparency. Commercial satellites have been envisioned to operate at the "leading edge of transparency" (Baker, Williamson, and O'Connell 2001) and fit into a more general trend of global transparency powered by technological development (Dehqanzada and Florini 2000; Lord 2006; Larkin 2016). Along the same lines, private satellite imagery providers regularly commit to enhance or bring about transparency to address global challenges from security to environmental and humanitarian issues (Jablonsky 2018; O'Shea 2018). Unsurprisingly, it also features prominently in the goals of non-governmental actors including security think tanks, human rights organizations, humanitarian actors or environmental groups. They embrace transparency and make it an essential part of their mission – or even names such as the Asia Maritime Transparency Initiative.

Delving deeper into the motivations, practices and goals of satellite imagery analysts, providers and users reveals the nature of transparency that they seek. In a 2018 speech, the CEO of Planet concretizes his vision of transparency (Marshall 2018b): After reaching its first major milestone, the company produces imagery of the planet's landmass on a daily basis. The next step entails transforming the live imagery archive into information and create a searchable planet. Information such as road networks, tree cover changes, the melting of glaciers, activity at nuclear power plants, refugee camps, factories, and activity at shopping mall parking lots are to be automatically derived from satellite imagery. The Earth's surface is to become queryable for anyone. In this sense, transparency is reduced to information. It is a quantitative rather than

qualitative measure. More information, more satellite imagery is equated with more transparency. In this line of thinking, the significance or extent of the change discovered on a satellite image is secondary. It is additional information and, therefore, increases transparency of the area of interest. There are various problems with such an understanding:

> *The implications of greater transparency depend not just on what it shows, but also how information revealed by transparency is interpreted. What information people pay attention to and the meaning they draw from that information depends on preexisting ideas and values that can change slowly even when new information calls those views into question. To cope with the volume of information received each day, people tend to interpret new information in the context of existing views and values and discard contradictory data. As the weight of contradictory evidence grows, most people will adjust their views accordingly. However, information is rarely so clear-cut and people are not quick to change. The implication is that the marginal increase of information we gain from increased transparency may have limited meaning in the short term. Greater transparency eventually may help us to know others better, but not soon* (Lord 2006: 120).

Paradoxically, users and analysts of satellite imagery acknowledge the problematique of interpretation. They are well aware of the limitations of satellite imagery on the operational level because they experience it in their operations on a daily basis. More specifically, chapter 5 has shown that the interpretation of satellite imagery is difficult and liable to human and technical errors. On a more abstract level, however, informants backtrack and re-emphasize the objective nature of remote sensing. The idea that the sheer availability of information creates transparency rests on the assumption that "pictures don't lie" (Marshall 2018b) and everybody understands the imagery in the same way. It assumes that information and its interpretation are uncontested. In that case, knowledge becomes a property of information (cf. McCarthy and Fluck 2016). How satellite imagery is collected and interpreted fades into the background; together with the common disagreements over and diverging assessments of the same image. In this mode of thinking, increasing the amount of satellite imagery directly contributes to transparency.

At the same time, more government-owned spy satellites do not have the same effect. Consequently, another important dimension of transparency is the accessibility of information. Albeit restrictions remain (see chapter 5), the commercialization of remote sensing has made satellite imagery accessible to a broader public. Moreover, non-governmental users of satellite imagery share the information as widely as possible. So, only when the information derived from satellite images is publicly accessible it fulfills the purpose of transparency. Taken together, then,

non-governmental remote sensing understands transparency as the amount of publicly available information on a security threat.

Transparency and Security

In non-governmental remote sensing, transparency is conceived as a virtue (cf. Birchall 2012). There are different beliefs about the power of transparency to create better policies, post-hoc accountability and to deter potential security threats from happening in the first place. Overall, however, non-governmental actors agree that the more transparency is created the better. Echoing much of the existing research and news reporting, informants discuss the benefits of satellite-based transparency on an operational or case-by-case basis. In public statements of imagery providers, analysts, government officials, space agency employees or space enthusiasts it is usually the same handful of use cases that are presented to demonstrate the benefits of transparency in general and EO satellites in particular. Examples are listed that show how satellite imagery contributes to efforts to promote arms control, increase refugee safety, monitor human rights or advance environmental protection. The bottom line, however, remains the same: transparency is good. As such, it serves to justify the use of satellite imagery across a diverse set of issue areas including active conflicts. All the while, informants acknowledge the risk of malicious actors using the same public information for harm. However, they are quick to add that, overall, it is a "net benefit" (Informant #14). They generally "err on the side of transparency" (Informant #3), believe that there is "more value to get from using the imagery as opposed to blocking the imagery from being seen by rebels" (Informant #5) and "think on balance it's overwhelmingly a good development" (Informant #46). Being focused on the operational level, more abstract risks are disregarded and questions who, when or even, if somebody should be maximizing global transparency are blocked out.

The drive to maximize transparency is also fueled by the conviction that transparency helps to bring about peace and security in global politics. It is associated with conflict resolution and international cooperation because it lifts the fog of war that arguably fuels mistrust and miscalculation in conflicts. This is also in line with the U.S. National Space Policy which argues that "[s]atellites contribute to increased transparency and stability among nations and provide a vital communications path for avoiding potential conflicts" (US Government 2010: 1). Overall, non-governmental actors agree with this general assessment that has been around at least since the Cold War. They assume an immediate relation between transparency and security, although they struggle with spelling out the mechanisms: "I hope, I still hope, somehow, some way, that transparency makes us safer. That was the whole premise between the U.S. and the Soviet Union. If I can see what you're doing and you can see what I'm doing, that should create some uneasy level of trust" (Informant #47). Ongoing research points towards contextual factors that need to

be in place for transparency contributing to security (Lord 2006). It is by no means an undisputed relation. Nevertheless, non-governmental users of satellite imagery consistently emphasize "ultimately transparency serves everyone" (Informant #24).

Right to Transparency

Because transparency is constructed as virtue that is beneficial for everyone, non-governmental actors presume a right or even a moral obligation to maximize transparency. This fits into a larger narrative about growing transparency that has corporations, international organizations and governments willfully disclose information (Florini 1998). The commercialization of satellite imagery has been a part and driver of this narrative. It has normalized the overhead view of remote sensing and led to an expectation that imagery is available within hours, not days, when reports are emerging about a natural disaster or conflict. Moreover, because everyone is supposed to comply to the new virtue of the "age of transparency" (Larkin 2016), secrecy alone is rendered suspicious. For non-governmental remote sensing there is no difference between observing Pakistan, Yemen and North Korea or Canada and Norway because "everybody has to be transparent now" (Informant #14). Crucially, though, it is the observers that invoke the right to transparency and it is the observers that choose who has to become more transparent. No permission or prior engagement is required. In that logic, more hesitant or secretive countries such as North Korea bring it upon themselves to become a subject of consistent non-governmental remote sensing. If only it would abide to Western standards of openness, it would stop the "what's happening in North Korea industry" dead in its tracks (Informant #41). In fact, some informants imply a moral obligation to maximize transparency because it not only benefits everyone but it saves lives: "So, the more clearly you can penetrate the fog of war and give all sides accurate information; then you might be able to save more lives. […] Indecision and inaction are a moral choice that you can make. But oftentimes if you are indecisive or fail to act, your indecision or failure to act will cost more lives" (Informant #13). Non-governmental users of satellite imagery infer that secrecy is suspicious and that they have a prerogative to extract information if it is not voluntarily provided. In that sense, they force transparency. It is forced in two ways. First, because the information is not voluntarily disclosed. Second, because it is a one-sided extraction of information that is not reciprocated. From this position of power and convinced of the overall net benefit of global transparency, non-governmental remote sensing advocates "full-throttle transparency" (Informant #47).

From Surveillance to Transparency and Back Again

Against this background, it becomes increasingly difficult to conceptually separate the transparency of non-governmental remote sensing from the surveillance of governmental

geospatial intelligence. Both violently extract information from somebody who is not providing it voluntarily. Moreover, it is no reciprocal relationship. Transparency is forced in one direction. Moreover, the observed rarely participate in the remote sensing efforts nor are they engaged based on the information extracted from them. As has been shown in the previous chapters, the owners and users of commercial satellite imagery are largely U.S. or European companies and non-governmental actors. Their efforts to increase transparency are focused on the Global South (Rothe and Shim 2018). In this sense, they are forcing their idea of transparency upon others. Despite the belief that transparency serves everyone, the benefits appear unequally distributed. In fact, if transparency is based on one-sided extraction the promised benefits arguably require a re-evaluation. Voluntary transparency in which an entity willingly discloses information is often by itself considered a show of trust and good will. On the other hand, involuntary transparency is associated with hidden or malicious agendas. Consequently, the political effects of forced transparency differ from the expectations of most non-governmental actors that associate it with conflict resolution, trust and cooperation. First, forced transparency, just like surveillance, rather serves to reveal injustice, name and shame and hold others accountable. While this is important, it stops short of including the observed into the project of non-governmental remote sensing or create opportunities for participation and engagement that would lay the foundation for shared interests and mutual trust. Second, even if the information is provided publicly it does not benefit everyone in the same way depending on what is exposed and how it is interpreted. In other words, the "diffusion of information is not politically neutral" (Lord 2006: 4). Although more information might benefit the weak in some ways, powerful actors are more likely to have the means to absorb and take advantage of the ever-growing amount of information. Despite the differences between voluntary and forced transparency, non-governmental remote sensing keeps maximizing the latter.

7.2.2. Maximizing a Virtue: The Technologized Cycle of Transparency

Incomplete Transparency?

The ongoing maximization of forced transparency, that is promoted by non-governmental remote sensing, is embedded in a self-reinforcing cycle. Satellite imagery analysts and users acknowledge the imperfection of remote sensing. The co-production of security threats based on EO satellites introduces technological, political, economic and human limitations (see chapter 5). The acquisition of commercial satellite imagery is already biased. Techno-political reasons from orbital limitations to cloud cover to the U.S. influence over tasking decisions distort and skew the imagery archives. On top of that, non-governmental actors often face limited financial means to buy the imagery they need to adequately address their problems. During imagery interpretation additional issue arise: A lack of expertise in the non-governmental sector exacerbates the

difficulties of satellite imagery analysis. And even hiring professional analysts cannot eliminate the complications brought about by the materiality of security threats. Despite those constraints, non-governmental actors employ satellite imagery of security threats to make sure that the public is made "aware of those sorts of things and that the extent of these violations can be better quantified" (Informant #3). While they do believe in improving the understanding and transparency of security threats, they also acknowledge that it remains incomplete or imperfect. An individual satellite imagery alone cannot achieve the virtue of complete transparency.

Following the definition outlined above, incomplete transparency is nothing but a lack of information – a quantity not a quality problem. Satellite imagery analysis of security threats does not at once produce transparency. It is an incremental process. Consequently, the problem of incomplete transparency can be solved by additional information or, more specifically, additional satellite imagery: "we're working from outside here, sort of hacking away at a lack of transparency, if you will, or not enough of it" (Informant #15). Accordingly, non-governmental remote sensing keeps striving for ever more data to finally achieve a state of complete transparency.

A Technologized Response to a Lack of Information

Although the reasons for incomplete transparency are inherent to satellite imagery itself, non-governmental actors imagine a technological fix to solve this problem. In this way, the maximization of virtue is reinforced by the technological potentials of satellite observation.
Satellite imagery analysts in particular argue that increasing the imagery quality automatically produces more information because "for every doubling of the spatial resolution, there's a quadrupling of the interpretability. So, to go from 2m to 1m, you will be able to extract more details" (Informant #6). In fact, they are excited about the possibilities of even better high-resolution satellite imagery than the current 25cm limit as required by current U.S. legislation. It is believed to be important because more information, i.e. more transparency, translates into more influence on events on the ground. This can be illustrated by the example of North Korea's political prison camp system (see also Olbrich 2019a). As a site of crimes against humanity including unlawful detention, torture and executions, it is a paramount focus of multiple human rights NGOs as well as a Commission of Inquiry of the United Nations (UN). The UN commission has produced a report based on open-source material including refugee testimony as well as satellite imagery. The report includes a note of regret about North Korea's uncooperative behavior but also about the reluctance of other states to provide governmental satellite imagery since "[a]lmost certainly, higher resolution satellite imagery produced by more technologically advanced states would have provided further information. Unfortunately, despite requests, these images were not made available to the Commission" (UN Commission of Inquiry on Human Rights

in the Democratic People's Republic of Korea 2014: 14). Because governments would not allow UN investigators access to their national capabilities, they have used commercial satellite imagery instead. The report suggests that if only the resolution of satellite imagery would be better, they could define human rights violations even more accurately and hold the DPRK accountable for "satellite imagery resolution is eventually going to bring it to a point where the North Korean regime can no longer deny that these camps exist" (Informant #9). Furthermore, it would finally make the global public realize the extent and urgency of the human rights situation in North Korea (Hong 2011; Hawk 2012). Apparently, the human rights community identifies incomplete transparency and a lack of information as the obstacle to political impact. To counter this lack they seek to extract ever more information from every satellite image. This is also the promise of providers and early adopters of spectral satellite imagery. Instead of reducing the pixel size for better spatial resolution that eventually makes it easier to identify visible objects on an image, they pay attention to "what information is held within that pixel regardless of what it is" (Informant #22). As every material object reflects light in unique ways, it has a particular spectral fingerprint. This way it is possible to identify different gases in the atmosphere, locate natural resources across large areas or determine plant species from satellite imagery. Taken together, the belief in increasing the amount of information drawn from an image for great political impact re-affirms the understanding of transparency as information that is received, understood and used by everyone in the same way.

Improvements of the temporal resolution of commercial remote sensing are identified as a second fix to incomplete transparency. The growing number of imagery providers have made it possible to receive daily updates of satellite imagery should the weather conditions allow for it. Many of the informants argue that this development has

> *"just fundamentally changed the way we look at imagery now. Daily images of the planet before like ten years ago was absurd. That's like a science fiction, Orwellian future thing. And say what you will about that, I'm super excited about it because I can check all of the sites that I found or that I'm interested in in North Korea and I can see what's happening there on a daily basis and that has just changed everything"* (Informant #20).

Although the statement implies some consideration of privacy violations, possible misuse or unintended consequences, the potential of daily imagery to bring about complete transparency is fully embraced. The growing amount of satellite imagery would involve an even greater number of amateur and professional analysts as well as the development of new techniques. This includes automated analyses that provide real-time information on changes in poverty, deforestation or military movements. Some informants even fantasize about constant, CCTV-like remote sensing

that would allow for patterns of life analyses that are more difficult to do with individual shots which are days apart.

When it comes to addressing problems with incomplete transparency, the non-governmental remote sensing community banks on technological development to fix the problem. There is a strong belief that resolution is only going to improve and there is going to be more imagery: "So, the importance of satellite imagery as a critical tool in the tool kit made available to the human rights researcher, that importance is going to continue to increase" (Informant #38). The determination about the value of non-governmental remote sensing also finds expression in the suggested economic prospects of commercial satellite imagery whose "market will only get saturated with 24-hours a day video. That's the point when it gets saturated. In high-resolution at 1m per pixel. Because now you're watching everything on Earth all the time. That's the only – that's not too much – but that's the point where you probably don't need more" (Informant #21). This idea of technologized virtue maximization renders it difficult to imagine a point when enough transparency has been achieved. Non-governmental actors identify a lack of transparency as the central problem for sound policymaking, cooperation and enhancing security. The growing number and capabilities of EO satellites are the chosen fix because they afford the potentials for more information. Therefore, "companies should be unleashed. We should stop limiting the technological progress and financial bottom line – like DigitalGlobe. If we are in an argument about different types of imaging operations that we are to allow or not allow under licensing regimes: If the technology can do it, let it be" (Informant #47). Increasingly, this also means the combination of satellite imagery with other (big) data sources such social media feeds, conflict datasets, tracking data from ships or planes and so forth.

Fitting into the narrative of incomplete transparency are demands to expand non-governmental remote sensing to other issue areas. In this sense, the virtue of transparency becomes universally applicable. More publicly available information serves everybody:

> *I'm interested in seeing the model expanded and applied to other emerging global threats such as a pandemic or a dirty bomb or civil unrest, famine, a tsunami, environmental degradation, toxic pollution, a radiation leak caused by tsunami or earthquake or other types of emerging global threats that require international cooperation and transparent information sharing in near real-time including among states that may not be politically aligned. For example, if a virus breaks out it has no political identity, it does not stop at a border checkpoint. So, if there is a fast-moving epidemic of a virus, then states who may not be inclined to cooperate need to be able to quickly share information transparently to solve the problem* (Informant #13).

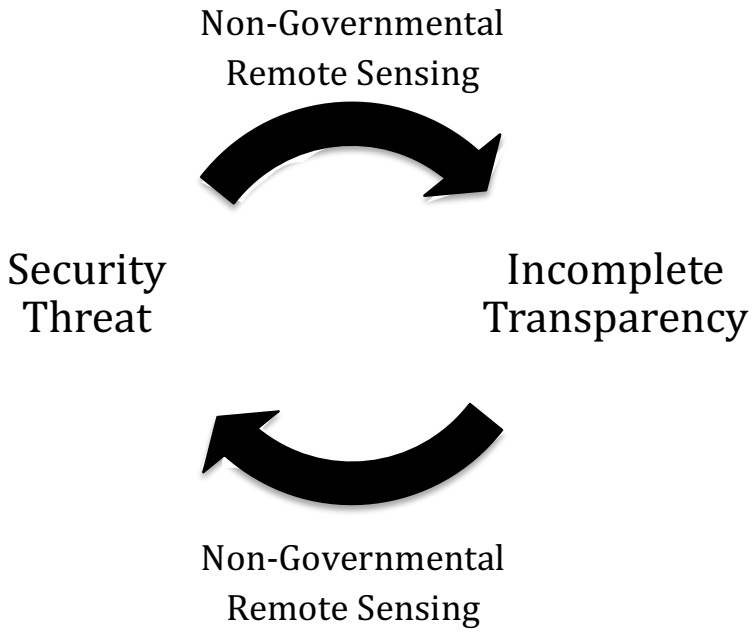
According to this and other informants, non-governmental remote sensing works in bringing about transparency. However, to achieve a greater political impact the practice needs to spread and extend further. As technological development breaks down entry barriers and reduces imagery prices, the vision is to scale satellite imagery projects across NGOs and civil society on a global level. Non-governmental remote sensing is driven by the virtue of transparency. As this pursuit becomes technologized, though, transparency is consistently being forced.

Technologized Cycle of Transparency

What is not a part of this line of thinking, though, is the impossibility of complete transparency. No matter how good the spatial, spectral and temporal resolution of commercial satellite imagery is going to become, it will not be enough to create unambiguous information about material security threats. Even if a one-time satellite imagery produced an objectively transparent assessment of the current state of affairs, it would leave future risks unaddressed. In this sense, the necessary amount of publicly available information to create transparency is infinite.

Put differently, non-governmental remote sensing is caught up in a technologized cycle of transparency (see figure 4): The virtue of transparency is consistently being reinforced by the technological potentials and constraints of satellite technology. More specifically, uncertainty about a security threat starts the cycle with non-governmental remote sensing. Commercial satellite imagery is used to produce more transparency about the threat. However, due to techno-political limitations inherent in commercial satellite imagery, this only leads to incomplete transparency. As this is understood as a lack of information, more and better non-governmental remote sensing is requested which restarts the cycle.

Figure 4: Technologized Cycle of Transparency



Although complete transparency is impossible, the cycle keeps maximizing forced transparency. It extracts information from the observed. This cycle is fundamentally driven by the technological potentials and constraints of commercial satellite imagery in that the maximization of virtue goes hand in hand with the maximization of technological fixes. Commercial satellite imagery gives non-governmental actors the fairly straightforward techno-political potentials to demand and produce transparency on a global scale. However, one informant noted in a discussion about the effects of non-governmental remote sensing that "what they sometimes don't realize is that a genuine desire to help can sometimes have very negative consequences" (Informant #19). Indeed, the technologized cycle of transparency encapsulates the good intentions of non-governmental users of satellite imagery. At the same time, the maximization of forced transparency bears considerable risks. In a dialogue with Maurizio Ferraris, Jacques Derrida gets to the heart of the value of secrecy in an open society when he argues that "the demand that everything be paraded in the public square and that there be no internal forum is a glaring sign of the totalitarianization of democracy. I can rephrase this in terms of political ethics: if a right to the secret is not maintained, we are in a totalitarian space" (Derrida and Ferraris 2001: 59). Secrecy is a constitutive part of transparency. Once it is eliminated, transparency borders totalitarianism. The conceptual ambiguity between surveillance and forced transparency further emphasizes the importance of weighing the potential fallout from increasing non-governmental remote sensing. While assessments of remote sensing mention negative effects, they commonly focus on operational, individual errors. The following section takes it to a more abstract level by examining non-governmental remote sensing as a global security practice.

7.3. Risks and Implications of Forcing Transparency

7.3.1. Remote Governance

As non-governmental remote sensing forces transparency, it also increases the political reach of non-governmental actors. Commercial satellite imagery enables and contributes to a form of non-governmental remote governance. Access to EO satellites moderates time, workforce and financial factors in the decision-making of NGOs and think tanks and allows them to monitor and control various areas at the same time. This way, it is possible to address security problems without delay over logistics, bureaucratic red tape and funding. Moreover, aid and governance efforts are not to be stopped by inaccessible terrain, bad weather or violence. At the same time, multiple crises can be tackled at once and across issue areas. Effectively, a small-scale NGO in a Washington back office can monitor a number of security hotspots worldwide concerning issues as far-ranging as regional conflict, deforestation, trafficking, global health and forced displacement. This is possible without permission, on-site personnel or knowledge about the local context. Effectively, non-governmental actors reach into states to extract information and act upon both belligerent and malicious actors as well as vulnerable or insecure populations. Because the information situation is usually worse in countries of the Global South, they become the focus of remote governance which "reifies a global discourse of alterity" (Rothe and Shim 2018: 425). EO-powered remote governance fits well into a trend of personnel retreat, bunkerization and technological responses in journalism, diplomacy or international humanitarian aid (Willmott 2010; Worth 2012; Jacobsen and Sandvik 2018; Kalkman 2018). In doing so, however, it not only reinforces skewed power relations and discourages engagement but also manages insecurities instead of addressing their root causes.

Biased Power Relations

Forcing transparency means the extraction of information from others. This one-sided relation translates into corresponding forms of governance in which the observed are rendered passive and silent. This is reinforced by the hierarchy of evidence implicit in non-governmental remote sensing (see chapter 5). Material threats are more likely to find their way on the political agenda than the intangible concerns and interests of the observed. It is more difficult to deny the legitimacy and existence of matter (Barry 2013a: 145-147). Moreover, the evidentiary character of a material threat makes verbal contributions to or objection against the same issue presumptuous. The observed and governed are in no position to add anything substantial because they cannot offer a counter-narrative "which follows the same hierarchy of material evidence" (Olbrich 2019a: 78). Despite the various uncertainties inherent to satellite imagery analysis, the observed face an uphill battle against the visuo-material persuasiveness of remote sensing. Consequently, assertions of innocence or pointing out the complexity of the local political

situation are rendered moot. This applies to North Korean insistence on the peacefulness of its space program (Olbrich 2019a; Olbrich and Shim 2019) as well as the monitoring of global forest fires where it "was much easier to tell looking at the images that these were related to land clearing. And most likely the companies in charge of the concession are using the fire to clear their land. Although they would also claim that they were just getting encroached by others" (Informant #32). The observed are not to be believed over material facts derived from satellite imagery. In fact, the very advantage of technologized transparency is the independence from interest-driven sources and politically biased interjections. In other words, consulting the observed and governed distorts the technoscientific way of knowledge production.

At first glance, the translation of security threats into material terms could be associated with a depoliticization of the issue at hand. After all, the materiality suggests to provide irrefutable facts free from political taint so that deliberation appears unnecessary to determine the nature and urgency of security problematizations. Effectively, though, non-governmental remote sensing can lead to both depoliticization as well as politicization depending on the conditions. By way of illustration, when numbers are invoked in political debates they can support a strong quantitative argument that serves to close a controversy and end discussions. On the other hand, the same persuasiveness can arguably be employed to politicize a hitherto neglected political issue and put it on the agenda. This raises public awareness of the matter and motivates groups to politically position themselves (Baele, Balzacq, and Bourbeau 2017). Similarly, Delf Rothe (2015) contends that the (de)politicizing effects of technologies in securitization discourse about climate change are ambivalent. Digital climate models and other technologies have the power to create publics and politicize climate change. At the same time, they tend to ignore the socio-political context and shift political responsibility and decision-making onto material actors which depoliticizes the issue (Rothe 2015: 119-120).

The same applies to forced transparency. Non-governmental remote sensing translates material manifestations on an image into security threats. Voluntary or not, the publicly available information can either raise the public saliency of the threat or forestall further political debate. Regardless of the (de)politicizing effect, however, the observed are usually silenced. Even when a security issue makes it to the top of the agenda and political groups start to position themselves, the observed are rarely actively included or engaged. The question is not whether (satellite) technologies depoliticize security threats or not but who is excluded in political debates about how to problematize and address them. In many remote sensing projects, the observed are not only literally invisible on the satellite image but also absent from discussions about the problematization. When NGOs and think tanks map security threats, environmental exploitation or humanitarian needs, they usually do not engage the concerned people on the ground. In the

cases of actors like North Korea or Iran, they do not expect honest, apolitical contributions to objective transparency while disaster-affected populations cannot rival the overhead view afforded by EO satellites. As such, non-governmental remote sensing reifies power relations between the observers and the observed. Transferred to an economic context, global self-regulating insurances become imaginable that protect farmers against droughts and other severe weather events: Based on satellite-based data, insurance payments could be made automated without consulting the claimant while assertions that contradict the data are simply not eligible.

Disengaging the Observed

Non-governmental remote sensing enables a one-way remote governance that is unresponsive to discursive contributions of the observed because they do not follow the same hierarchy of evidence as satellite imagery. Moreover, when it comes to real-time monitoring of security threats, engagement of on-the-ground sources usually slows things down. As a result of the one-sidedness of remote governance, non-governmental users of satellite imagery face ethical, sometimes life-or-death, decisions. Two examples serve to illustrate the nature, power distribution and implications of the governance relation between observers and observed.

In December 2016, members of the White Helmets contacted the Harvard Humanitarian Initiative (HHI) (Livingston and Drake 2017). They were trapped in eastern Aleppo with their families, surrounded by Russian and Syrian government forces asking for an evacuation route to safety. Quickly, satellite imagery analysts, human rights researchers and commercial imagery providers assembled around the common cause. In the evening analysts received high-resolution satellite imagery of the White Helmets' location from the same morning to identify potential threats and determine a safe way out of Aleppo. The time pressure and high stakes of the situation made everybody involved realize that they were responsible for the outcome (Livingston and Drake 2017). Perhaps it was possible to identify and draw up a safe route based on the satellite imagery at hand and provide clear enough instructions to follow. However, the volatile security environment jeopardized any potentially safe escape route because troops and military vehicles could have moved the second after the imagery was taken. So, even though the imagery was acquired so quickly, it could not provide information that was current enough. Therefore, the researchers and imagery analysts faced the decision whether to provide the White Helmets with the best analysis possible and let them decide whether to leave their hiding space, or withhold the information. Acknowledging the difficulty of the question, they concluded not to share the information: "we could not involve ourselves in life-or-death decisions, even though technology presented us with an opportunity. Perhaps with even more commercially provided information, we at Harvard and AAAS might have come to embrace the role technology had afforded us" (Livingston and Drake 2017). Faced with an exceptional burden of the situation, the group of non-

governmental actors acknowledged the limits of transparency. They were aware of the dire situation of the White Helmets and reasonably inferred that they might follow the evacuation route without appropriately accounting for the considerable risk. At the same time, the network of AAAS and Harvard confirms the idea of the technologized cycle of transparency when they contemplate whether they had reversed their decision if only there was more information and more transparency possible. In any case, it was their decision – not the one of the observed – upholding the idea of one-way remote governance.

One informant reported on a similar situation, in which researchers and analysts had decided differently.[27] They received near-real-time satellite imagery of an evolving security situation that showed military troops closing in on a rebel-held town including a hospital. Previous observations suggested that the troops were likely to bomb the area indiscriminately. Despite a heated debate, one group member called the hospital to warn about the imminent danger. As it turned out, the hospital was evacuated and targeted but not hit during the bombardment. Understandably, the informant struggled to ethically evaluate the decision to inform the hospital but eventually concluded that "giving people the information and letting them make their own decisions is ethical" (Informant #X). In the second example, the group of non-governmental researchers similarly acknowledges the limitations of transparency but ultimately, and not without controversy, leaves the observed free to decide how to respond to the information.

Both cases describe exceptional episodes. Nonetheless, they illustrate the power relations involved in non-governmental remote sensing. Given their exclusive access to EO satellites, the observers hold sway over what information finds its way into the public and to the observed. Regardless of their decision to share the information, it remains at their discretion how to move forward. Admittedly, they face tough ethical decisions. But they also act from a position of safety; no matter how they decide they are not physically harmed. Taken together, non-governmental remote sensing holds the potential to both politicize and depoliticize security threats. In both scenarios, however, the observed are not actively engaged but silenced as they neither can make a substantial contribution nor keep up with the speed. This reinforces a one-sided form of remote governance in which the observed are at the mercy of the observers.

Transparency Replaces Dialogue

Forced transparency risks excluding vulnerable and insecure populations as passive and detached objects of observation. As a result, political dialogue and engagement are increasingly rendered as a non-starter because satellite imagery plainly "shows" human rights violations, nuclear

[27] Given the exceptionality of the story, the time and place as well as the identifying number of the informant are left out to protect her/his anonymity.

threats, illegal deforestation and who is in need. Put differently, "seeing" insecurities trumps talking to the insecure and those responsible while further satellite imagery reinforces this logic (see section 7.2.2.). While non-governmental actors argue forcing transparency benefits everybody including the observed, the observed are rarely engaged based on the information gathered. Instead, the information itself is supposed to take their place because its indisputable, evidentiary attributes better represents their position. Similarly, the information is not employed to connect with the perpetrators of insecurity or start a dialogue. Instead, satellite imagery is embedded in strategies of naming and shaming. In short, transparency replaces dialogue and engagement with the observed.

However, forcing transparency does not occur in a political and discursive vacuum. More often than not, non-governmental remote sensing focuses on existing security threats with a considerable history. North Korean human rights violations, land reclamation activities in the South China Sea or forest mismanagement in Indonesia are no new topics to international politics. Focusing on the long-standing security issues with North Korea helps illustrating this point. The human rights violations as well as the on-going nuclear program are rarely disputed. The latter was even acknowledged by the North Korean regime when it included its status as a nuclear weapons state in the constitution. Regular remote sensing incrementally increases knowledge about both threats, although it is usually quite marginal. Because of the alleged credibility of satellite imagery, it acts "as a stand in for North Korea as a dialogue partner and lays the ground for a policy strategy that discourages dialogue but rather aims for regime change" (Olbrich 2019a: 79). Going further, non-governmental remote sensing barely needs North Korea or any of the observed but as a projection surface for satellite imagery of security threats (Olbrich 2019a). As such, it discourages political dialogue and forces transparency to monitor and discipline the observed.

Nevertheless, non-governmental actors bank on more information as an adequate response to long-standing disputes. Ignoring the potential side-effects and perception of producing more of the same information they keep forcing transparency: "We have a stated mission, that mission is not China bashing. The mission is transparency" (Informant #7). Accordingly, the political impact of information is closely followed and success is measured in global media traction and making an appearance in traditional political and diplomatic settings such as U.S. Congress hearing or the United Nations.

Managing Insecurities

When non-governmental remote sensing discourages dialogue but forces transparency, root causes of security threats remain unaddressed. The ever-growing amount of information

remotely manages, monitors and controls insecurities instead of confronting them. If non-governmental remote sensing is not used to directly engage the observed, its impact depends on the existing system of global politics. It will add relevant information about security threats to the political discourse and in rare cases even provide a "smoking gun." However, even a smoking gun does not inevitably lead to political accountability and consequences. Herein lies the tragedy of the technologized cycle of transparency: It suggests to proponents of non-governmental remote sensing that once more and better satellite imagery is available, transparency will pierce through that system. However, as of now, forcing transparency has not solved the political will problem: Even when clear-cut, public information is available, relevant and capable political agents needs to act on it.

Although it does not affect the cycle of transparency, some disillusionment is already taking hold in the non-governmental remote sensing community. Given the dearth of satellite imagery released on security threats in Syria, Ukraine or Myanmar, there is growing pessimism "about being able to use this technology to make the case to pursue a particular course of action" (Informant #6). The impact of forced transparency hinges on the political will to enforce norms when they are violated – even less likely in authoritarian, corrupt or administratively weak political systems. Similarly, there are doubts about the deterring effects of non-governmental remote sensing. This idea suggests that the consistent surveillance prevents norm violations from happening and incidentally dispenses with the need for post-hoc punitive action. Among others, human rights projects like the Satellite Sentinel Project or Eyes on Darfur have applied this logic with limited success. The civil war and humanitarian catastrophe in Syria are also regularly cited as a reason for growing skepticism. Unlike any other conflict before, it has been consistently observed which produced a ton of potential evidence to bring perpetrators to justice. However, "the continued level of violence that we're seeing in many of those conflicts around the world is pretty strong evidence that to the extent that there is a deterrent effect, it may be a pretty mild one" (Informant #4). Yet, perhaps it is too early to tell. Once the satellite imagery is used in courts the effects might appear more forcefully.

As of now, non-governmental remote sensing enables a one-sided form of remote governance that renders the observed silent and passive bystanders. They are disregarded as relevant stakeholders for the pursuit of transparency. Moreover, the firm belief in the virtue of transparency prevents political engagement with the observed to address the security threats. Instead, transparency manages insecurities. The amount of public information about human rights violations, environmental degradation and military programs surpasses anything ever before so that "the world can't say they didn't know. The only thing they can say is they don't care, sadly" (Informant #47). However, if non-governmental actors do not employ satellite imagery to

start a political dialogue and engage the observed, it does not matter how objective or telling the information appears. Because ultimately forced transparency is subject to the same political constraints.

7.3.2. Diplomacy Under Forced Transparency

Diplomatic Complications

At the same time, forced transparency becomes a condition of global politics and changes the environment in which political agents act. Secrecy, uncertainty and the strategic use of information are an important part of diplomacy so that global transparency shifts incentives and constraints concerning political options. As the hypothetical scenario of the Cuban Missile Crisis has illustrated, "[t]ransparency complicates diplomacy. Governments once had more control over what information was available to the public and derived influence from that control. Now governments must compete with more and more independent sources of information and are less in control of their message" (Lord 2006: 127). As the reluctance of governments to share satellite imagery with the UN to document North Korea's political prison camp shows, they still shy away from tipping their hand by revealing their knowledge and technical capabilities. Of course, militaries have been under satellite surveillance for decades. The change and inconvenience lie in the publicity that defines the notion of transparency inherent in non-governmental remote sensing. Although this does not necessarily have immediate negative effects on national security, it forces governments to relate to the public and forces a conversation.

Once a security threat is made known to the public, whether the government already knew about it or not, it often evokes a public reaction. In any case, the public is given a reason to demand a statement that depending on the situation at hand signals resolve, condemns what is happening, assures support or simply acknowledges that the situation will henceforth be monitored. Non-governmental actors acknowledge that when they are publicly accusing governments of wrongdoing, this might prompt mere rationalizations; but "at least now they're being forced to provide some explanations – however absurd they may be at times – as opposed to operating in complete darkness where they don't have to explain themselves to anybody" (Informant #7). In the end, forced transparency compels governments to explain their actions and create some kind of narrative to justify them – of course, whether it is true or not is another matter.

Limiting Policy Options

This also concerns powerful countries that see their monopoly of information erode. For example, working on information provided by a dissident group, a D.C. think tank used commercial satellite imagery to pressure the Bush administration to acknowledge the existence of Iran's nuclear enrichment program (Aday and Livingston 2009). As this happened in the follow-up to the Iraq

invasion, it distorted the U.S. administration's messaging. While it knew about the Iranian nuclear sites it decided to keep it secret and concentrate on the alleged Iraqi WMD program. So, in addition to forcing a conversation, global transparency more readily introduces the domestic and global audience into foreign policy making. As such, forced transparency is not just an inconvenience to diplomats and policymakers but holds tangible implications for global politics.

Similarly, various South Korean administrations are reported to have strategically publicized or withheld information on North Korea. For example, planting information about its nuclear program could serve to distract from unfavorable domestic debates. In times of rapprochement, however, there is a reserve on the part of some South Korean lawmakers for communicating a lot about the extreme human rights abuses in North Korea as this might polarize the situation. In this sense, forced transparency might limit the room for maneuver in terms of political options. With non-governmental remote sensing of North Korea in high demand, it regularly finds its way into national newspapers. As new discoveries are rare, the reports frequently focus on the ongoing nuclear and missile program and the disastrous human rights record and consistently reinforce the negative image of North Korea (Hong 2013; Shim 2014). In this way, forced transparency holds in place a view of North Korea as illegitimate, brutal and resistant to change which, in turn, makes it more difficult to advocate for serious engagement or humanitarian support. Following this very logic, an additional section has been added to the U.S. North Korea Sanctions legislation that requires the Secretary of State to submit a report about North Korea's political prison camp system and "to include satellite imagery of the camp, in a format that, if published, would not compromise the sources and methods used by the United States intelligence community to capture geospatial imagery" (North Korea Sanctions and Policy Enhancement Act of 2016). As the legislation effectively excludes the use of national satellite sources, it enrolls non-governmental remote sensing into formal policymaking. The provision is added "to force the State Department to stop downplaying the human rights issue for fear of offending Pyongyang" (Informant #10). At the same time, though, it deprives the State Department from strategically adjusting its messaging when it deems useful for ongoing negotiations.

All in all, forced transparency alters the political conditions of diplomacy. The Cuban Missile Crisis probably would have turned out quite differently with commercial satellite imagery of the Soviet missiles immediately publicly available. At the same time, not every country is affected equally. Powerful governments with advanced intelligence capabilities see parts of their monopoly on information erode. Only in rare circumstances would think tanks or NGOs reveal and report on security threats that they were not already aware of. The observed countries, on the other hand, potentially find information about their critical infrastructure or weapons programs in public

sources. Consequently, they need to adapt to a new reality of forced transparency which will be discussed in the following section.

7.3.3. Adaptation Strategies of the Observed

The early days of non-governmental remote sensing are characterized by adaptation processes of the observed which were finding themselves in a novel political environment. At the beginning, some complained about the new transparency of their actions. In 2006, for example, pro-Israeli groups criticized a report by AAAS that documented the damage the Israeli military had brought on Beirut and southern Lebanon (AAAS 2006). The satellite imagery analysis produced upon the request of Amnesty International shows the destruction of civilian buildings and infrastructure reportedly inflicted by cluster bombs, artillery shells and airstrikes. Amnesty also requested damage assessments from Northern Israel. However, the Kyl-Bingaman Amendment prevented the purchase of high-resolution satellite imagery of Israel (see chapter 5). Consequently, critics condemned it as unbalanced and biased reporting that would solely denounce Israel without showing the aggressions of Hezbollah. Even so, this has not stopped non-governmental remote sensing. Nowadays, informants rarely report on complaints about their satellite imagery operations. While the observed were surprised by the new possibilities at first, they have gotten used to and developed strategies for dealing with forced transparency – similar to how intelligence bears counter-intelligence (Prunckun 2012).

Camouflage, Concealment and Deception

One part of what the military calls camouflage, concealment and deception (CCD) tactics is to deny observers an unobstructed view from satellites. The most straightforward ways to do so are timing particular activities when there is cloud cover or at night or transfer activities inside if possible. When North Korea launched a satellite in 2012 from the Sohae Satellite Launching Station, it was relatively easy to observe preparations and follow the progress on satellite imagery. Since then, however, the regime has covered the near-by railway station, built an on-pad assembly hall that can move the rocket to the gantry tower and installed an environmental shroud to hide a possible rocket. In doing so, North Korea limits satellite imagery analyses to assessments of traffic patterns and general activity at the facility so that it becomes much more difficult to assess preparations of another rocket launch. The awareness of forced transparency has also dawned on non-state actors such as IS: They covered a number of streets in Raqqa with metal awnings in anticipation of an impending attack. Arguably, while camouflaging or concealing on-going activities makes clear-cut identification on satellite imagery harder, it also suggests a guilty knowledge.

Another strategy relies on deceiving the observers. During the Cold War, the U.S. military issued so-called Satellite Reconnaissance Advanced Notifications (SatRAN) so that military bases were given a warning of Soviet spy satellites. The orbits of commercial EO satellites are also fixed and, therefore, predictable. Consequently, the observed can time activities accordingly to either avoid or co-occur with an overflight. Sufficiently organized actors are able to feed the observers with information: "[P]laces like China and North Korea, who have active propaganda organs, who have media manipulation historically as a corner stone of their government information policies, have new avenues that they can use with satellite imagery" (Informant #14). This means that the observed can both pretend to have capabilities they do not have or showcase existing technology to signal strength. As such, they can rope in non-governmental remote sensing for their own purposes. At the same time, this adds to the factors that potentially lead to misinterpretation and misunderstandings of security threats.

Counter-Visuals

At times, the observed also choose to offer a counter-narrative based on the same or alternative satellite imagery. Offering a different analysis of the same imagery has the advantage of following the same hierarchy of evidence as the satellite imagery itself remains undisputed. On satellite imagery, the detention camps in China's Xinjiang province are rather non-descript buildings that appear inconspicuous at first glance. Therefore, China does not dispute the existence of those facilities to counter claims of wrongful mass detention and violent ideological re-education of ethnic minorities. Instead, it ascribes a different function to them and claims that they are part of a vocational education and training program for the underprivileged (Doman et al. 2018). Going one step further, "states are now pushing back with their own satellite imagery and producing these sort of counter-narratives" (Informant #3). In one of such cases, Russia deliberately mislabeled satellite imagery in the investigation of the downing of flight MH17 in Eastern Ukraine. In a public press briefing, the Russian Ministry of Defense employed satellite imagery to claim that Ukrainian air defense units were active in the area of July 17, the day of the incident. However, when comparing the image to commercial satellite imagery from July 17, Bellingcat – a network of investigative open-source researchers – found multiple discrepancies indicating that the Russian government misdated the satellite imagery to shift responsibility to Ukraine (Higgins 2015).

Lastly, the perhaps most obvious adaptation strategy for observed non-state actors is to adopt commercial and open-source satellite imagery themselves. To this effect, there are multiple reports of terrorist groups using satellite imagery from GoogleEarth in the planning and preparation of operations as well as in their propaganda videos. After the Mumbai attacks of 2008,

it came to light that the attackers used GoogleEarth to familiarize themselves with the terrain and their targets leading to claims to block imagery of sensitive sites on the platform (Bedi 2008).
After initial adaptive difficulties, forced transparency has become the new normal for the observed. It has changed the tactics of militias and terrorist groups as well as how countries have to be deceptive: "[W]e had an advantage that we could watch them without them knowing. But now they know. So, they're just gonna change their methods. Just like criminals have always done. Once they've become aware of new ways to get caught, then they figure out a way to get around it" (Informant #4). Satellite imagery analysts have to take into account the new adaptation strategies in the form of CCD tactics and counter-narratives to avoid misinterpretations and being instrumentalized as amplifiers of propaganda and misinformation. As this makes it increasingly clear that the observers are entangled with the security threats themselves, the following section discusses how they reflect on their relation with the observed.

7.3.4. Becoming Part of the Security Threat

The Temporality of Security Dynamics

The episodes about the evacuation of the White Helmets and the hospital in danger of being bombarded have already illustrated that non-governmental actors at times become actively involved in the conflicts they observe. For decades, human rights NGOs have interviewed victims and perpetrators, reviewed government documents and photographs in order to reconstruct and document crimes and abuses. However, satellite imagery in concert with social media allows for the monitoring of conflicts in near-real time. Informants find this to be a crucial change to their previous work:

> *So, it meant that we were providing what could be perceived as…you know we were part of a kinetic environment…I mean we were monitoring an active conflict…where there are two armed groups on either side and we were reporting on both; yet it was for the purpose of looking at what was happening to the civilian population. So, it made us ask a lot of questions about what standards need to be in place? Data security procedures, the ethics of doing this type of work…and so it really showed us that these are going to be a lot of the emerging questions* (Informant #36).

Steven Livingston and Jonathan Drake, who were part of the group attempt to help the White Helmets in Aleppo, come to a similar conclusion that real-time observation is qualitatively different (Livingston and Drake 2017). In other words, the temporal component makes the difference if satellite imagery involves observers more actively in the events on the ground. It is an important distinction because it suggests that only then observers are accountable for the consequences of what, when and how they made information public. Admittedly, the intensity of

the involvement differs depending on the situation at hand. Near-real time observation of active conflicts introduces a particularly sensitive dimension because it might endanger already vulnerable populations. Having said that, when non-governmental actors force transparency they become entangled with the problematization regardless of the timeline. Non-governmental remote sensing does not allow for neutral, detached observation. Albeit some activities do not immediately jeopardize the safety of the observed, the political impact renders them participants in the security dynamics. Satellite imagery is used to verify or refute claims made by parties to the conflict or point a finger at suspected perpetrators. In either case, it adds to the complexity of the situation. Even when long-standing security issues are monitored on a regular basis, the consistent surveillance can be instrumentalized by countries to showcase their military capabilities or other actors that profit from highlighting the existence of a security threat including political parties, weapon manufacturers or advocacy groups.

Non-Governmental Reflection of Satellite Imaging

The above quotation already acknowledges some ethical reflection regarding non-governmental remote sensing as a security practice. Mostly, this is the result of post-hoc analysis. Non-governmental actors accepted the virtue of transparency as publicly available objective information only to learn that they actually become entangled in the security situation on the ground. As a result, they potentially endanger the beneficiaries or unrelated observed populations. Similar effects have been documented for other technologies such as when the public data of wearable fitness trackers identified the location of military bases (Hsu 2018) or crowd-sourced crisis maps increased the risk of attacks against humanitarian and development workers (Zwitter 2015). As a response to that, some working strategies have emerged to protect vulnerable populations. Especially in security situations that evolve in real-time, non-governmental actors would commonly withhold the specific coordinates of satellite images. While the geolocation adds a layer of credibility to the analysis, it also risks endangering vulnerable populations, conflicting parties, cultural artefacts or aid workers all of which are potential targets: "We didn't want to give either side a firing solution on a fixed position to be able to target their opponents. So, we might say, this is an image of a tank but we wouldn't say 'and here are the geo-coordinates'" (Informant #13). In doing so, they remain in their documenting role and would only provide the precise coordinates if they are necessary for later investigation. In other instances, the release of information is delayed until the security situation has settled. For example, the so-called Islamic State (IS) made it part of its strategy to destroy cultural heritage sites in Iraq and Syria. Non-governmental groups used satellite imagery to remotely assess the extent of destruction. In doing so, they would also identify archaeological and cultural sites that for whatever reasons had been spared and were still in-tact. As a result, they shied away from

releasing imagery to prevent provoking IS fighters and putting them on the target list. Similarly, some NGOs have delayed the release of satellite imagery showing people who found refuge in a compound or of military facilities that fit the targeting profile of violent groups in the area.

Beyond immediately harmful risks, the question of privacy is largely discounted in non-governmental remote sensing. This is particularly true for environmental groups that usually cover large areas of uninhabited ground. However, even when satellite imagery shows groups of people, the informants commonly argue that the currently available spatial resolution is insufficient to identify a person. Consequently, privacy is a non-issue for them. They largely refrain from engaging the debate on the power and risks of data collection and the associated calls for a more effective governance and an ethical code of conduct for the growing use of data by non-governmental actors (Zwitter 2015; Zwitter and Zicari 2017). This is particularly true for personally identifiable information (PII) which characterizes debates about state surveillance, privacy and civil rights. Simply put, users of commercial satellite imagery argue that no PII is collected and, thereby, any regulatory or ethical demands do not apply to their activities. Expanding such debates for the human rights and humanitarian context, Nathaniel Raymond (2017) outlines the notion of demographically identifiable information (DII). Regulations related to PII are insufficient for the remote generation of information because the practice effectively precludes options to gain individual informed consent from the observed. Moreover, non-governmental actors are not predominantly interested in personal information but group information to support their operations. As a result, they more frequently combine and integrate multiple data streams including satellite imagery which obscures potential risks from resulting data sets. Raymond proposes to acknowledge the growing challenges emanating from the remote generation and combination of data. Consequently, he proposes to implement adequate regulatory and ethical guidelines for non-governmental actors to early on consider the risks of harming vulnerable populations (N. A. Raymond 2017; see also N. Raymond and Card 2015; Sandvik and Raymond 2017). In any case, to a certain extent, non-governmental actors have realized in practice that "by choosing to release this information you're saying that you've thought about what the impact might be on the ground" (Informant #4).

Overall, the extent of thought that is put in the consequences of releasing satellite imagery varies across sectors. Humanitarian and human rights NGOs are more inclined to accept ethical responsibility for the release of conflict information. Arguably, they have more experience working in active conflict and humanitarian settings. Moreover, parts of their operations are built on the foundation of international human rights and humanitarian law which introduces rights and restrictions. In contrast, the security and environmental portion of non-governmental remote sensing shows less hesitation. In these domains, imagery analysts usually focus on long-standing

security threats linked to national military programs or illicit business activities. Therefore, they are more skeptical when it comes to endangering populations or affecting the target list of conflicting parties. In any case, they do not buy into the argumentation that publicly showing those images increases the risk because the locations are already known or accessible through tools like GoogleEarth: "I think most people who are actually involved on the ground, they know where the refugees are. They already know where the burnt villages are in Darfur. So, showing imagery of a burnt-out village and providing an overhead context is not gonna provide the rebels who did the damage anything new" (Informant #5). However, if that is the case then why do many Western security analysts refrain from publishing satellite imagery over current U.S. or coalition partner military operations citing concerns for safety? In such cases, non-governmental actors tend to play down the negative side-effects of remote sensing and deal with ethical complications as they appear.

At the same time, others have identified this problematique and come up with countermeasures. Reflecting on its experience with the Satellite Sentinel Project, the Harvard Humanitarian Initiative has started an annual summer workshop that teaches remote sensing basics for humanitarian actors. Moreover, it has published on the role of humanitarian principles in relation to satellite and other information technologies as well as interpretation guides on satellite imagery analysis for review of damage assessments after disasters and human rights violations (e.g. N. Raymond and Card 2015; Al Achkar, Baker, and Raymond 2016). The Geospatial Technologies Project of AAAS has published similar analysis guides that introduce remote sensing to practitioners (AAAS 2018; AAAS 2014; AAAS 2015).

This rather mixed and varied response to the ethical responsibility of the observers shows it is still an emerging practice. Large parts of the non-governmental sector have only begun to grapple with how extensive the new vulnerabilities are that the technology introduces from an ethical, legal and operational perspective. Early efforts to develop ethical and practical standards for non-governmental remote sensing, at once, are meant to improve the quality of analysis and protect the credibility of the technology. Mostly, these efforts focus on minimizing risks and managing the ethical responsibility that comes with the release of satellite imagery over security situations. Taken together, there is no oversight of the emergent practice of non-governmental remote sensing and organizations approach the same technology very differently. Consequently, ethical decisions that come with what, why, when and how to release satellite imagery are addressed on a case-by-case basis. The non-governmental remote sensing community has not collectively thought through where the limitations of the virtue of transparency lie. Instead, from their position of safety, they are willing to make mistakes and learn by doing which makes non-

governmental remote sensing less predictable and might put people as well as cultural heritage sites in harm's way.

7.3.5. From Documentation to Intervention

Among other things, the ethical ramifications of forced transparency intensify with the proliferation of commercial satellite imagery, the development of satellite technology and, in particular, the growing sophistication of computer-assisted analysis. When non-governmental actors integrate commercial satellite imagery into their regular operations, this usually takes the form of research, monitoring and documentation. Most of the informants, however, already look forward to the future of non-governmental remote sensing that is set to further maximize the virtue of transparency by way of automated analysis.

Data Abundance and Automated Analysis

Much of this future imaginary is based on an assumed abundance of satellite imagery that becomes accessible and exploitable through big data analytics. In the logic of transparency as publicly available information, non-governmental actors embrace the growing quantity of satellite imagery because it helps addressing situations of incomplete information. Dealing with this amount of satellite data is expected to be a serious problem. While human analysts can be specifically trained to identify even vague signatures on an image, they face natural limits when looking at snapshots of 25km^2. When EO satellites capture millions of square kilometers per day, there simply will not be enough analysts to look at all the satellite imagery: The bottleneck shifts from imagery access to comprehensive and meaningful analytics. Consequently, computer vision and machine learning are set to become key in screening, sorting and pre-analyzing large parts of Earth observation data before it reaches a human analyst. In the process, automated tools pre-select which events and features on the image are detected, marked up and forwarded for further analysis. In other words, automated analysis prepares the data for satellite imagery analysts.

When a security think tank employs satellite imagery to observe multiple missile and nuclear sites in different countries, it usually follows a combination of two strategies: First, scanning the media for potential security threats and order satellite imagery when there are reports about suspicious activities. Second, following the imagery catalogues of satellite operators and order every new collection of a set list of areas of interest. Change detection algorithms that run on the streams of satellite data could replace this approach. Instead, it would alarm a satellite imagery analyst whenever there is a somehow defined change in comparison to previous satellite imagery. This way, the security think tank would save the time and money to monitor media reports or new collections. Instead, it would make the news by releasing a satellite imagery analysis of yet unreported security developments.

In addition to change detection, feature extraction relieves analysts from cumbersome and repetitive tasks. This includes marking the same feature over and over again or searching large areas for pre-defined signatures such as tree cover loss, ships at sea or military activities in a desert. Commercial imagery providers and analytics companies already provide tools to automatically identify roads, buildings or vegetation in satellite imagery. The overall idea is to bring to bear the advantages of big data analytics for satellite imagery analysis. In this sense, non-governmental remote sensing follows the technological vision of the U.S. National Geospatial-Intelligence Agency (NGA) that takes automated imagery analysis as a way to "reduce data dimensionality, provide investigative cues based on data correlation and object/change detection, and help the analyst transition from a forensic-based to a model-based approach to GEOINT analysis" (NGA 2014: 3-4). In other words, the human involvement in satellite imagery analysis shifts from self-guided interpretation to supervision and maintenance of the proper functioning of machine-guided analysis.

Interventionist Imaging

Visions of automated satellite imagery analysis also change the time dimension of non-governmental remote sensing. Usually, the focus is on post-hoc analysis of security threats. Approaches such as the Satellite Sentinel Project have already attempted to monitor active conflicts in near-real time. Going further, automated, quicker analysis of larger quantities of satellite imagery hold the promise of forecasting developments on the ground. In this scenario, the political impact of forced transparency moves from documentation, advocacy and accountability to prediction and prevention.

Commercial satellite imagery providers keep moving farther along the value chain of satellite data and aim to provide their customers with pre-analyzed imagery and actionable information. As a result, non-governmental actors depart from looking back into the past "[b]ut now I think we're on the brink of an era where we may be able to do interventionist imaging" (Informant #33). After nearly 20 years of non-governmental remote sensing, imagery providers and analysts have collated a substantial pool of imagery and information. Big data analytics can be employed to mine this wealth of data to identify patterns and correlations hitherto unknown to analysts (Olbrich and Witjes 2016). Projecting these findings into the future allows for making forecasts about security developments on the ground. In other words, taking the human out of the loop of non-governmental remote sensing increases the speed and extent of transparency. The computer-assisted, model-based approaches of imagery analysis produce predictive information that ultimately enables preventive action. Instead of monitoring environmental crimes, security threats and human rights violations, non-governmental remote sensing can contribute "to prevent these things from happening in the first place" (Informant #37). This includes infrastructure

monitoring to anticipate technical disasters, early detection of illegal deforestation, discovering signs of violations of arms control agreements as well as imminent attacks on vulnerable populations. In one prominent example, satellite imagery is employed to help predict illegal elephant poaching in the Democratic Republic of the Congo. Based on predictive analytics of satellite imagery and additional data, it is possible to identify the most likely spots for poachers. Effectively, this reduced the area rangers had to patrol by 90% making it more likely to intervene and prevent the killing of elephants (DigitalGlobe 2015). The same approach was then transferred to other security threats such as tracking rebels or terrorists in inaccessible and vast terrain.

Risks of Predictive Analytics

The automated analysis of an abundance of satellite imagery accelerates the collapse of space and time in the relation between the observers and the observed. Initially, the observed were rendered passive by-standers that interfere with the maximization of transparency. The next step prepares to cut out the observers out of the process of imagery analysis, elevating the role of non-humans in remote governance. The additional technologization of transparency at once further legitimizes the results it brings to light while masking the technological constraints inherent to satellite imagery analysis. As outlined in chapter 5, security threats are produced by way of material approximations on a satellite image: For example, vehicle activity indicates nuclear test preparations, burnt vegetation proves a missile test or untended fields suggest forced displacement. Automated satellite imagery analysis further de-contextualizes those security problematizations when it highlights particular events as suspicious or threatening. In doing so, it delays the possibility for challenging security threats. Before, satellite imagery analysts would serve as intermediaries between the image and the public. They identified a security problematization and proved their analysis in public at the risk of losing their reputation. Yet, once a security problem is highlighted by an automated algorithm the threat is arguably valid until proven otherwise. Moreover, any challengers face the task of disproving an allegedly disinterested, apolitical machine.

Lastly, predictive analytics risk intensifying the involvement of the observers in security dynamics if it becomes possible to forecast migration patterns, attacks on refugees, missile tests or the razing of rural villages. In what ways is there a responsibility to warn populations that might be in danger? Are there ethical or legal obligations to influence what is playing out in real-time? What confidence level does the analysis need to surpass to legitimize action? In the absence of clear principles or guidelines, non-governmental remote sensing moves from forcing transparency to encouraging preemption. Having said that, the technical barriers to predictive analytics remain high. Against this background, the following section discusses how this might affect or even roll back the power relations of non-governmental remote sensing.

7.3.6. Return of the Government

Non-governmental organizations and think tanks encounter various difficulties when working with commercial satellite imagery. Most importantly, sustainable operations require considerable financial resources and know-how to acquire satellite data and properly analyze it. Albeit a growth in commercial EO services is projected to lower the prices, gaining access to the advantages of continued data flows still calls for sizeable investments. Moreover, dealing with geospatial big data instead of individual satellite images requires skills in software programming and machine learning – which are also in high demand in the private and government sector. Consequently, non-governmental remote sensing faces significant barriers in realizing the vision of predictive analytics and interventionist imaging. Instead, the advent of geospatial big data implies a (re)emergence of the role of the government in commercial remote sensing. The economic and human capabilities necessary to reap the benefits of the current techno-political developments are firmly held by large corporations and governments.

The Lasting Influence of the Government

Of course, the government consistently played an important role in non-governmental remote sensing. The present analysis has already revealed various qualifications of the narrative that the commercialization of satellite imagery triggered a power shift from state to non-state actors (see chapter 5). The commercial availability of EO data gives countries without a space program access to intelligence-grade satellite imagery regardless of their democratic commitment or areas of application. In fact, DigitalGlobe states that their "international defense and intelligence customers include friendly foreign governments, many in volatile parts of the world, that rely on us to keep their nations safe" (DigitalGlobe 2017: 8). Moreover, governments use commercial satellite imagery in their organizational and public relations because it saves them the trouble to declassify satellite imagery. In a nutshell, governments remain a relevant driver, regulator and customer of commercial imaging and exert considerable albeit hidden influence on the satellite imagery that enables non-governmental remote sensing.

Overwhelming Data

In the next step of maximizing transparency, satellite imagery is complemented by additional sources such as social media feeds, conflict datasets, weather data and so forth. The value of geospatial big data analytics is the convergence of different sources – similar to the mass data mode (see chapter 6). The majority of informants have indicated an interest in being a part of these developments and reported on limited pilot projects. As of now, however, they are confronted with a "sensory overload" (Informant #20) in that they are partially overwhelmed by the mass of satellite imagery that is currently available. Automatic imagery analysis and the dynamic integration of additional information is even more demanding and sophisticated and

arguably beyond the capabilities of many NGOs and think tanks. Even technologically advanced groups, that could afford the next-level analytics offered by imagery providers, are still hesitant: "We're still figuring out really how we would use it but it's really interesting" (Informant #32).

Government Driver of Geospatial Analytics

The non-governmental sector is no match to better-resourced government entities. Intelligence agencies in particular seek to capitalize on the abundance of data and employ machine-learning for automated surveillance at a global scale. In this sense, the techno-political development of commercial satellite imagery and geospatial analytics does not follow the proven cycle of private innovation in which the government is both late to regulate and adopt the technological tools. Instead, the private satellite industry is actively positioning itself towards government needs and requirements. Leading remote sensing companies DigitalGlobe and Airbus are already closely connected to their respective governments and do not show any intentions of changing that. To the contrary, DigitalGlobe has signed a long-term contract with the U.S. intelligence community worth more than 900 million U.S. dollars over three years to provide satellite imagery and machine learning services (Erwin 2018). Similarly, the former Silicon Valley start-up Planet has acquired an analytics company because of its close links to the NGA and other U.S. government organizations. The merger creates the subsidiary Planet Federal to expand the company's U.S. government business.

In this way, the ongoing shift towards geospatial big data continues to follow a path in which the government acts as an early-adopter of technological innovation which is later marketed to larger corporations before the non-governmental sector takes up slightly adapted spin-offs. As such, the government holds the potential to actualize the technological potentials and follow the vision of interventionist imaging. With that said, this would not maximize transparency because the information is not provided publicly. Instead geospatial big data would enable the "totalizing power of the nation-state," as one informant put it (Informant #49). She or he addresses the risk of governments using the excess of satellite data to automatize and normalize surveillance of people – including its own citizens. While commercial satellite imagery already complements national spy satellites to monitor global security hotspots, an abundance of data and automated analytics set free capacities for domestic surveillance. In such scenarios, the technologies that serve to monitor and detect illegal logging, human rights violations and arms production are put to use for more mundane crimes. In other words, remote sensing would turn from a mostly foreign policy tool into a technology for local law enforcement. Building on ongoing research, geospatial big data then allows for the early detection and sanctioning of illegal activities such as informal building construction (Khalili Moghadam, Delavar, and Hanachee 2015), illicit dumping sites (Angelino et al. 2018) or drug production (U.S. Department of State 2016). Provided a high-

enough resolution, remote sensing could automatically monitor the building of unregistered garden sheds across a predefined jurisdiction. In terms of power relations, the commercial satellite imagery initially allowed non-state actors a peek over the fence. However, the efficiency gains promised by machine learning can only be harnessed with the necessary technical understanding and economic resources. Consequently, the current techno-political trajectory rather favors governments and potentially reverses gains in power of non-governmental remote sensing.

7.4. Conclusion

The chapter shows how the socio-materiality of non-governmental remote sensing forces transparency. From the beginning, transparency has been the key motive for non-governmental actors to use satellite imagery. Hitherto, research has largely focused on the operational level and shows on the basis of case studies how satellite imagery reveals human rights violations, illegal burning of forest or illicit weapons development. Generally, it is portrayed as a tool to reduce uncertainty and inform policy-making. Acknowledging the practical advantages of non-governmental remote sensing, the chapter adds a more critical and abstract perspective to arrive at a holistic assessment of the consequences of transparency. Following the conceptual framework, it first traces how non-governmental actors conceptualize satellite-based transparency in order to allow for an analysis of the overall risks and implications.

Non-governmental remote sensing understands transparency as the amount of publicly available information on a security threat. As such, it is reduced to a quantitative measure so that more information automatically means more transparency. Fitting into a general trend towards transparency in global politics (Dehqanzada and Florini 2000; Lord 2006; Larkin 2016), non-governmental actors generally praise the value of transparency and emphasize its contributions to peace and security. Consequently, they conceive of it as a virtue that needs to be maximized. Going further, it becomes a right or even moral obligation to increase transparency also against resistances. As secrecy is rendered suspicious, information is extracted when not voluntarily provided. This begins to undermine the conceptual distinction to surveillance. At the same time, this discourages participation of and engagement with the observed. They neither have a say in the nature and extent of their observation nor is the information employed to start a constructive dialogue. Instead, forced transparency emphasizes questioning, challenging, blaming and discrediting the observed. The potentials and constraints of EO satellites enable a technologized cycle of forced transparency in which there is no end to more and better non-governmental remote sensing. Because of the inherent shortcomings of satellite imagery, it will only result in incomplete transparency. As this is interpreted as a lack of information, the response is more information, i.e. more satellite imagery. However, this ignores that no matter the technological

improvements, transparency and security are never absolute: The pursuit of complete transparency is therefore as infinite as it is futile. The continued forcing of transparency by non-governmental remote sensing entails risks and implications beyond the operational level.

First, forced transparency enables a form of remote governance by non-governmental actors. Commercial satellite imagery increases the political reach even of small NGOs and think tanks to a global level. The one-sided extraction of information is reflected in corresponding governance relations. Forced transparency renders the observed silent and passive as they cannot compete with the hierarchy of evidence. The material evidence of security threats outweighs talking to the observed. As such, forced transparency discourages dialogue and engagement which, in turn, complicates addressing the root causes of insecurities. Instead, non-governmental remote sensing manages insecurities. Because regardless of the extent of transparency, the problem remains that political actors need to act on the information provided. Second, the public availability of security-relevant information complicates international diplomacy. It forces governments to offer explanations or rationalizations of their actions because it introduces domestic and global publics into the debates. Moreover, non-governmental remote sensing makes it more difficult for governments to make strategic use of information and to dictate messaging when deemed useful in international negotiations. Third, after a brief transition period, the observed have adopted strategies to respond to the constant observation. Even violent non-state actors use tactics to camouflage or conceal their activities. Moreover, the observers are at risk of being instrumentalized when the observed deliberately show real or fake signals of strength. Fourth, when non-governmental actors force transparency, they often become entangled with the security threats themselves. In any case, they add to the complexity of the security situation. Still, there are no coherent guidelines for non-governmental remote sensing. Instead, ethical decisions about what, when or how information is released are made individually on a case-by-case basis and adds to the uncertainty of security problems. Fifth, automated satellite imagery analysis promises to further force transparency. Geospatial big data analytics open up possibilities of predictive analytics and interventionist imaging. If realized, it would elevate the role of non-humans in remote governance and encourage premature intervention. Lastly, given the considerable financial and analytical resources necessary to realize the vision of predictive analytics, governments (re-)emerge as dominant actors of commercial remote sensing. This further qualifies narratives of power gains by non-governmental actors as a result of the commercialization of satellite imagery.

Taken together, the chapter examines the potential fallout from non-governmental remote sensing as a global security practice. As such, it does not question the benefits of transparency or public information on an operational level. Rather, it points towards the repercussions of forcing

transparency at scale. Non-governmental actors all but declare maximizing the virtue of transparency a moral obligation. Consequently, they violently extract information when it is not voluntarily provided blurring distinctions to surveillance. However, contrary to their conviction the benefits of transparency are unequally distributed and reinforce existing power relations. Surely, some situations call for the close monitoring and naming-and-shaming that is made possible by commercial satellite imagery. At the same time, alternative ways of non-governmental remote sensing that support political dialogue and engage the observed provide useful additions to address security threats more sustainably. Among other things, they will be discussed in the concluding chapter.

8 Conclusion

8.1. Introduction

The commercialization of satellite imagery provides non-governmental actors from NGOs to think tanks to universities access to a technology that was previously reserved for military and intelligence agencies. Over the past 20 years, satellite imagery has become a common sight in print, online and TV news reporting. Commercial imagery providers deliver almost daily imagery updates with resolutions of up to 31cm – the size of a laptop. This enables non-governmental actors to monitor various security threats including nuclear programs, weapons deployments, missile testing, forced displacement, mass graves, deforestation, illegal fishing and so forth. This development is often associated with what has been called a geospatial revolution that allegedly creates global transparency and promotes peace. Hitherto, research on this form of technologized security governance has focused on episodic representations of how non-governmental actors that make use of satellite imagery. Academics, policy and business experts from various backgrounds examine isolated cases or pilot projects of NGOs using satellite imagery based on anecdotal evidence, visual analyses or small interview samples. The variety of theoretical perspectives, purposes and idiosyncratic results has led to an incoherent research landscape that does not acknowledge each other's existence and presents contradictory findings.

In contrast, the thesis offers a comprehensive analysis of non-governmental remote sensing as a form of technologized security governance. By drawing on classic security governance literature as well as socio-material approaches to security (SMAS), a conceptual framework introduces the force of technology into the analysis instead of treating it as a neutral instrument or driver of security politics. Grounded theory methods guide the structured collection and analysis of data from various sources including 50 interviews to account for the socio-material interaction at play in security governance. The thesis takes into consideration the perspectives of satellite imagery analysts, human rights and environmental NGOs, security think tanks, humanitarian actors, government officials, satellite imagery providers and analytics companies. At the same time, it pays due attention to the potentials and constraints introduced by satellite technologies and the visual imagery. Building on the conceptual framework, the analysis of empirical data is guided by three central questions. First, how do human and technological factors interact in non-governmental remote sensing to credibly problematize and create security threats? Chapter 5 challenges the human control and language bias involved in the construction of security threats. Instead, it shows how security threats are co-produced by human and material factors. Among other things, satellite technology prescribes the problem space and co-determines which threats are addressed by non-governmental actors. Second, what types of non-governmental remote

sensing have emerged in terms of users, practices, goals and issue areas? Chapter 6 demonstrates that the non-governmental community has adopted commercial satellite imagery in various, uneven and fragmented ways. However, four different stabilized modes of non-governmental remote sensing emerge that are defined by their goals and the potentials of satellite imagery they actualize. Third, what kind of transparency is produced by non-governmental remote sensing and what are the security risks and implications? Chapter 7 defines the notion of forced transparency. Non-governmental actors keep calling for more satellite surveillance in the allegedly virtuous pursuit of creating public information about security threats. This forces transparency upon the – largely non-Western – observed and governed with a myriad of hidden risks and implications.

The next section recapitulates and summarizes each chapter's main points concerning the study of non-governmental remote sensing as a form of technologized security governance. Then, the chapter proceeds to particularly highlight the broader contributions in terms of the methodological approach to the study of technology in security research (section 8.3.) as well as how satellite technology co-produces security threats and surveillance practices, and mediates the effects of remote sensing (section 8.4.). Next, the conclusion considers the study's limitations and avenues for further research before it closes with reflections about the room for political resistance in technologized security governance.

8.2. Non-Governmental Remote Sensing as Technologized Security Governance

Analyzing non-governmental remote sensing as a form of technologized security governance, chapter 2 assesses the current state of research concerning theoretical approaches to the nexus of security governance and technology. Security governance offers alternatives to dominant IR theories in response to the deepening and widening of security concepts in the wake of the Cold War. In essence, it conceptually captures forms of security practices that are removed from the hierarchical authority of nation-states. It accounts for the proliferation of security actors and a growing number of new threats that lie beyond the capabilities and interests of individual governments. Technology, however, is not among those new actors but remains exogenous to politics and, therefore, political analysis. Rather, objects and technical devices are conceived as neutral instruments or drivers of the political. In order to conceptually grasp how technology influences security practices and decisions, chapter 2 turns to socio-material approaches to security (SMAS). This diverse research program brings together scholars from a variety of disciplines that are unified in their emphasis on the force of matter. SMAS introduce the "missing masses" (Latour 1992) to socio-political analysis. Despite their diversity, it is argued, they share three common theoretical concerns: (1) Material agency denotes the power of technology to impact security governance in terms of dispositions, potentialities, resistance or constraints. In

this sense, it is not equated with intentional human agency but technology matters in distributed assemblages of humans and things. (2) The focus on relations deconstructs pre-conceived social categories such as nation-states, international organizations or large technical systems. (3) These categories are empirically contingent upon relations between material artefacts, social constructs and human actors. Taken together, this culminates in an inductive, empiricist approach to trace these relations to examine the workings of security governance. The refusal of a conceptual framework and the focus on micropolitics lead to considerable interpretive flexibility. This makes it difficult to comprehend the at times peculiar theorizing and to sufficiently structure data collection and analysis.

Addressing these shortcomings, chapter 3 constructs a conceptual framework that, at once, acknowledges the role of technology in security governance and introduces guidelines for research practice. The purpose of the conceptual framework is to provide the analytical vocabulary for the empirical analysis, increase the accessibility for both SMAS and security governance scholars and, importantly, make explicit key theoretical assumptions that otherwise remain hidden. In doing so, the framework outlines three central concepts that are useful to think through the role of technology in security governance. In line with the understanding of security governance as an assemblage of humans and things, the chapter defines technology as a material object that imbues its various relations with potentials and constraints. These potentials are actualized or not but at least exist as virtual possibilities. As a central proposition, an analysis of technologized security governance zooms in on the problematization of security which captures the human-material co-production of security threats and scrutinizes the legitimacy of technologies to become central for addressing them. Moreover, given the latent volatility of security governance assemblages, the notion of stabilization turns to the actions and objects that lock in certain assemblages, practices and goals. Lastly, looking at the durable effects of technologized security governance completes the framework. Technology stabilizes security practices and repetitive patterns that reinforce security goals. In this way, these goals and norms are maximized up to a point where they can bring about unexpected consequences.

Limiting the framework to central concepts structures and guides the analysis while remaining responsive to the empirical material at hand. In order to take advantage of this interpretive openness, chapter 4 introduces constructivist grounded theory methods. They retain the sensibility to the force of technology but direct data collection and analysis. In this sense, the chapter usefully complements SMAS that frequently remain silent on their research practices. In grounded theory, data collection and analysis alternate as they are intertwined. Data collection is guided by theoretical interest and followed by immediate analysis. Initial findings inform further data collection until theoretical saturation is achieved. All in all, the thesis draws on 50 interviews

with informants including satellite imagery analysts, NGOs, think tanks, regulators and companies as well as supplementary documentation such as satellite imagery, policy decisions, NGO reports, satellite regulations etc. The conceptual framework provides sensitizing concepts that drive open coding in which blocks of content are formed into units of meaning. During the analysis, the researcher constantly writes memos and compares existing codes with each other. The continuous coding condenses the empirical material and increases theoretical abstraction but guarantees a close connection to the empirical data. In short, the researcher actively co-constructs data collection and analysis.

Chapter 5 employs this approach to investigate how non-governmental actors problematize security in interaction with EO satellites. For doing so, it analytically traces the socio-material interaction following the standard procedure of imagery acquisition, imagery interpretation and dissemination. The technology definition firmly integrates satellite imagery into the analysis and reveals how its potentials and constraints co-produce security threats. Despite claims to the contrary, commercial EO satellites do not offer a uniform, unbiased image of the globe. Most remote sensing applications are dependent on favorable light and cloud conditions and only record narrow strips of imagery. Consequently, commercial imagery providers diligently task their satellites to image particular areas of interest in accordance with customer demands. As governments and their defense and intelligence communities are responsible for the largest share of their profits they influence which areas are observed. This introduces a governmental bias into the imagery archives toward non-Western countries and national security hotspots. For financial reasons, non-governmental actors mostly use this archival imagery. In doing so, they are constrained to preselected security problematizations and carry further the national security bias of governments. Chapter 5 also distorts the myth that satellite imagery allows for unmistakably seeing security threats. Satellite imagery analysis is liable to technical and human errors. Most NGOs and think tanks did not have any experience with this technology to start with. As a result, they have developed customized, self-taught analytics for handling imagery analysis which carry the risk of producing flawed or overbearing results. Hiring former intelligence and military analysts, on the other hand, might lead to militarized forms of interpretation as they are not trained for the specific issue area of the NGO or think tank such as human rights, humanitarian or environmental concerns. Regardless of this, the section conceptualizes satellite imagery analysis as the translation of matter into security threats. Security threats are not immediately visible on a satellite image. Instead, they are reduced to material indicators or proxies that act as stand-ins for suspicious and dangerous actions: Vehicle activity suggests missile test preparations while disturbed earth indicates mass graves. The material fetish limits the problems that can be addressed, simplifies their representation and predefines what are considered appropriate responses. Finally, the chapter examines how security threats are rendered legitimate by way of

non-governmental remote sensing. The visual and material dimension of satellite imagery, at once, emotionalize and rationalize security threats. Despite the difficulties for laypeople to identify anything on satellite images, it gives rise to the impression that anyone can see for themselves. The materiality of the satellite technology as well as the security threats further imply a scientificity and objectivity that is difficult to shake. Moreover, satellite imagery analyses of non-state actors are increasingly integrated in official reports and public speeches of government agencies and international organizations. The endorsement of non-governmental remote sensing as a security practice by established institutions further imbues it with legitimacy and authority. Taken together, chapter 5 shows how the potentials and constraints of commercial satellite imagery co-produce security problematizations as credible and legitimate

Given the material affordances of satellite technology and the inexperience of non-governmental users, chapter 6 offers a classification of four different modes of remote sensing. Non-governmental remote sensing rests on a fragmented community of NGOs, think tanks and analysts. These actors have adopted satellite technology as a result of rather idiosyncratic and often personal interactions with a few champions of this technology. Consequently, instead of a uniform, routinized practice, non-governmental actors actualize very differing potentials of commercial satellite imagery. Some are interested in the visual product while others rather rely on the data potential of remote sensing. Relatedly, imagery is put to use for different goals that oscillate between providing public objective information and advocating for a particular cause. First, similar to Cold War intelligence practice, the public intelligence mode focuses on the visual analysis of individual satellite images to characterize and monitor security threats. Accordingly, the focus of application usually is on conventional security threats including nuclear weapons or other military programs as well as violent conflict. Diverging from governments, though, non-governmental users aim to introduce their findings into public security debates. In this understanding, the lack of objective information lies at the root of misconceived security policy and alarmist distractions which both are addressed by way of non-governmental remote sensing. Second, the mapping mode draws on the data potential of commercial remote sensing products to create overview maps for humanitarian and crisis responders' geographical areas. The geospatial, actionable information is usually intended for supporting decision-makers and planners on the ground. In this mode, the visual dimension of satellite imagery fades into the background. Instead, non-governmental users annotate large areas to show passable roads, destroyed buildings or the geospatial distribution of different kinds of infrastructure. Third, the visual advocacy mode employs satellite imagery to effect a change of policy and influence public opinion. For this purpose, the visual potential of remote sensing becomes important. Predominantly, NGOs and think tanks monitor human rights violations and security threats to build a political platform, raise awareness and hold people accountable. They become investigators of security threats and seek

to produce visual evidence. In this function, accuracy and transparency of analysis becomes important for the credibility of analysis. Fourth, the mass data mode relies on a large amount of satellite data to produce global scientific datasets mostly on environmental or conservation issues. To achieve advocacy and accountability goals, the data is often presented on interactive online platforms which users can freely navigate, select issues and determine areas of interest. This way, journalists and other NGOs can use the information in their own advocacy efforts. Given the technological complexity, the number of non-governmental actors is rather small in the mass data mode and confined to larger NGOs with sufficient financial means and know-how or university-based projects.

In sync with the conceptual framework, chapter 7 looks at the durable effects of non-governmental remote sensing. It builds on the finding that the great majority of non-governmental users of satellite imagery promote the importance of making security threats transparent for the global public. In this light, it extracts their understanding of transparency as the amount of publicly available information on a security threat; it becomes a quantitative measure. Moreover, transparency is conceived as a virtue. Across modes, non-governmental users hold the belief that transparency fosters peace and security. In this sense, non-governmental remote sensing not only implies a right but a moral obligation to produce more satellite imagery because it means more transparency. As no amount of satellite imagery leads to complete transparency, this fuels a technologized cycle that keeps maximizing the virtue of transparency. A lack of transparency is rendered problematic, suspicious and in opposition to general trends toward openness. If necessary, then, non-governmental users force transparency if it is not voluntarily created. Effectively, this blurs the lines between transparency and surveillance. It also makes clear that the maximization of satellite-based transparency does not benefit everyone in the same way and carries various implications for the observers and the observed. First, forced transparency enables a form of remote governance that silences the observed and discourages dialogue and engagement. Second, the public availability of security-relevant information risks complicating international diplomacy as it introduces a public audience to the security controversy. Third, the observed develop adaptation strategies in order to deceive or instrumentalize their observation. Fourth, in the absence of ethical guidelines non-governmental observers become part of the security dynamics on the ground and add complexity to the situation. Fifth, automated and predictive analytics might legitimate prejudgement and encourage premature intervention. Lastly, the expansion of data sources and sophisticated analytics reintroduces the government as a dominant player in commercial remote sensing.

Taken together, the thesis offers two main take-aways: On a conceptual note, it introduces the strengths of grounded theory to organize and systematize the study of technology in security

governance. Based on this, it then questions largely positive narratives of the commercialization of satellite imagery and problematizes the power of technology to legitimate security practices. The following two sections each discuss one aspect in more detail.

8.3. Grounded Theory and the Study of Technology in Security Governance

SMAS are suspicious of preconceived theoretical notions and instead emphasize a necessity for close empirical work. However, they remain surprisingly silent on specific modes of data collection and analysis. The thesis implements its conceptual framework by drawing on grounded theory methods to systematically analyze the role of technology in security governance. It argues that grounded theory – a well-established approach in the social sciences and humanities at large – is helpful to pragmatically fill this gap.

It is a welcome contribution that SMAS seek to acknowledge and analyze the power of technology and objects in the workings of global security. For doing so, they propose to turn to the micro level. This focus goes hand in hand with an empiricist project to trace the specific relations of actors and practices and their repercussions on higher levels. Referring to the sociological tradition encapsulated by many SMAS, Diana Coole (2013: 465) notes:

> *"It is striking just how often sociologists like Bourdieu, Latour and Foucault emphasise these terms: concrete, real, empirical, material, detailed, meticulous. This is where bodies' material needs, their consumer habits, their daily routines, come under scrutiny in an existential and bio-physical way. The challenge is therefore to attend to the myriad and mundane dust of ordinary lives while recognising the tentacles of power that pervade them from higher levels."*

In order to address this challenge, security and IR scholars regularly turn to concepts from Science and Technology Studies, the Philosophy of Technology or related disciplines. Imported concepts are quickly framed as "research tools" (Bueger and Stockbruegger 2018: 49) that support a "theoretically informed empiricism" (Barry 2013b: 419). However, instead of leading to detailed descriptions of how researchers collect or analyze empirical data, it too often results in idiosyncratic and abstract presentations of research practice that are difficult to comprehend or link up to. In its worst forms, these approaches demand what Kieran Healy (Healy 2017: 121) calls "connoisseurs" who are characterized by their belief in a "distinctive (often metaphorically expressed and at times seemingly ineffable) ability to grasp and express the richness, texture, and flow of social reality itself." Taken together, the general inadequacy or silence of SMAS on methods of data collection and analysis unnecessarily misses an opportunity to become compatible with more classic security governance research and more effectively promote the relevance of the role of technology in global security.

In an attempt to address this, the thesis makes two decisions that seem rather unconventional for socio-material approaches but quite common and fundamental for mainstream Security Studies and IR. First, it develops a conceptual framework to guide the empirical analysis. Second, grounded theory methods are introduced to organize and systematize the data collection and analysis. In doing so, the thesis attempts a balancing act to embrace the empiricism of SMAS but to conceptually channel it in accordance with the research questions. This leads to several advantages. The variety and complexity of SMAS encourage idiosyncratic theorizing and empirical findings that, in turn, make it difficult to connect to other security research. In fact,

> *"the language employed can be opaque and lead up to rather quirky concepts and terms. The open-ended character and multi-vocality of the narratives developed and the experimentation with different literary styles tends to simultaneously fascinate and alienate many readers. Indeed, it makes ANT studies at times very difficult to access"* (Bueger and Gadinger 2014: 50).

Conceptual frameworks increase coherence and make the research more accessible for fellow security scholars by clearly stating the scope of the study and defining the conceptual vocabulary. In doing so, they also take seriously a problem of research practice: The process of analysis requires decisions which empirical observations to include or exclude and how to assess their relevance (Fine 2005: 95-96; Rekret 2016). While a conceptual framework does not solve or remove these problems, it makes the decisions explicit and at best provides an acceptable justification. In any case, SMAS are not too far removed from established constructivist security governance research when it comes to their empiricist approach and their interest in the reproduction of power (Coole 2013: 456). Consequently, both research programs mutually benefit from each other by including both a focus on the workings of technology as well as a more systematic research practice. With that said, it should be restated that a conceptual framework should not be understood as a bureaucratic template that relentlessly needs to find a concrete category for every piece of data. Instead, it provides guidelines for data collection and analysis while accounting for the messiness and complexity of empirical data that still requires context-sensitive interpretation by the researcher.

More specifically, then, the thesis collects and analyzes data by turning to methods of grounded theory. Surprisingly, SMAS have not yet explicitly drawn on grounded theory methods but either chose to re-invent the wheel, casually mention the use of interview or fieldwork data, or hold back on providing details on how the empirical work actually takes place. While the conceptual framework provides overall guidance on data collection and analysis, grounded theory is a pragmatic research approach that looks for typical actions which lead to typical consequences.

It was already formulated in the 1960s as a response to criticism that questioned the legitimacy and validity of qualitative approaches in the social sciences (Glaser and Strauss 1967). Ever since, its theoretical assumptions and methods have been revised and updated (Charmaz 2006; Tucker 2016). In a nutshell, grounded theory involves the constant alternation of data collection and analysis. This means whenever data is collected in the form of field observations, interviews, photographs, legal text or press statements, the researcher immediately starts with the analysis. The provisional findings then guide the decision which data is necessary to verify, contradict or elaborate on the previous results. The conceptual framework helps keeping the analysis within the boundaries of the overall research questions and formalizes preexisting knowledge, interests and theoretical notions (Charmaz 2006; Kelle 2005; Strauss and Corbin 1998). In this sense, the call of so many SMAS to follow an empiricist agenda are already included in a decades-old, established collection of methods that similarly embrace data-driven theorizing within the limits of a formulated research interest (Charmaz 2006; Hülst 2010). Importantly, grounded theory is agnostic about the form, size and content of data so that it readily lends itself for the exploration of technology in global politics. For grounded theorists "all is data" – although, of course, it varies in terms of access, quality and relevance (Glaser 2001; see also Hülst 2010: 283; Charmaz 2006: 16). This opens up creative ways for researchers to investigate the power of matter through interviews, photographs, drawings, observations, regulations, experiments or other sources. Taken together, the conceptual framework and grounded theory methods put a check on potential excesses of any "connoisseur" (Healy 2017) because the researcher is forced to stay close to the empirical data even in his or her theorizing.

8.4. Forced Transparency: The Limits of Non-Governmental Remote Sensing

Building on the research approach outlined above, the thesis distorts prevalent narratives of the commercialization of satellite imagery and the associated practice of non-governmental remote sensing. Most importantly, satellite technology is identified as an influential element through its power to incentivize, constrain and mediate action which is neglected in previous studies. The analysis shows how socio-material potentials and constraints co-produce the problematization of security, stabilize the assemblage of actors and practices and force transparency.

The recent growth and progress of satellite technology allegedly promise open, easy and inexpensive access to aerial imagery with a lasting impact on a wide range of policy areas. This development – in concert with accompanying trends such as an ongoing digitalization – is in some places described as the "geospatial revolution" (Masback 2015; O'Connell 2017). Consequently, the commercialization of satellite imagery is associated with a democratized access to data or a power shift from government to non-governmental actors (cf. Olbrich 2019c). However, the idea is misleading because it problematically equates the commercial availability with global and equal

access. On top, it presumes a uniform process of how satellite imagery is utilized by a variety of actors in different areas of applications. In doing so, it obscures remaining barriers on the level of practice in terms of awareness, access, analytics as well as operational sustainability and integration. Contrary to the revolution terminology, access is anything but global and democratized. High-resolution and radar satellite imagery remain too expensive and, therefore, virtually out of reach for many non-governmental organizations and think tanks – especially if projects require continuous access. The thesis points towards the remaining influence of governments over commercial Earth observation. In the case of DigitalGlobe, the largest provider of high-resolution imagery, the U.S. government consistently accounts for more than 60% of its revenue. This makes it the by-far single largest customer. As such, it noticeably drives which areas of the globe are being imaged. Accordingly, the satellite imagery archives of commercial providers are biased towards government-selected national security hotspots. Thereby, they co-define the scope of security threats non-governmental actors can address (cf. Olbrich 2019b). The remaining high prices and government involvement effectively constrain and channel non-governmental access to satellite imagery. The findings of this thesis render buzzwords such as a democratization of satellite imagery or geospatial revolution euphemisms that rather reflect wishful thinking and economic aspirations than daily practice (cf. Olbrich 2019c). On top of that, the use of satellite imagery is an active, complex and political process. Analysts that employ satellite imagery for non-proliferation and disarmament hold very different requirements than organizations that monitor the globe for deforestation or illicit fishing. Differences permeate various categories from the kind and amount of imagery required to the specific goals pursued to the analytical know-how to the way of integration and dissemination of geospatial information. As a consequence, the thesis has identified four distinct modes of non-governmental remote sensing which are testament to the variety and differences of actors' responses to the technological potentials and constraints of commercial satellite imagery.

Users and academics alike portray non-governmental remote sensing as an objective and dispassionate endeavor. This derives from the belief that technology in general and satellite imagery in particular are perceived as neutral instruments obedient to human intentions. In this understanding, security threats and their observation are independent and distinct from one another: The security threat is a fact and satellite imagery is conclusive evidence about its existence. The empirical material yields a number of quotations that express this conviction in a variety of ways such as "I don't have to believe your word if you can prove it to me with an image" (Informant #42). In contrast to this understanding, the thesis holds that security threats are socio-material co-productions. Satellite technology plays an active role in what and how security is problematized. This argument is substantiated along the process of non-governmental remote sensing including imagery acquisition, analysis and dissemination. The orbital, natural and

technological constraints of high-resolution satellites already prevent constant imaging. Earth observation is not comparable to global CCTV. This means, users of commercial satellite imagery cannot order imagery of any place on Earth at any point in time. They are dependent on the orbital conditions of the satellite, its spectral bands, swath width, resolution, imaging capacity as well as the weather and light conditions. In this sense, satellite technologies co-produce what security threats are observable to begin with favoring large natural changes and built infrastructure. This puts immediate constraints on the possibilities of what can be monitored via satellite-based remote sensing. In any case, early expectations to use commercial satellite imagery for the verification and monitoring of international treaties on a broad scale gave way to more narrow and pragmatic ways of application (Olbrich 2019c). Relatedly, materiality becomes a prerequisite for security threats. As a result, vehicles, smoke, disturbed earth or tree cover loss become indicators of security-relevant developments. Satellite imagery is blind to motives and intentions. In this line of thinking, vehicle activity or melted snow on a roof at the Nyŏngbyŏn nuclear complex are used as proxies for possible intensifications of North Korea's nuclear program. In short, matter is translated into security threats. Further, the material and visual dimensions of non-governmental remote sensing render it credible and legitimate. All the while, contestations are ineffective as long they do not follow the same hierarchy of material evidence (Olbrich 2019a).

Across applications of non-governmental remote sensing, users share a sense of moral right and obligation to increase global transparency. Non-governmental remote sensing is rendered a virtuous practice that promotes peace and security. This becomes problematic when transparency is understood as the quantitative amount of publicly available information. All the while, the aspects of how the information is produced, processed and used are underrated or neglected. Similar to leaks of classified or proprietary data that are often unstructured and messy, the mere availability of more information is considered to increase transparency. While the socio-material limits of satellite imagery make complete transparency impossible, this does not stop the mission to keep pushing for, keep forcing more transparency. If information is not voluntarily provided, commercial satellite imagery has become a tool to forcefully implement it also against anyone's will – allegedly, for the benefit of all. This state of forced transparency is seemingly rendered objective, beneficial and equal by the use of technology. The technologized nature of non-governmental remote sensing legitimates satellite-based surveillance. However, this view neglects that it takes place in and reproduces unequal power structures. There are different stakes involved for rich and poor, Western and non-Western, U.S.-aligned and non-aligned countries. The thesis has pointed to a number of tangible complications that arise from the growing use of satellite imagery. Among other things, the allegedly objective position of knowledge production silences the observed because satellite imagery "shows" the security threat. This assessment does not eradicate the benefits of satellite-based transparency of increasing public information about

hard-to-access security, human rights, humanitarian and environmental situations. Yet, it demonstrates that the technologization of security governance does not isolate it from politics. Non-governmental remote sensing is political.

8.5. Limitations of Studying Dynamic Socio-Material Practices

Non-governmental remote sensing is an emergent security practice that is tightly linked to the nascent technological development and ongoing commercialization of satellite imagery. NGOs, think tanks and universities based in the U.S. were among the first to adopt and integrate the technology into its operations. As the data collection focuses on first-hand users of satellite imagery, it is biased towards the practices, norms and political conditions of U.S.-based organizations. However, these actors were not only among the first who adopted the technology but also significantly influenced practices across other national and international contexts. As a case in point, data from non-U.S. contexts equally supports arguments about the remaining power of governments in regulating, financing and promoting their respective satellite imagery markets. They are an important determinant for how local users are able to take up and make use of commercial satellite imagery. Having said that, the concrete configuration of relations among actors might translate into different practices: NGOs and think tanks in other settings from India, Israel or South Korea might face different potentials and constraints depending on their relations with relevant government and business stakeholders. Arguably, the governmental origins of satellite imagery extend into its commercialization and in the process elevate the importance of the national context so that the U.S. focus of the thesis comes with limitations in terms of generalizability.

Relatedly, commercial and open-source Earth observation is a dynamic field. The number of available commercial satellite imagery providers across the globe has proliferated during the study period, new sensors and analytical techniques were introduced and non-governmental imagery access varied as a result of government support, personal relations and new marketing strategies. Cognizant of the dynamism of the study object, the thesis chose a methodological approach that allows for continuous data collection. As a result, the data was not collected in a single large effort at one point in time but included interview series from 2014 to 2018. The dynamism became clearly apparent in the empirical data because of the inherent interdependence of human and technological factors in non-governmental remote sensing. In this context, the thesis concentrated on common practices, constraints and potentials that remained constant during the study period. Moreover, it has been demonstrated that assertions of technological breakthroughs and revolutionary changes more often than not remain behind expectations (Olbrich 2019c). For instance, proponents of the idea of democratized access to satellite data might argue that existing constraints will disappear as a result of global market competition.

Indeed, the costs to develop and launch satellites of any kind have fallen significantly over the past years due to growing supply in the launch market and the miniaturization of Earth observation satellites. However, the thesis has also shown that lower barriers to entry and technological innovation have not yet resulted in a sustainable commercial market for satellite imagery independent from governments. Still, research on emerging and dynamic political practices such as non-governmental remote sensing faces the risk of producing results with a limited half-life so that the central findings require constant review, validation and, if necessary, adjustment.

Lastly, the conceptual framework pursues an eclectic strategy that combines insights from security governance and SMAS. This allows for a structured analysis of the role of technology in security practices. Arguably, however, the strengths of the approach are also its weaknesses. Given its compromise positions, the conceptual approach remains vulnerable to some of the critique leveled against SMAS and classic security governance alike. Although the framework does not U-turn into hypothesis testing, indicator development and statistical analysis, it pre-structures the empirical analysis by way of the central concepts of problematization, stabilization and durable effects. At the same time, though, it remains an interpretive framework and stays attuned to the empirical material at hand, which imposes great responsibility on careful data collection and analysis by the researcher. Purists of either one research program might focus on the shortcomings that such a compromise position necessarily entails. However, it should rather be understood as an invitation to modify and fine-tune the approach in correspondence with the respective research interest and questions.

8.6. Recommendations for Further Research

The limitations of the study described above help devise an agenda for further research. The ongoing commercialization of satellite imagery is global in scale. Comparative approaches that investigate non-governmental remote sensing communities in non-U.S. countries including Europe would lend themselves to compare and complement major findings of the thesis. In doing so, it could also address remaining puzzles with respect to the geographic distribution of non-governmental remote sensing. The mentioned U.S. bias in the empirical data is not a result of a deliberate or theory-driven decision but rather representative of current practices during the time of data collection. Even within international NGOs it is often the U.S. affiliate that drives the integration of satellite imagery. Investigating the pioneering role of the U.S.-based NGO sector and the hesitance of its European counterparts promises interesting results that go beyond the use of Earth observation data but shed light on the capacity of and attitudes towards the use of technologies in the non-governmental sector as a whole.

One potential reason for the skepticism of some non-governmental actors towards remote sensing might lie in its proximity to the military and intelligence apparatus of governments – either

directly or through imagery providers that maintain close relationships. In this context, the thesis has pointed to risks associated with the growing integration of commercial satellite imagery with other geospatial big data and automated analytics. While non-governmental actors express great interest in experimenting with these new possibilities, governments are currently better suited to harness geospatial big data analytics. This is not only because they traditionally hold the analytical expertise to work with remote sensing data. But governments also have access to various security-relevant data sources to integrate with geospatial data. Further investigating the role of the state also helps to re-examine the prevalent assessment that the commercialization of satellite imagery is connected to a power shift from government to non-governmental actors that has been questioned in this thesis. Moreover, this line of research could also tie in with existing studies on the governmental uses of big data (e.g. Amoore and Raley 2017; Baele, Balzacq, and Bourbeau 2017; Leese 2014) as well as the political ramifications of predictive analytics and intervention (e.g. Aradau and Blanke 2017; Amoore 2009; Olbrich and Witjes 2016; Zwitter 2015). Because regardless of who pushes for the expansion of geospatial big data analytics, the growing complexity adds to the overall risks of consequential misinterpretation because "failures are inevitable in complex, tightly coupled systems and the sheer complexity of the system inhibits predicting when and how failures are likely to occur" (Scharre 2018: 147).

Finally, the thesis is a contribution to a growing interest in the politics of space and space applications. Both the expansion of government programs as well as the growing commercial interest have tightly connected space applications to everyday life including global politics. Communication satellites are a cornerstone of global military and civil information and communication systems, Earth observation satellites keep track of climate change, humanitarian disaster and security developments and the different GPS constellations have become a taken-for-granted feature for mobile applications, global transport and public services infrastructure. Hitherto, much of the research in this domain has been driven by industrial and organizational professionals that work at major space companies or governmental organizations (Schrögl et al. 2015; Sadeh 2015). While this leads to interesting findings, they often remain focused on immediate policy problems on the level of governments or international organizations in lieu of more theoretical considerations. Increasingly, however, academics from IR and Security Studies discover space as an important study area (Bowen 2018; Peoples 2018; Olbrich and Shim 2019; Sheehan 2007; Stroikos 2016). The integration of space applications into policies pursuant of the UN Sustainable Development Goals, the dangers of space debris, the weaponization of space or discussions about the introduction of a Space Force as a separate branch of the U.S. military concern questions and problems that are at the heart of IR scholarship. Future research should deploy the broad collection of theoretical tools to space politics to inform ongoing political

controversy and, if necessary, revise conceptual approaches to accommodate the particular characteristics of extra-terrestrial politics.

8.7. Conclusion

The politics of non-governmental remote sensing are co-produced by both human and technological factors. The thesis qualifies claims that the commercialization of satellite imagery unambiguously increases global transparency and promotes peace and security. Such positive assessments as well as related hopes and expectations are usually based on an understanding of technology as neutral and controllable. Accordingly, while it can be used for nefarious purposes, most (non-)governmental actors are provided an essential tool to eliminate uncertainty and secrecy in global politics which are believed to complicate efforts of global cooperation. However, the socio-technical analysis of how satellite imagery is integrated in the daily operations of NGOs and think tanks reveals the force of technology. The organizations do not control or use but interact with remote sensing satellites. They are bound by the potentials and constraints of satellites which effectively co-determine which security threats they target, how they operate and what kind of transparency is produced.

Surely, non-governmental remote sensing can reduce uncertainty about matters of global security in that it produces public information about threats to the environment and human security. However, the thesis has also shown that users of satellite imagery equate the availability of information with transparency without acknowledging the conditions of its acquisition, interpretation and impact. Consequently, it becomes a virtuous mission for them to expand non-governmental remote sensing. Transparency is effectively technologized as satellite imagery becomes better and more accessible. In the end, information is extracted if it is not voluntarily provided so that non-governmental remote sensing forces transparency for the greater good. This generally ignores power differentials between the observers and the observed and discourages political dialogue and engagement between them. In doing so, the dividing line between forced transparency and surveillance becomes ever more blurred. Ultimately, this challenges beliefs that satellite-based transparency and non-governmental remote sensing in its current form per se promote peace and security.

While this is a sobering assessment, forced transparency is no foregone conclusion. Conceptually acknowledging the power of technology does not, in turn, render human actors powerless. The conceptual framework endorses the interplay of material and human agency. In doing so, it usefully unmasks the putative self-evidence of security threats but reveals their socio-material co-production. This constitutes an open and accessible moment for political intervention. Self-reflective human agents can resist technological affordances and formulate alternatives with regard to what constitutes a security threat and how to respond to it. In support of such efforts,

the framework urges researchers to acknowledge the materiality of technology and its force to co-determine security threats, stabilize security practices and legitimate the maximization of alleged virtues. In doing so, researchers can reanimate the controversies that precede the technologization of security governance and re-politicize security practices in order to shun demands of de-technologizing security.

References

AAAS [American Association for the Advancement of Science]. 2018. "High-Resolution Satellite Imagery Ordering and Analysis Handbook." *Scientific Responsibility, Human Rights & Law Program*. Accessed May 22. https://www.aaas.org/resources/high-resolution-satellite-imagery-ordering-and-analysis-handbook.

———. 2006. "Lebanon: Destruction in Civilian Areas Case Study Report."

———. 2014. "Human Rights Applications of Remote Sensing: Case Studies from the Geospatial Technologies and Human Rights Project."

———. 2015. "Monitoring Border Conflicts with Satellite Imagery: A Handbook for Practitioners." https://www.aaas.org/report/monitoring-border-conflicts-satellite-imagery-handbook-practitioners.

———. 2016. "Assessing the Status of Medical Facilities in Syria: Al-Quds."

Aas, Katja Franko. 2012. "(In)Security-at-a-Distance: Rescaling Justice, Risk and Warfare in a Transnational Age." *Global Crime* 13 (4): 235–53.

Abrahamsen, Rita, and Michael C. Williams. 2011. *Security beyond the State: Private Security in International Politics*. Cambridge: Cambridge University Press.

Achkar, Ziad Al, Isaac L. Baker, and Nathaniel A. Raymond. 2016. "Imagery Interpretation Guide: Assessing Wind Disaster Damage to Structures." *Harvard Humanitarian Initiative*. Cambridge.

Acuto, Michele, and Simon Curtis. 2014. "Assemblage Thinking and International Relations." In *Reassembling International Theory: Assemblage Thinking and International Relations*, edited by Michele Acuto and Simon Curtis, 1–15. Basingstoke: Palgrave.

Aday, Sean, and Steven Livingston. 2009. "NGOs as Intelligence Agencies: The Empowerment of Transnational Advocacy Networks and the Media by Commercial Remote Sensing in the Case of the Iranian Nuclear Program." *Geoforum* 40 (4): 514–22.

Adey, Peter, and Ben Anderson. 2012. "Anticipating Emergencies: Technologies of Preparedness and the Matter of Security." *Security Dialogue* 43 (2): 99–117.

Adler, Emanuel, and Steven Bernstein. 2005. "Knowledge in Power: The Epistemic Construction of Global Governance." In *Power in Global Governance*, edited by Michael Barnett and Raymond Duvall, 294–318. Cambridge: Cambridge University Press.

Adler, Emanuel, and Vincent Pouliot. 2011. "International Practices: Introduction and Framework." In *International Practices*, edited by Emanuel Adler and Vincent Pouliot, 3–35. Cambridge: Cambridge University Press.

Allan, Bentley B. 2017. "Producing the Climate: States, Scientists, and the Constitution of Global Governance Objects." *International Organization* 71 (1): 131–62.

Allenby, Braden R. 2011. "Governance and Technology Systems: The Challenge of Emerging Technologies." In *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem*, edited by Gary E. Marchant, Braden R. Allenby, and Joseph R. Herkert, 3–18. Heidelberg: Springer.

Allison, Graham T. 1971. *Essence of Decision: Explaining the Cuban Missile Crisis*. Boston: Little, Brown and Company.

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

Amnesty International. 2018. “‘We Will Destory Everything’ - Military Responsibility for Crimes Against Humanity in Rakhine State, Myanmar.”

Amoore, Louise. 2009. “Algorithmic War: Everyday Geographies of the War on Terror.” *Antipode* 41 (1): 49–69.

Amoore, Louise, and Rita Raley. 2017. “Securing with Algorithms: Knowledge, Decision, Sovereignty.” *Security Dialogue* 48 (1): 3–10.

AMTI [Asia Maritime Transparency Initiative]. 2017. “Update: China’s Continuing Reclamation In the Paraclels.” *Center for Strategic and International Studies*. Accessed August 23. https://amti.csis.org/paracels-beijings-other-buildup/.

———. 2018. “Occupation and Island Building.” Accessed August 23. https://amti.csis.org/island-tracker/.

Andersson, Ruben, and Florian Weigand. 2015. “Intervention at Risk: The Vicious Cycle of Distance and Danger in Mali and Afghanistan.” *Journal of Intervention and Statebuilding* 9 (4). Taylor & Francis: 519–41.

Andonova, Liliana B., and Gilles Carbonnier. 2014. “Business–Humanitarian Partnerships: Processes of Normative Legitimation.” *Globalizations* 11 (3): 349–67.

Angelino, C.V., M. Focareta, S. Parrilli, L. Cicala, G. Piacquadio, G. Meoli, and M. De Mizio. 2018. “A Case Study on the Detection of Illegal Dumps with GIS and Remote Sensing Images.” *Proceedings of SPIE* 10790. 10.1117/12.2325557.

Aradau, Claudia. 2010. “Security That Matters: Critical Infrastructure and Objects of Protection.” *Security Dialogue* 41 (5): 491–514.

Aradau, Claudia, and Tobias Blanke. 2017. “Politics of Prediction: Security and the Time/Space of Governmentality in the Age of Big Data.” *European Journal of Social Theory* 20 (3): 373–91.

Avant, Deborah D. 2005. *The Market for Force: The Consequences of Privatizing Security*. Cambridge: Cambridge University Press.

———. 2016. “Pragmatic Networks and Transnational Governance of Private Military and Security Services.” *International Studies Quarterly* 60 (2): 330–42.

Avant, Deborah D., Martha Finnemore, and Susan K. Sell. 2010a. “Conclusion: Authority, Legitimacy, and Accountability in Global Politics.” In *Who Governs the Globe?*, edited by Deborah D. Avant, Martha Finnemore, and Susan K. Sell, 356–70. Cambridge: Cambridge University Press.

———. 2010b. “Who Governs the Globe?” In *Who Governs the Globe?*, edited by Deborah D. Avant, Martha Finnemore, and Susan K. Sell, 1–31. Cambridge: Cambridge University Press.

Avant, Deborah D., and Virginia Haufler. 2012. “Transnational Organisations and Security.” *Global Crime* 13 (4): 254–75.

Avant, Deborah D., and Oliver Westerwinter. 2016. “Introduction: Networks and Transnational Security Governance.” In *The New Power Politics: Networks and Transitional Security Governance*, edited by Deborah Avant and Oliver Westerwinter, 1–18. Oxford: Oxford University Press.

Bäckstrand, Karin, and Mikael Kylsäter. 2014. "Old Wine in New Bottles? The Legitimation and Delegitimation of UN Public–Private Partnerships for Sustainable Development from the Johannesburg Summit to the Rio+20 Summit." *Globalizations* 11 (3): 331–47.

Baele, Stephane J., Thierry Balzacq, and Philippe Bourbeau. 2017. "Numbers in Global Security Governance." *European Journal of International Security* 3 (1): 22–44.

Baker, John C. 2001. "New Users and Established Experts: Bridging the Knowledge Gap in Interpreting Commercial Satellite Imagery." In *Commercial Observation Satellites: At the Leading Edge of Global Transparency*, edited by John C. Baker, Kevin M. O'Connell, and Ray A. Williamson, 533–57. Arlington: RAND.

Baker, John C., Kevin M. O'Connell, and John Robertson. 2003. "Commercial Observation Satellites: Dual-Use Technology in an Age of Global Transparency." *Georgetown Journal of International Affairs* 4 (2): 127–30.

Baker, John C., and Ray A. Williamson. 2000. "The Implications of Emerging Satellite Information Technologies for Global Transparency and International Security." In *Power and Conflict in the Age of Transparency*, 221–55. New York: Palgrave Macmillan.

———. 2006. "Satellite Imagery Activism: Sharpening the Focus on Tropical Deforestation." *Singapore Journal of Tropical Geography* 27 (1): 4–14.

Baker, John C., Ray A. Williamson, and Kevin M. O'Connell. 2001. "Introduction." In *Commercial Observation Satellites: At the Leading Edge of Global Transparency*, edited by John C. Baker, Ray A. Williamson, and Kevin M. O'Connell, 1–11. Arlington: RAND.

Baldwin, David A. 1997. "The Concept of Security." *Review of International Studies* 23 (1–2): 5–26.

Barad, Karen. 2003. "Posthumanist Performativity: Toward an Understanding of How Matter Comes to Matter." *Signs: Journal of Women in Culture and Society* 28 (3): 801–31.

———. 2007. *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*. Durham & London: Duke University Press.

Barnett, Michael. 2016. "Accountability and Global Governance: The View from Paternalism." *Regulation and Governance* 10 (2): 134–48.

Barnett, Michael, and Raymond Duvall. 2005. "Power in Global Governance." In *Power in Global Governance*, edited by Michael Barnett and Raymond Duvall, 1–32. Cambridge: Cambridge University Press.

Barnett, Michael, and Martha Finnemore. 2004. *Rules for the World: International Organizations in Global Politics*. Ithaca: Cornell University Press.

Baron, Luis Fernando, and Ricardo Gomez. 2016. "The Associations between Technologies and Societies: The Utility of Actor-Network Theory." *Science Technology & Society* 21 (2): 129–48.

Barry, Andrew. 2001. *Political Machines: Governing a Technological Society*. London: Athlone Press.

———. 2013a. *Material Politics: Disputes along the Pipeline*. Oxford: Wiley-Blackwell.

———. 2013b. "The Translation Zone: Between Actor-Network Theory and International Relations." *Millennium - Journal of International Studies* 41 (3): 413–29.

BBC. 2014. "Battle for Kobane: Before and after Images." Accessed December 13.

https://www.bbc.com/news/world-middle-east-29667113.

Beck, Ulrich. 1986. *Risikogesellschaft: Auf Dem Weg in Eine Andere Moderne*. Frankfurt: Suhrkamp.

Bedi, Rahul. 2008. "Mumbai Attacks: Indian Suit against Google Earth over Image Use by Terrorists." *The Telegraph*.

Bellanova, Rocco, and Denis Duez. 2012. "A Different View on the 'making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage." *European Foreign Affairs Review* 17 (2012): 109–24. http://www.kluwerlawonline.com/abstract.php?area=Journals&id=EERR2012017.

Bennett, Jane. 2005. "The Agency of Assemblages and the North American Blackout." *Public Culture* 17 (3): 445–66.

———. 2010. *Vibrant Matter: A Political Ecology of Things*. Durham & London: Duke University Press.

Bermudez, Joseph S., Andy Dinville, and Mike Eley. 2016. "North Korea: Camp No. 25 - Update 2." Accessed November 28. https://www.hrnk.org/uploads/pdfs/ASA_HRNK_Camp25_Update2.pdf.

Bermudez, Joseph S., Frank Pabian, and Jack Liu. 2018. "North Korea Likely Preparing for New Rocket Engine Test at Sohae." *38 North*. Accessed May 23. https://www.38north.org/2018/01/sohae010418/.

Berndtsson, Joakim, and Maria Stern. 2011. "Private Security and the Public-Private Divide: Contested Lines of Distinction and Modes of Governance in the Stockholm-Arlanda Security Assemblage." *International Political Sociology* 5 (4): 408–25.

Berterö, Carina. 2012. "Grounded Theory Methodology - Has It Become a Movement?" *International Journal of Qualitative Studies on Health and Well-Being* 7: 1–3.

Bevir, Mark, and Ian Hall. 2014. "The Rise of Security Governance." In *Interpreting Global Security*, edited by Mark Bevir, Oliver Daddow, and Ian Hall, 17–34. London: Routledge.

Bexell, Magdalena. 2014. "Global Governance, Legitimacy and (De)Legitimation." *Globalizations* 11 (3): 289–99.

Beyond Parallel. 2016. "Decrease in Trade After Nuclear Test." *Center for Strategic and International Studies*. Accessed May 23. https://beyondparallel.csis.org/decrease-in-trade-after-nuclear-test/.

Bijker, Wiebe E. 2010. "How Is Technology Made?--That Is the Question!" *Cambridge Journal of Economics* 34 (1): 63–76.

Bimber, Bruce. 1990. "Three Faces of Technological Determinism." In *Does Technology Drive History? The Dilemma of Technological Determinism*, edited by Merritt Roe Smith and Leo Marx, 79–100. Cambridge: MIT Press.

Birchall, Clare. 2012. "Introduction to 'Secrecy and Transparency': The Politics of Opacity and Openness." *Theory, Culture & Society* 28 (7–8): 7–25.

Bleiker, Roland. 2015. "Pluralist Methods for Visual Global Politics." *Millennium - Journal of International Studies* 43 (3): 872–90.

Blumer, Herbert. 1969. *Symbolic Interactionism: Perspective and Method*. Englewood Cliffs: Prentice Hall.

Borowitz, Mariel. 2017. *Open Space: The Global Effort for Open Access to Environmental Satellite Data*. Cambridge, MA & London: MIT Press.

Börzel, Tanja. 2010. "European Governance: Negotiation and Competition in the Shadow of Hierarchy." *Journal of Common Market Studies* 48 (2): 191–219.

Börzel, Tanja, Jana Hönke, and Christian R. Thauer. 2012. "Does It Really Take the State? Corporate Responsibility, Multinational Corporations, and Nation States." *Business and Politics* 14 (3): 1–34.

Bourdieu, Pierre. 1988. "Vive La Crise!: For Heterodoxy in Social Science." *Theory and Society* 17 (5): 773–87.

Bourne, Mike. 2012. "Guns Don't Kill People, Cyborgs Do: A Latourian Provocation for Transformatory Arms Control and Disarmament." *Global Change, Peace & Security* 24 (1): 141–63.

———. 2016. "Invention and Uninvention in Nuclear Weapons Politics." *Critical Studies on Security* 4 (1): 6–23.

Bousquet, Antoine. 2014. "Welcome to the Machine: Rethinking Technology through Assemblage Theory." In *Reassembling International Theory: Assemblage Thinking and International Relations*, edited by Michele Acuto and Simon Curtis, 91–97. Basingstoke: Palgrave.

———. 2017. "Lethal Visions: The Eye as Function of the Weapon." *Critical Studies on Security* Forthcomin.

Bowen, Bleddyn E. 2018. "British Strategy and Outer Space: A Missing Link?" *The British Journal of Politics and International Relations* 20 (2): 323–340.

Brandenburg, Natalie C. 2017. "EU Mediation as an Assemblage of Practices: Introducing a New Approach to the Study of EU Conflict Resolution." *Journal of Common Market Studies*, no. OnlineFirst: 1–16.

Branovic, Zeljko, and Sven Chojnacki. 2011. "The Logic of Security Markets: Security Governance in Failed States." *Security Dialogue* 42 (6): 553–69.

Breu, Christopher. 2016. "Why Materialisms Matter." *Symploke* 24 (1–2): 9–26.

Browning, Christopher S., and Matt McDonald. 2011. "The Future of Critical Security Studies: Ethics and the Politics of Security." *European Journal of International Relations* 19 (2): 235–55.

Bryden, Alan. 2006. "Approaching the Privatisation of Security from a Security Governance Perspective." In *Private Actors and Security Governance*, edited by Alan Bryden and Marina Caparini, 3–19. Geneva: Centre for the Democratic Control of Armed Forces.

Bryman, Alan. 2008. *Social Research Methods*. Oxford: Oxford University Press.

Bueger, Christian. 2013. "Actor-Network Theory, Methodology, and International Organization." *International Political Sociology* 7 (3): 338–43.

———. 2014. "Thinking Assemblages Methodologically: Some Rules of Thumb." In *Reassembling International Theory: Assemblage Thinking and International Relations*, edited by Michele Acuto and Simon Curtis, 58–66. Basingstoke: Palgrave.

———. 2016. "Doing Europe: Agency and the European Union in the Field of Counter-Piracy Practice." *European Security* 25 (4). Taylor & Francis: 407–22.

Bueger, Christian, and Frank Gadinger. 2014. *International Practice Theory: New Perspectives*. Basingstoke: Palgrave Macmillan.

———. 2015. "The Play of International Practice." *International Studies Quarterly* 59: 449–60.

Bueger, Christian, and Jan Stockbruegger. 2018. "Actor-Network Theory: Objects and Actants, Networks and Narratives." In *Technology and World Politics: An Introduction*, edited by Daniel R. McCarthy, 42–59. London: Routledge.

Burgess, Peter. 2014. "The Future of Security Research in the Social Sciences and Humanities." European Science Foundation. http://www.esf.org/uploads/media/future_security_research.pdf.

Burningham, Grant. 2016. "How Satellite Imaging Will Revolutionize Everything From Stock Picking to Farming." *Newsweek*. Accessed October 10. http://europe.newsweek.com/why-satellite-imaging-next-big-thing-496443?rm=eu.

Buzan, Barry. 1991. *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Boulder: Lynne Rienner Publishers.

Buzan, Barry, and Lene Hansen. 2009. *The Evolution of International Security Studies*. *Political Science*. Cambridge: Cambridge University Press.

Byman, Daniel. 2013. "Why Drones Work: The Case for Washington's Weapon of Choice." *Foreign Affairs* 92 (July/August): 32–43.

Callon, Michel. 1986a. "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St. Brieue Bay." In *Power, Action and Belief: A New Sociology of Knowledge?*, edited by John Law, 196–223. London: Routledge.

———. 1986b. "The Sociology of an Actor-Network: The Case of the Electric Vehicle." In *Mapping the Dynamics of Science and Technology: Sociology of Science in the Real World*, edited by Michel Callon, John Law, and Arie Rip, 19–34. Basingstoke: Macmillan Press.

Callon, Michel, and Bruno Latour. 1981. "Unscrewing the Big Leviathan: How Actors Macrostructure Reality and How Sociologists Help Them to Do So." In *Advances in Social Theory and Methodology: Toward an Integration of Micro- and Macro-Sociologies*, edited by Karin Knorr-Cetina and Aaron Victor Cicourel, 277–303. London: Routledge.

Campbell, David. 2007. "Geopolitics and Visuality: Sighting the Darfur Conflict." *Political Geography* 26 (4): 357–82.

Carpenter, Charli. 2016a. *Network Relations and Human Security Norm Development: Agenda-Setting and Agenda-Vetting around Collateral Damage Control*. Edited by Deborah Avant and Oliver Westerwinter. *The New Power Politics: Networks and Transitional Security Governance*. Oxford: Oxford University Press.

———. 2016b. "The Future of Global Security Studies." *Journal of Global Security Studies* 1 (1): 92–94.

Casey-Maslen, Stuart. 2014. "The Use of Armed Drones." In *Weapons under International Human Rights Law*, edited by Stuart Casey-Maslen, 382–407. Cambridge: Cambridge University Press.

Ceccorulli, Michela, Carlo Frappi, and Sonia Lucarelli. 2017. "On Regional Security Governance Once Again: How Analysis of the Southern Caucasus Can Advance the Concept." *European Security* 26 (1). Taylor & Francis: 59–78.

Ceyhan, Ayse. 2008. “Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics.” *Surveillance and Society* 5 (2): 102–23. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3430.

Cha, Victor D. 2015. “Assessing the North Korea Threat and U.S. Policy: Strategic Patience of Effective Deterrence?” *Statement before the Senate Committee on Foreign Relations, Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*. Accessed October 1. http://www.foreign.senate.gov/imo/media/doc/100715_Cha_Testimony.pdf.

Cha, Victor D., and Lisa Collins. 2018. “The Markets: Private Economy and Capitalism in North Korea?” *Beyond Parallel*. Accessed October 15. https://beyondparallel.csis.org/markets-private-economy-capitalism-north-korea/.

Chandler, David. 2016. “New Narratives of International Security Governance: The Shift from Global Interventionism to Global Self-Policing.” *Global Crime* Online: 1–17.

———. 2017. “Securing the Anthropocene? International Policy Experiments in Digital Hacktivism: A Case Study of Jakarta.” *Security Dialogue* 48 (2): 1–18.

Charmaz, Kathy. 2000. “Grounded Theory: Objectivist and Contructivist Methods.” In *Handbook of Qualitative Research*, edited by Norman K. Denzin and Yvonna S. Lincoln, 509–35. Thousand Oaks: Sage Publications.

———. 2006. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. *Book*. London: SAGE Publishing.

———. 2017. “The Power of Constructivist Grounded Theory for Critical Inquiry.” *Qualitative Inquiry* 23 (1): 34–45.

Christou, George, Stuart Croft, Michela Ceccorulli, and Sonia Lucarelli. 2010. “European Union Security Governance: Putting the ‘Security’ Back In.” *European Security* 19 (3): 341–59.

Clem, Ralph S. 2016. “Here’s How to Catch Atrocities and Human Rights Violations. (We’re Looking at You, Burundi.).” *Washington Post*. Accessed February 24. https://www.washingtonpost.com/news/monkey-cage/wp/2016/02/23/heres-how-you-catch-atrocities-and-rights-violations-were-looking-at-you-burundi/.

Coen, David, and Tom Pegram. 2015. “Wanted: A Third Generation of Global Governance Research.” *Governance: An International Journal of Policy, Administration, and Institutions* 28 (4): 417–20.

Commission on Global Governance. 1995. *Our Global Neighbourhood*. Oxford: Oxford University Press.

Connolly, William E. 2013. “The ‘New Materialism’ and the Fragility of Things.” *Millennium - Journal of International Studies* 41 (3): 399–412.

Convergne, Elodie, and Michael R. Snyder. 2015. “Making Maps to Make Peace: Geospatial Technology as a Tool for UN Peacekeeping.” *International Peacekeeping* 22 (5): 565–86.

Cook, Damen. 2017. “North Korea’s Most Important Submarine Base.” *The Diplomat*. Accessed May 23. https://thediplomat.com/2017/03/north-koreas-most-important-submarine-base/.

Coole, Diana. 2013. “Agentic Capacities and Capacious Historical Materialism: Thinking with New Materialisms in the Political Sciences.” *Millennium - Journal of International Studies* 41 (3): 451–69.

Coole, Diana, and Samantha Frost. 2010. “Introducing the New Materialisms.” In *New Materialisms: Ontology, Agency, and Politics*, edited by Diana Coole and Samantha Frost, 1–43. Durham & London: Duke University Press.

Cudworth, Erika, and Stephen Hobden. 2013. “Of Parts and Wholes: International Relations beyond the Human.” *Millennium - Journal of International Studies* 41 (3): 430–50.

Daase, Christopher, and Stefan Engert. 2008. “Global Security Governance: Kritische Anmerkungen Zur Effektivität Und Legitimität Neuer Formen Der Sicherheitspolitik.” In *Governance in Einer Sich Wandelnden Welt*, edited by Gunnar Folke Schuppert and Michael Zürn, 475–98. Wiesbaden: VS Verlag.

Daase, Christopher, and Cornelius Friesendorf. 2010. “Introduction: Security Governance and the Problem of Unintended Consequences.” In *Rethinking Security Governance: The Problem of Unintended Consequences*, edited by Christopher Daase and Cornelius Friesendorf, 1–20. London: Routledge.

Datta, Anusuya. 2018. “Key Trends in Earth Observation and How They Are Driving Commercialization & Democratization.” *Geospatial World*. Accessed June 10. https://www.geospatialworld.net/blogs/key-trends-in-earth-observation/.

Davenport, Christian. 2018. *The Space Barons: Elon Musk, Jeff Bezos, and the Quest to Colonize the Cosmos*. New York: Public Affairs.

Defense Mapping Agency. 1996. *Photo Interpretation Student Handbook: Photo Interpretation Principles (Unclassified)*. Washington, D.C.: United States Government. http://sites.miis.edu/geospatialtools2012/files/2012/07/Photo-Interpretation-Student-Handbook.-Photo-Interpretation-Principles.pdf.

Dehqanzada, Yahya A., and Ann M. Florini. 2000. *Secrets for Sale: How Commercial Satellite Imagery Will Change the World*. Washington, D.C.: Carnegie Endowment for International Peace.

DeLanda, Manuel. 2009. *A New Philosophy of Society: Assemblage Theory and Global Complexity*. London: Continuum.

Deleuze, Gilles, and Félix Guattari. 1987. *A Thousand Plateaus*. Minneapolis: University of Minnesota Press.

Derian, James Der. 2009. *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*. 2nd ed. New York: Routledge.

———. 2013. “From War 2.0 to Quantum War: The Superpositionality of Global Violence.” *Australian Journal of International Affairs* 67 (5). Taylor & Francis: 570–85.

Derrida, Jacques, and Maurizio Ferraris. 2001. *A Taste for the Secret*. Cambridge: Polity.

Diehl, Paul F. 2000. “Forks in the Road: Theoretical and Policy Concerns for 21st Century Peacekeeping.” *Global Society* 14 (3): 337–60.

DigitalGlobe. 2015. “Poachers Without Borders: New Satellite Imaging and Predictive Mapping to Empower Park Rangers and Combat Ivory Traffickers in Garamba National Park.” Accessed November 8. http://www.enoughproject.org/files/PoachersWithoutBorders_28Jan2015.pdf.

———. 2017. “2016 Annual Report.”

Dillon, Michael, and Julian Reid. 2001. “Global Liberal Governance: Biopolitics, Security and War.” *Millennium - Journal of International Studies* 30 (1): 41–66.

Dittmer, J. 2014. “Geopolitical Assemblages and Complexity.” *Progress in Human Geography* 38 (3): 385–401.

Dobbs, Michael. 2008. *One Minute to Midnight: Kennedy, Khrushchev, and Castro on the Brink of Nuclear War*. New York: Alfred A. Knopf.

Doman, Mark, Stephen Hutcheon, Dylan Welch, and Kyle Taylor. 2018. “China’s Frontier of Fear.” *ABC News*. Accessed February 11. https://www.abc.net.au/news/2018-11-01/satellite-images-expose-chinas-network-of-re-education-camps/10432924.

Duffield, Mark. 2001. *Global Governance and the New Wars*. London: Zed Books.

Ehrhart, Hans-Georg, Hendrik Hegemann, and Martin Kahl. 2014a. “Putting Security Governance to the Test: Conceptual, Empirical, and Normative Challenges.” *European Security* 23 (2): 119–25.

———. 2014b. “Towards Security Governance as a Critical Tool: A Conceptual Outline.” *European Security* 23 (2): 145–62.

Ellul, Jaques. 1964. *The Technological Society*. New York: Vintage Books.

Engstrom, Ryan, Jonathan Hersh, and David Newhouse. 2017. “Poverty from Space: Using High-Resolution Satellite Imagery for Estimating Economic Well-Being.” WPS8284. Washington, D.C.

Erickson, Andrew S., and Andrew R. Wilson. 2006. “China’s Aircraft Carrier Dilemma.” *Naval War College Review* 59 (4): 12–45.

Erwin, Sandra. 2018. “DigitalGlobe: New Commercial Players Not Threatening Our Government Business.” *SpaceNews*. Accessed November 26. https://spacenews.com/digitalglobe-new-commercial-players-not-threatening-our-government-business/.

Euroconsult. 2018. “Earth Observation Data Market to Reach $2.4 Billion, VAS Market Potentially at $9 Billion by 2027.”

Farrell, Theo. 2007. “The Limits of Security Governance: Technology, Law, and War.” In *Technology and Security: Governing Threats in the New Millennium*, edited by Brian Rappert, 111–32. Basingstoke: Palgrave Macmillan.

Feenberg, Andrew. 1991. *Critical Theory of Technology*. Oxford: Oxford University Press.

———. 2005. “Critical Theory of Technology: An Overview.” *Tailoring Biotechnologies* 1 (1): 47–64.

———. 2017. “A Critical Theory of Technology.” In *The Handbook of Science and Technology Studies*, edited by Ulrike Felt, Rayvon Fouché, Clark A. Miller, and Laurel Smith-Doerr, 4th ed., 633–63. Cambridge: MIT Press.

Feldman, Gregory. 2011. “If Ethnography Is More than Participant-Observation, Then Relations Are More than Connections: The Case for Nonlocal Ethnography in a World of Apparatuses.” *Anthropological Theory* 11 (4): 375–95.

Fine, Ben. 2002. *The World of Consumption: The Material and Cultural Revisited*. 2nd ed. London: Routledge.

———. 2005. “From Actor-Network Theory to Political Economy.” *Capitalism Nature Socialism* 16 (4): 91–108.

Flohr, Annegret, Lothar Rieth, Sandra Schwindenhammer, and Klaus Dieter Wolf. 2010. *The Role of Business in Global Governance: Corporations as Norm-Entrepreneurs*. Basingstoke: Palgrave Macmillan.

Florini, Ann M. 1988. “The Opening Skies: Third-Party Imaging Satellites and U.S. Security.” *International Security* 13 (2): 91–123.

———. 1998. “The End of Secrecy.” *Foreign Policy* 111 (Summer): 50–63.

Folkers, Andreas. 2013. “Wast Ist Neu Am Neuen Materialismus? - Von Der Praxis Zum Ereignis.” In *Critical Matter: Diskussionen Eines Neuen Materialismus*, edited by Tobias Goll, Daniel Keil, and Thomas Telios, 17–34. Münster: edition assemblage.

Foucault, Michel. 1972. *The Archaeology of Knowledge & the Discourse on Language*. New York: Pantheon Books.

Friedrichs, Jörg. 2010. “The Privatization of Force and Its Consequences: Unintended But Not Unpredictable.” In *Rethinking Security Governance: The Problem of Unintended Consequences*, edited by Christopher Daase and Cornelius Friesendorf, 176–97. London: Routledge.

Friesendorf, Cornelius. 2007a. “Pathologies of Security Governance: Efforts Against Human Trafficking in Europe.” *Security Dialogue* 38 (3): 379–402.

———. 2007b. *US Foreign Policy and the War on Drugs: Displacing the Cocaine and Heroin Industry*. New York: Routledge.

Friesendorf, Cornelius, and Christopher Daase. 2010. “Conclusion: Analyzing and Avoiding Unintended Consequences of Security Governance.” In *Rethinking Security Governance: The Problem of Unintended Consequences*, edited by Christopher Daase and Cornelius Friesendorf, 198–213. London: Routledge.

Fritsch, Stefan. 2011. “Technology and Global Affairs.” *International Studies Perspectives* 12 (1): 27–45.

———. 2016. “Technological Ambivalence and International Relations.” *E-International Relations*. Accessed February 25. http://www.e-ir.info/2016/02/24/technological-ambivalence-and-international-relations/#_edn15.

Gigova, Radina. 2017. “Who Vladimir Putin Thinks Will Rule the World.” *CNN*.

Glaser, Barney G. 1978. *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*. Mill Valley: Sociology Press.

———. 1992. *Basics of Grounded Theory Analysis: Emergence vs. Forcing*. Mill Valley: Sociology Press.

———. 2001. *The Grounded Theory Perspective: Conceptualization Contrasted with Description*. Mill Valley: Sociology Press.

Glaser, Barney G., and Anselm L. Strauss. 1967. *The Discovery of Grounded Theory*. Chicago: Aldine Transaction.

Gregory, Derek. 2011. “From a View to a Kill: Drones and Late Modern War.” *Theory, Culture & Society* 28 (7–8): 188–215.

Grove, Jairus. 2016. “An Insurgency of Things: Foray into the World of Improvised Explosive Devices.” *International Political Sociology* Online: 1–19.

Gusterson, Hugh. 2008. “Ethnographic Research.” In *Qualitative Methods in International Relations: A Pluralist Guide*, edited by Audie Klotz and Deepa Prakash, 93–113. New York: Palgrave Macmillan.

Hall, Rodney Bruce, and Thomas J. Biersteker. 2002. “The Emergence of Private Authority in the International System.” In *The Emergence of Private Authority in Global Governance*, edited by Rodney Bruce Hall and Thomas J. Biersteker, 3–22. Cambridge: Cambridge University Press.

Hänggi, Heiner. 2005. “Approaching Peacebuilding from a Security Governance Perspective.” In *Security Governance in Post-Conflict Peacebuilding*, edited by Alan Bryden and Heiner Hänggi, 3–19. Münster: LIT.

Hansen, Nick. 2013. “North Korea Halts Construction of New Long-Range Rocket Launch Facilities.” *38 North*. Accessed May 24. https://www.38north.org/2013/07/tonghae072213/.

Hanson, Marianne. 2002. “Nuclear Weapons as Obstacles to International Security.” *International Relations* 16 (3): 361–79.

Harman, Graham. 2009. *Prince of Networks: Bruno Latour and Metaphysics*. Melbourne: re.press.

———. 2014. “Conclusions: Assemblage Theory and Its Future.” In *Reassembling International Theory: Assemblage Thinking and International Relations*, edited by Michele Acuto and Simon Curtis, 106–12. Basingstoke: Palgrave.

Harraway, Donna J. 1991. *Simians, Cyborgs, and Women: The Reinvention of Nature*. New York: Routledge.

Harvard Humanitarian Initiative. 2011a. “In Close Proximity: Alleged Abduction, Detention and Extrajudicial Killings by Abu Tira.” Accessed November 29. http://www.satsentinel.org/report/close-proximity-alleged-abduction-detention-and-extra-judicial-killings-abu-tira.

———. 2011b. “Launch Point: Corroboration of Reported SAF Air Attacks in South Sudan.” Accessed November 29. http://www.satsentinel.org/sites/default/files/Satellite Sentinel Project report 15 November 2011.pdf.

Hasian, Marouf Jr. 2016. *Forensic Rhetorics and Satellite Surveillance: The Visualization of War Crimes and Human Rights Violations*. Lanham: Lexington Books.

Hawk, David. 2003. “The Hidden Gulag - Exposing North Korea’s Prison Camps.” *Committee for Human Rights in North Korea*. Accessed October 25. http://www.hrnk.org/uploads/pdfs/The_Hidden_Gulag.pdf.

———. 2012. “The Hidden Gulag - Second Edition.” *Committee for Human Rights in North Korea*. Accessed February 12. https://www.hrnk.org/uploads/pdfs/HRNK_HiddenGulag2_Web_5-18.pdf.

Healy, Kieran. 2017. “Fuck Nuance.” *Sociological Theory* 35 (2): 118–27. http://kieranhealy.org/files/papers/fuck-nuance.pdf.

Hegemann, Hendrik, and Martin Kahl. 2016. “(Re-)Politisierung Der Sicherheit? Legitimation Und Kontestation Geheimdienstlicher Überwachung Nach Snowden.” *Zeitschrift Für Internationale Beziehungen* 23 (2): 6–41.

Heilbroner, Robert L. 1967. “Do Machines Make History?” *Technology and Culture* 8 (3): 335–45.

Held, David, and Kevin Young. 2013. “Transforming Global Governance? Structural Deficits and Recent Developments in Security and Finance.” In *The Quest for Global Security: Protection Without Protectionism and the Challenge of Global Governance*, edited by Mary Kaldor and Joseph E. Stiglitz, 355–80. New York: Columbia University Press.

Herrera, Geoffrey L. 2003. “Technology and International Systems.” *Millennium - Journal of International Studies* 32 (3): 559–93.

———. 2006. *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*. Albany: SUNY Press.

Herscher, Andrew. 2014. “Surveillant Witnessing: Satellite Imagery and the Visual Politics of Human Rights.” *Public Culture* 26 (3): 469–500.

Higgins, Eliot. 2015. “New July 17th Satellite Imagery Confirms Russia Produced Fake MH17 Evidence.” *Bellingcat*. Accessed February 11. https://www.bellingcat.com/news/uk-and-europe/2015/06/12/july-17-imagery-mod-comparison/.

Hodder, Ian. 2014. “The Entanglements of Humans and Things: A Long-Term View.” *New Literary History* 45 (1): 19–36.

Hodgson, Camilla. 2018. “Satellite Images Show How the Tiny Ugandan Village of Bidi Bidi Became the World’s Largest Refugee Camp.” *Business Insider*. Accessed December 13. https://www.businessinsider.de/birdi-satellite-images-refugees-south-sudan-2018-1?r=US&IR=T.

Hoijtink, Marijn. 2017. “Governing in the Space of the ‘Seam’: Airport Security after the Liquid Bomb Plot.” *International Political Sociology* 11: 308–26.

Hong, Adrian. 2011. “How to Free North Korea.” *Foreign Policy*. Accessed August 30. http://foreignpolicy.com/2011/12/19/how-to-free-north-korea/.

Hong, Christine. 2013. “The Mirror of North Korean Human Rights.” *Critical Asian Studies* 45 (4): 561–92.

Hönke, Jana, and Markus-Michael Müller. 2012. “Governing (in)Security in a Postcolonial World: Transnational Entanglements and the Worldliness of ‘local’ Practice.” *Security Dialogue* 43 (5): 383–401.

Hsu, Jeremy. 2018. “The Strava Heat Map and the End of Secrets.” *Wired*. Accessed August 20. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

Hülst, Dirk. 2010. “Grounded Theory.” In , edited by Barbara Friebertshäuser, Antje Langert, and Annedore Prengel, 281–300. München: Beltz Juventa.

Hutson, Jonathan. 2011. “The Promise of Peace and the Power of Satellite Imagery.” *Enough Project*.

Ikenberry, G. John. 2013. “Global Security Cooperation in the Twenty-First Century.” In *The Quest for Global Security: Protection Without Protectionism and the Challenge of Global Governance*, edited by Mary Kaldor and Joseph E. Stiglitz, 94–116. New York: Columbia University Press.

Jablonsky, Dan. 2018. “Seeing a Better World Is Built on Business Success.” Accessed January 22. http://blog.digitalglobe.com/industry/seeing-a-better-world-is-built-on-business-success/.

Jacobsen, Katja Lindskov. 2015. *The Politics of Humanitarian Technology: Good Intentions, Unintended Consequences and Insecurity*. Abingdon: Routledge.

Jacobsen, Katja Lindskov, and Kristin Bergtora Sandvik. 2018. "UNHCR and the Pursuit of International Protection: Accountability through Technology?" *Third World Quarterly*. Routledge, 1–17.

Jakobi, Anja P., and Klaus Dieter Wolf. 2013. "Non-State Actors and the Governance of Violence and Crime." In *The Transnational Governance of Violence and Crime: Non-State Actors in Security*, edited by Anja P. Jakobi and Klaus Dieter Wolf, 3–20. Basingstoke: Palgrave Macmillan.

Jasanoff, Sheila. 2004a. "Ordering Knowledge, Ordering Society." In *States of Knowledge: The Co-Production of Science and Social Order*, edited by Sheila Jasanoff, 13–45. London: Routledge.

———. 2004b. "The Idiom of Co-Production." In *States of Knowledge: The Co-Production of Science and Social Order*, edited by Sheila Jasanoff, 1–12. New York: Routledge.

———. 2016. *The Ethics of Invention: Technology and the Human Future*. New York: W. W. Norton.

———. 2017. "Science and Democracy." In *The Handbook of Science and Technology Studies*, edited by Ulrike Felt, Rayvon Fouché, Clark A. Miller, and Laurel Smith-Doerr, 4th ed., 259–87. Cambridge: MIT Press.

Jeandesboz, Julien. 2016. "Smartening Border Security in the European Union: An Associational Inquiry." *Security Dialogue* 47 (4): 292–309.

John F. Kennedy Presidential Library. 2019. "Radio and Television Report to the American People on the Soviet Arms Buildup in Cuba." Accessed June 4. https://microsites.jfklibrary.org/cmc/oct22/doc5.html.

Kaldor, Mary. 1999. *New and Old Wars: Organized Violence in a Global Era*. Cambridge: Polity.

———. 2013. "Restructuring Global Security for the Twenty-First Century." In *The Quest for Global Security: Protection Without Protectionism and the Challenge of Global Governance*, edited by Mary Kaldor and Joseph E. Stiglitz, 117–42. New York: Columbia University Press.

Kaldor, Mary, Ulrich Albrecht, and Genevieve Scheder. 1998. *The End of Military Fordism: Restructuring the the Global Military Sector*. Edited by Mary Kaldor, Ulrich Albrecht, and Genevieve Scheder. London: Pinter.

Kaldor, Mary, and Joseph E. Stiglitz. 2013. "Introduction: The Quest for Global Security." In *The Quest for Global Security: Protection Without Protectionism and the Challenge of Global Governance*, edited by Mary Kaldor and Joseph E. Stiglitz, 1–16. New York: Columbia University Press.

Kalkman, Jori Pascal. 2018. "Practices and Consequences of Using Humanitarian Technologies in Volatile Aid Settings." *Journal of International Humanitarian Action* 3 (1).

Kansakar, Pratistha, and Faisal Hossain. 2016. "A Review of Applications of Satellite Earth Observation Data for Global Societal Benefit and Stewardship of Planet Earth." *Space Policy* online fir. Elsevier Ltd: 1–9.

Kant, Immanuel. 1974. *Kritik Der Reinen Vernunft*. Edited by Wilhelm Weischedel. 1st ed. Wiesbaden: Suhrkamp.

Kaufmann, Stefan. 2016. "Security Through Technology? Logic, Ambivalence and Paradoxes of

Technologised Security." *European Journal for Security Research* 1 (1). Springer International Publishing: 77–95.

Kelle, Udo. 2005. "'Emergence' vs 'Forcing' of Empirical Data? A Crucial of 'Grounded Theory' Reconsidered." *Forum Qualitative Sozialforschung* 6 (2): 1–22.

Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.

Khalili Moghadam, N., M.R. Delavar, and P. Hanachee. 2015. "Automatic Urban Illegal Building Detection Using Multi-Temporal Satellite Imagery and Geospatial Information Systems." *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences* 40: 387–93.

Kinsley, S. 2014. "The Matter of 'virtual' Geographies." *Progress in Human Geography* 38 (3): 364–84.

Kirchner, Emil J., and Roberto Dominguez. 2014. "Security Governance in a Comparative Regional Perspective." *European Security* 23 (2): 163–78.

Kirchner, Emil J., and James Sperling. 2007. *EU Security Governance*. Manchester: Manchester University Press.

Koddenbrock, Kai Jonas. 2015. "Strategies of Critique in International Relations: From Foucault and Latour towards Marx." *European Journal of International Relations* 21 (2): 243–66.

Krahmann, Elke. 2003. "Conceptualizing Security Governance." *Cooperation and Conflict* 38 (1): 5–26.

Krause, Monika. 2013. "Recombining Micro/Macro: The Grammar of Theoretical Innovation." *European Journal of Social Theory* 16 (2): 139–52.

Kroenig, Matthew. 2018. *The Logic of American Nuclear Strategy: Why Strategic Superiority Matters*. London: Oxford University Press.

LaFoy, Scott, and JH Ahn. 2017. "North Korea Maintaining Assets at Kaesong Industrial Complex, Satellite Imagery Shows." *NK Pro*. Accessed May 24. https://www.nknews.org/pro/more-activity-underway-at-kaesong-industrial-complex-satellite-imagery-suggests/.

Lai, K.K. Rebecca, William J. Broad, and David E. Sanger. 2018. "North Korea Is Firing Up a Reactor. That Could Upset Trump's Talks With Kim." *New York TimesNew*. Accessed December 15. https://www.nytimes.com/interactive/2018/03/27/world/asia/north-korea-nuclear.html.

Larkin, Sean P. 2016. "The Age of Transparency." *Foreign Affairs*. Accessed May 12. https://www.foreignaffairs.com/articles/world/2016-04-18/age-transparency.

Larsson, Naomi. 2016. "How Satellites Are Being Used to Expose Human Rights Abuses." *The Guardian*. Accessed April 4. http://www.theguardian.com/global-development-professionals-network/2016/apr/04/how-satellites-are-being-used-to-expose-human-rights-abuses.

Latour, Bruno. 1987. *Science in Action: How to Follow Scientists and Engingeers through Society*. Cambridge: Harvard University Press.

———. 1991. "Technology Is Society Made Durable." In *A Sociology of Monsters: Essays on Power, Technology and Domination*, edited by John Law, 103–31. London: Routledge.

———. 1992. “Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts.” In *Shaping Technology/Building Society: Studies in Sociotechnical Change*, edited by Wiebe E. Bijker and John Law, 225–58. Cambridge: MIT Press.

———. 1993. *We Have Never Been Modern*. Cambridge: Harvard University Press.

———. 1999. “On Recalling ANT.” *The Sociological Review* 46 (1): 15–25.

———. 2005. *Reassembling the Social*. Oxford: Oxford University Press.

Law, John. 1991. “Introduction: Monsters, Machines and Sociotechnical Relations.” In *A Sociology of Monsters: Essays on Power, Technology and Domination*, edited by John Law, 1–23. London: Routledge.

———. 2004. *After Method: Mess in Social Science Research*. London: Routledge.

———. 2009. “Actor Network Theory and Material Semiotics.” In *The New Blackwell Companion to Social Theory*, edited by Bryan S. Turner, 141–58. Oxford: Blackwell Publishing.

———. 2010. “The Materials of STS.” In *The Oxford Handbook of Material Culture Studies*, edited by Mary C. Beaudry and Dan Hicks, 173–88. Oxford: Oxford University Press.

———. 2017. “STS as Method.” In *The Handbook of Science and Technology Studies*, edited by Ulrike Felt, Rayvon Fouché, Clark A. Miller, and Laurel Smith-Doerr, 4th ed., 31–57. Cambridge: MIT Press.

Laygo, Katrina, Thomas W. Gillespie, Noel Rayo, and Erin Garcia. 2012. “Drone Bombings in the Federally Administered Tribal Areas: Public Remote Sensing Applications for Security Monitoring.” *Journal of Geographic Information System*, no. 4: 136–41.

Leander, Anna. 2010a. “Commercial Security Practices.” In *The Routledge Handbook of New Security Studies*, edited by J. Peter Burgess, 208–16. London: Routledge.

———. 2010b. “The Privatization of International Security.” In *The Routledge Handbook of Security Studies*, edited by Myriam Dunn Cavelty and Victor Mauer, 200–210. London: Routledge.

———. 2013. “Technological Agency in the Co-Constitution of Legal Expertise and the US Drone Program.” *Leiden Journal of International Law* 26 (4): 811–31.

———. 2014. “Understanding US National Intelligence: Analyzing Practices to Capture the Chimera.” In *The Return of the Public in Global Governance*, edited by Jacqueline Best and Alexandra Gheciu, 197–220. Cambridge: Cambridge University Press.

———. 2016a. “‘Strong Objectivity’ in Security Studies: Ethnographic Contributions to Method Development.” *International Studies Perspectives* 17 (4): 462–475.

———. 2016b. “The Politics of Whitelisting: Regulatory Work and Topologies in Commercial Security.” *Environment and Planning D: Society and Space* 34 (1): 48–66.

Leander, Anna, and Rens van Munster. 2007. “Private Security Contractors in the Debate about Darfur: Reflecting and Reinforcing Neo-Liberal Governmentality.” *International Relations* 21 (2): 201–16.

Lederach, Jean Paul. 1998. *Building Peace: Sustainable Reconciliation in Divided Societies*. Washington, D.C.: United States Institute for Peace.

Leese, Matthias. 2014. “The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-

Discriminatory Safeguards in the European Union." *Security Dialogue* 45 (5): 494–511.

———. 2015. "'We Were Taken by Surprise': Body Scanners, Technology Adjustment, and the Eradication of Failure." *Critical Studies on Security* 3 (3): 269–82.

Leese, Matthias, and Marijn Hoijtink. 2019. "How (Not) to Talk about Technology: International Relations and the Question of Agency." In *Technology and Agency in International Relations*, edited by Marijn Hoijtink and Matthias Leese, forthcoming. London: Routledge.

Lepgold, Joseph. 1998. "NATO's Post-Cold War Collective Action Problem." *International Security* 23 (1): 78–106.

Levinger, Matthew. 2009. "Geographical Information Systems Technology as a Tool for Genocide Prevention: The Case of Darfur." *Space and Polity* 13 (1): 69–76.

Litfin, Karen T. 1997. "The Gendered Eye in the Sky: A Feminist Perspective on EArth Observation Satellites." *Frontiers: A Journal of Women Studies* 28 (2): 26–47.

———. 1998. "Satellites and Sovereign Knowledge: Remote Sensing of the Global Environment." In *The Greening of Sovereignty in World Politics*, 193–221. Cambridge: MIT Press.

———. 2002. "Public Eyes: Satellite Imagery, the Globalization of Transparency, and New Networks of Surveillance." In *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, edited by James N. Rosenau and J. P. Singh, 65–88. Albany: SUNY Press.

Livingston, Steven. 2015. "Commercial Remote Sensing Satellites and the Regulation of Violence in Areas of Limited Statehood." http://www.global.asc.upenn.edu/app/uploads/2015/01/Livingston_Final.pdf.

Livingston, Steven, and Jonathan Drake. 2017. "We Tried to Save 150 People in Aleppo from 5,000 Miles Away." *Washington Post*. Accessed January 10. https://www.washingtonpost.com/news/monkey-cage/wp/2017/01/09/we-tried-to-save-150-people-in-aleppo-from-5000-miles-away/?utm_term=.9a2fe7347c6b&wpisrc=nl_cage&wpmm=1.

Livingston, Steven, and W. Lucas Robinson. 2003. "Mapping Fears: The Use of Commercial High-Resolution Satellite Imagery in International Affairs." *Astropolitics* 1 (2): 3–25.

Lord, Kristin M. 2006. *Global Transparency: Why the Informations Revolution May Not Lead to Security, Democracy, or Peace*. New York: SUNY Press.

Lubin, Rhian. 2017. "Dramatic Satellite Images Show How Syrian City of Raqqa Has Been Completely Flattened during Relentless Bombing Campaign." *Mirror*. Accessed December 13. https://www.mirror.co.uk/news/world-news/dramatic-satellite-images-show-how-11045549.

Lundborg, Tom, and Nick Vaughan-Williams. 2015. "New Materialisms, Discourse Analysis, and International Relations: A Radical Intertextual Approach." *Review of International Studies* 41 (1): 1–23.

MacKay, Joseph, and Jamie Levin. 2015. "Hanging Out in International Politics: Two Kinds of Explanatory Political Ethnography for IR." *International Studies Review* 17 (2): 163–88.

Markowitz, Kenneth J. 2002. "Legal Challenges and Market Rewards to the Use and Acceptance of Remote Sensing and Digital Information as Evidence." *Duke Environmental Law and Policy Forum* 12 (2): 219–64.

Marres, Noortje, and Javier Lezaun. 2011. “Materials and Devices of the Public: An Introduction.” *Economy and Society* 40 (4): 489–509.

Marshall, Will. 2014. “Tiny Satellites Show Us the Earth as It Changes in Near-Real-Time.” *TED Talks*. Accessed November 11. http://www.ted.com/talks/will_marshall_teeny_tiny_satellites_that_photograph_the_entire_planet_every_day/transcript?language=en.

———. 2018a. “Democratize Access to Data.” *Geospatial World*. Accessed February 15. https://www.geospatialworld.net/article/democratize-access-to-data/.

———. 2018b. “The Mission to Create a Searchable Database of Earth’s Surface.” *TED Talks*. Accessed January 30. https://www.ted.com/talks/will_marshall_the_mission_to_create_a_searchable_database_of_earth_s_surface/transcript#t-361247.

Marx, Andrew, and Samuel Goward. 2013. “Remote Sensing in Human Rights and International Humanitarian Law Monitoring: Concepts and Methods.” *Geographical Review* 103 (1): 100–111.

Masback, Keith J. 2015. “The GEOINT Revolution.” *Trajectory Magazine*. Accessed February 3. http://trajectorymagazine.com/the-geoint-revolution/.

Mathews, Jessica Tuchman. 1989. “Redefining Security.” *Foreign Affairs* 68 (2): 162–77.

Mayer, Maximilian. 2012. “Chaotic Climate Change and Security.” *International Political Sociology* 6: 165–85.

Mayer, Maximilian, and Michele Acuto. 2015. “The Global Governance of Large Technical Systems.” *Millennium - Journal of International Studies* 43 (2): 660–83.

Mayer, Maximilian, Mariana Carpes, and Ruth Knoblich. 2014. “The Global Politics of Science and Technology: An Introduction.” In *The Global Politics of Science and Technology: Concepts Form International Relations and Other Disciplines*, edited by Maximilian Mayer, Mariana Carpes, and Ruth Knoblich, 1–35. Heidelberg: Springer.

Mayntz, Renate. 2009. “Zur Selektivität Der Steuerungstheoretischen Perspektive.” In *Über Governance: Institutionen Und Prozesse Politischer Regelung*, 29–40. Frankfurt: Campus.

Mayring, Philipp. 2014. *Qualitative Content Analysis: Theoretical Foundation, Basic Procedures and Software Solution*. Klagenfurt: Open Access Repository.

McCarthy, Daniel R. 2013. “Technology and ‘the International’ or: How I Learned to Stop Worrying and Love Determinism.” *Millennium - Journal of International Studies* 41 (3): 470–90. http://mil.sagepub.com/cgi/content/long/41/3/470.

———. 2018. “Introduction: Technology and World Politics.” In *Technology and World Politics: An Introduction*, edited by Daniel R. McCarthy, 1–21. London: Routledge.

McCarthy, Daniel R., and Matthew Fluck. 2016. “The Concept of Transparency in International Relations: Towards a Critical Approach.” *European Journal of International Relations* Online: 1–25.

McCourt, David M. 2016. “Practice Theory and Relationalism as the New Constructivism.” *International Studies Quarterly* 60 (3): 475–85.

McDowell, Robin, Martha Mendoza, and Margie Mason. 2015. “AP Tracks Slave Boats to Papua

New Guinea." *Associated Press*. Accessed October 18. https://www.ap.org/explore/seafood-from-slaves/ap-tracks-slave-boats-to-papua-new-guinea.html.

Meiches, Benjamin. 2015. "A Political Ecology of the Camp." *Security Dialogue* 46 (5): 476–92.

Meier, Patrick. 2014. "Crisis-Mapping in Areas of Limited Statehood." In *Bits and Atoms: Informaiton and Communication Technology in Areas of Limited Statehood*, edited by Steven Livingston and Gregor Walter-Drop, online version. Oxford: Oxford University Press.

———. 2015. *Digital Humanitarians: How Big Data Is Changing the Face of Humanitarian Response*. Boca Raton: CRC Press.

Melvin, Curtis. 2009. "North Korea Uncovered." *North Korean Economy Watch*. Accessed October 15. http://www.nkeconwatch.com/north-korea-uncovered-google-earth/.

Mérand, Frédéric, Stéphanie C. Hofmann, and Bastien Irondelle. 2011. "Governance and State Power: A Network Analysis of European Security." *Journal of Common Market Studies* 49 (1): 121–47.

Mettler, Simon A., and Dan Reiter. 2013. "Ballistic Missiles and International Conflict." *Journal of Conflict Resolution* 57 (5): 854–80.

Miller, Lynn H. 1999. "The Idea and the Reality of Collective Security." *Global Governance* 5 (3): 303–32.

Mol, Annemarie. 2002. *The Body Multiple: Ontology in Medical Practice*. Durham & London: Duke University Press.

Muller, Benjamin J. 2009. "Borders, Risks, Exclusions." *Studies in Social Justice* 3 (1): 67–78.

Müller, Martin. 2015. "Assemblages and Actor-Networks: Rethinking Socio-Material Power, Politics and Space." *Geography Compass* 9 (1): 27–41.

Müller, Martin, and Carolin Schurr. 2016. "Assemblage Thinking and Actor-Network Theory: Conjunctions, Disjunctions, Cross-Fertilisations." *Transactions of the Institute of British Geographers* 41: 217–29.

Neumann, Iver B., and Ole Jacob Sending. 2010. *Governing the Global Polity*. Ann Arbor: University of Michigan.

Nexon, Daniel H., and Vincent Pouliot. 2013. "'Things of Networks': Situating ANT in International Relations." *International Political Sociology* 7 (3): 342–45.

Neyland, Daniel. 2009. "Mundane Terror and the Threat of Everyday Objects." In *Technologies of InSecurity: The Surveillance of Everyday Life*, edited by Katja Franko Aas, Helene Oppen Gundhus, and Heidi Mork Lomell, 21–41. New York: Routledge.

NGA [National Geospatial-Intelligence Agency]. 2014. "2020 Analysis Technology Plan." Accessed February 12. ww.nga.mil/MediaRoom/PressReleases/Documents/NGAAnalysisTeckPlafl.Pdf.

North Atlantic Treaty Organization. 2014. "NATO Releases Satellite Imagery Showing Russian Combat Troops inside Ukraine." Accessed December 18. https://www.nato.int/cps/en/natohq/news_112193.htm.

North Korea Sanctions and Policy Enhancement Act of. 2016. "Public Law 114–122."

Northern Sky Research. 2018. "NSR Report: Earth Observation Markets to Generate $54 Billion in

Revenue by 2027." Accessed June 10. https://www.nsr.com/nsr-report-earth-observation-markets-to-generate-54-billion-revenue-by-2027/.

Notely, Tanya, and Camellia Webb-Gannon. 2016. "Visual Evidence from Above: Assessing the Value of Earth Observation Satellites for Supporting Human Rights." *The Fibreculture Journal* 27 (201).

O'Connell, Kevin M. 2017. "The Geospatial Revolution: What's a Government to Do?" *SpaceNews*. Accessed February 15. http://spacenews.com/op-ed-the-geospatial-revolution-whats-a-government-to-do/.

O'Shea, Tara. 2018. "Planet Hosts 150+ International Governors, State Secretaries, & Researchers At Climate.EO Event."

OECD [Organization of Economic Cooperation and Development]. 2014. *The Space Economy at a Glance 2014*. Paris: OECD.

Olbrich, Philipp. 2019a. "Security and Technology: Unraveling the Politics in Satellite Imagery of North Korea." In *Technology and Agency in International Relations*, edited by Marijn Hoijtink and Matthias Leese, 66–87. London: Routledge.

———. 2019b. "Transparency from Space: North Korea Through the Eyes of the United States." *Journal of Regional Security Studies* forthcomin.

———. 2019c. "Technological Expectations and Global Politics: Three Waves of Enthusiasm in Non-Governmental Remote Sensing." *Space Policy* 47 (September). Elsevier: 107–16.

Olbrich, Philipp, and David Shim. 2019. "Symbolic Practices of Legitimation: Exploring Domestic Motives of North Korea's Space Programme." *International Relations of the Asia-Pacific* 19 (1): 33–61.

Olbrich, Philipp, and Nina Witjes. 2015. "Earth Observation and International Security: The Role of Uncertainty in Satellite Imagery Analysis by Non-State Actors." Accessed December 1. http://www.espi.or.at/images/stories/dokumente/Perspectives/ESPI_Perspective_72.pdf.

———. 2016. "Sociotechnical Imaginaries of Big Data: Commercial Satellite Imagery and Its Promise of Speed and Transparency." In *Big Data Challenges: Society, Security, Innovation and Ethics*, edited by Anno Bunnik, Anthony Cawley, Michael Mulqueen, and Andrej Zwitter, 115–26. London: Palgrave Macmillan.

Ong, Aihwa, and Stephen J. Collier. 2005. "Global Assemblages, Anthropological Problems." In *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems*, 3–21. Malden: Blackwell Publishing.

Owen, Taylor, and Robert Gorwa. 2016. "Quantum Leap: China's Satellite and the New Arms Race." *Foreign Affairs*. Accessed September 12. https://www.foreignaffairs.com/articles/2016-09-07/quantum-leap.

Pabian, Frank, Joseph S. Bermudez, and Jack Liu. 2018a. "North Korea Has Begun Dismantlement of the Punggye-Ri Nuclear Test Site." *38 North*. Accessed May 24. https://www.38north.org/2018/05/punggye051418/.

Pabian, Frank V., Joseph S. Bermudez, and Jack Liu. 2018b. "North Korea's Punggye-Ri Nuclear Test Site: Unusual Activity Observed." *38 North*.

———. 2018c. "Not So Fast: A Closer Look at What's Really Going on with North Korea's Experimental Light Water Reactor." *38 North*. Accessed August 24.

https://www.38north.org/2018/03/yongbyon032918/.

Paris, Roland. 2001. “Human Security: Paradigm Shift or Hot Air?” *International Security* 26 (2): 87–102.

Parks, Lisa. 2009. “Digging into Google Earth: An Analysis of ‘Crisis in Darfur.’” *Geoforum* 40 (4): 535–45.

Parshley, Lois Farrow. 2012. “The 9 Most Important Lessons From the Cuban Missile Crisis.” *Foreign Policy*. Accessed June 4. https://foreignpolicy.com/2012/10/19/the-9-most-important-lessons-from-the-cuban-missile-crisis/.

Passoth, Jan-Hendrik, Birgit Peuker, and Michael Schillmeier. 2012. “Introduction.” In *Agency without Actors? New Approaches to Collective Action*, edited by Jan-Hendrik Passoth, Birgit Peuker, and Michael Schillmeier, 1–11. London: Routledge.

Peoples, Columba. 2010. *Justifying Ballistic Missile Defence: Technology, Security and Culture*. Cambridge: Cambridge University Press.

———. 2018. “Extra-Terrestrial Technopolitics: The Politics of Technology in Space.” In *Technology and World Politics: An Introduction*, edited by Daniel R. McCarthy, 182–203. London: Routledge.

Perkins, Chris, and Martin Dodge. 2009. “Satellite Imagery and the Spectacle of Secret Spaces.” *Geoforum* 40 (4). Elsevier Ltd: 546–60.

Pinch, Trevor J., and Wiebe E. Bijker. 1987. “The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other.” *Social Studies* 14 (3): 399–441.

Pouliot, Vincent. 2010. “The Materials of Practice: Nuclear Warheads, Rhetorical Commonplaces and Committee Meetings in Russian-Atlantic Relations.” *Cooperation and Conflict* 45 (3): 294–311.

———. 2016. *International Pecking Orders: The Politics and Practice of Multilateral Diplomacy*. Cambridge: Cambridge University Press.

Prunckun, Hank. 2012. *Counterintelligence: Theory and Practice*. Plymouth: Rowman and Littlefield.

Puccioni, Allison, and Elliot Serbin. 2018. “North Korean ELWR Makes Progress towards Operations.” *Jane’s*. Accessed May 24. http://www.janes.com/images/assets/853/76853/North_Korean_ELWR_makes_progress_towards_operations.pdf.

Pultarova, Tereza. 2017. “From Selling Data to Selling Answers, EO Market Faces Transformation.” *SpaceNews*. Accessed August 20. https://spacenews.com/from-selling-data-to-selling-answers-eo-market-faces-transformation/.

Pyle, Rod. 2019. *Space 2.0: How Private Spaceflight, a Resurgent NASA, and International Partners Are Creating a New Space Age*. Dallas: BenBella Books.

Rammert, Werner. 2012. “Distributed Agency and Advanced Technology. Or: How to Analyze Constellations of Collective Inter-Agency.” In *Agency without Actors? New Approaches to Collective Action*, edited by Jan-Hendrik Passoth, Birgit Peuker, and Michael Schillmeier, 89–112. London: Routledge.

Rappert, Brian, and Stuart Croft. 2007. “Introduction.” In *Technology and Security: Governing Threats in the New Millennium*, edited by Brian Rappert, 1–21. Basingstoke: Palgrave Macmillan.

Raymond, Nathaniel A. 2017. “Beyond ‘Do No Harm’ and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society’s Use of Data.” In *Group Privacy: New Challenges of Data Technologies*, edited by Taylor Linnet, Floridi Luciano, and Bart van der Sloot, 67–82. Cham: Springer.

Raymond, Nathaniel, and Brittany L. Card. 2015. “Applying Humanitarian Principles to Current Uses of Information Communication Technologies: Gaps in Doctrine and Challenges to Practice Harvard Humanitarian Initiative.” Cambridge.

Rekret, Paul. 2016. “A Critique of New Materialism: Ethics and Ontology.” *Subjectivity* 9 (3). Palgrave Macmillan UK: 225–45.

Risse, Thomas. 2012. “Governance in Areas of Limited Statehood: Introduction and Overview.” In *Oxford Handbook of Governance*, edited by David Levi-Faur, 1-12 [online version]. Oxford: Oxford University Press.

Rosenau, James N. 1992. “Governance, Order, and Change in World Politics.” In *Governance without Government: Order and Change in World Politics*, edited by James N. Rosenau and Ernst-Otto Czempiel, 1–29. Cambridge: Cambridge University Press.

———. 2002. “Information Technologes and the Skills, Networks, and Structures That Sustain World Affairs.” In *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, edited by James N. Rosenau and J. P. Singh, 275–87. Albany: SUNY Press.

Rothe, Delf. 2015. “Von Weitem Sieht Man Besser. Satellitensensoren Und Andere Akteure Der Versicherheitlichung.” *Zeitschrift Für Internationale Beziehungen* 22 (2): 97–124.

———. 2017. “Seeing like a Satellite: Remote Sensing and the Ontological Politics of Environmental Security.” *Security Dialogue* 48 (4): 334–53.

Rothe, Delf, and David Shim. 2018. “Sensing the Ground: On the Global Politics of Satellite-Based Activism.” *Review of International Studies* 44 (3): 414–37.

Sadeh, Eligar. 2015. “Obstacles to International Space Governance.” In *Handbook of Space Security: Policies, Applications and Programs*, edited by Kai-Uwe Schrögl, Peter L. Hays, Jana Robinson, Denis Moura, and Christina Giannopapa, 23–39. Heidelberg: Springer.

Sandvik, Kristin Bergtora, and Nathaniel A. Raymond. 2017. “Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response.” *Genocide Studies and Prevention* 11 (1): 9–24.

Sanger, David E., and William J. Broad. 2018. “In North Korea, Missile Bases Suggest a Great Deception.” *New York Times*. Accessed December 16. https://www.nytimes.com/2018/11/12/us/politics/north-korea-missile-bases.html?rref=collection%2Fbyline%2Fdavid-e.-sanger&action=click&contentCollection=undefined&region=stream&module=stream_unit&version=latest&contentPlacement=2&pgtype=collection.

Sarewitz, Daniel. 2011. “Anticipatory Governance of Emerging Technologies.” In *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem*, edited by Gary E. Marchant, Braden R. Allenby, and Joseph R. Herkert, 95–105. Heidelberg: Springer.

Sassen, Saskia. 2006. *Territory, Authority, Rights: From Medieval to Global Assemblages*. Princeton:

Princeton University Press.

Satellite Sentinel Project. 2013. “Civilians Caught in the Crossfire: The Bombing of Abu Kershola and Burning of Ad Dandour.” Accessed November 30. http://www.satsentinel.org/sites/default/files/Civilians_Caught_in_the_Crossfire.pdf.

Saugmann Andersen, Rune. 2017. “Video, Algorithms and Security: How Digital Video Platforms Produce Post-Sovereign Security Articulations.” *Security Dialogue*, 1–19.

Sayes, Edwin. 2014. “Actor-Network Theory and Methodology: Just What Does It Mean to Say That Nonhumans Have Agency?” *Social Studies of Science* 44 (1): 134–49.

Scarlatoiu, Greg. 2014. “The Shocking Truth about North Korean Tyranny.” *Hearing of the U.S. House of Representatives Committee on Foreign Affairs, Subcommittee on Asia and the Pacific*. Accessed October 31. http://docs.house.gov/meetings/FA/FA05/20140326/101981/HHRG-113-FA05-Transcript-20140326.pdf.

Scharre, Paul. 2018. *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton.

Schouten, Peer. 2013. “The Materiality of State Failure: Social Contract Theory, Infrastructure and Governmental Power in Congo.” *Millennium - Journal of International Studies* 41 (3): 553–74.

———. 2014a. “Security as Controversy: Reassembling Security at Amsterdam Airport.” *Security Dialogue* 45 (1): 23–42.

———. 2014b. “Security in Action: How John Dewey Can Help Us Follow the Production of Security Assemblages.” In *Reassembling International Theory: Assemblage Thinking and International Relations*, edited by Michele Acuto and Simon Curtis, 83–90. Basingstoke: Palgrave Macmillan.

Schouten, Peer, and Maximilian Mayer. 2017. “Materiality.” In *Routledge Handbook of International Political Sociology*, edited by Xavier Guillaume and Pinar Bilgin, 305–14. London: Routledge.

Schroeder, Ursula C. 2011. *The Organization of European Security Governance: Internal and External Security in Transition*. London: Routledge.

Schrögl, Kai-Uwe, Peter L. Hays, Jana Robinson, Denis Moura, and Christina Giannopapa. 2015. *Handbook of Space Security: Policies, Applications and Programs*. Heidelberg: Springer.

Sending, Ole Jacob, and Iver B. Neumann. 2006. “Governance to Governmentality: Analyzing NGOs, States, and Power.” *International Studies Quarterly* 50: 651–72.

Shaw, Ian G.R. 2017. “Robot Wars: US Empire and Geopolitics in the Robotic Age.” *Security Dialogue* 45 (8): 451–570.

Sheehan, Michael. 2007. *The International Politics of Space*. New York: Routledge.

Shepherd, Laura J. 2013. “Feminist Security Studies.” In *Critical Approaches to Security: An Introduction to Theories and Methods*, edited by Laura J. Shepherd, 11–23. London: Routledge.

Shim, David. 2013. *Visual Politics and North Korea: Seeing Is Believing*. London: Routledge.

———. 2014. “Remote Sensing Place: Satellite Images as Visual Spatial Imaginaries.” *Geoforum* 51. Elsevier Ltd: 152–60.

———. 2016. “Between the International and the Everyday: Geopolitics and Imaginaries of Home.” *International Studies Review* Online Ver: 1–17.

———. 2018. “Satellites.” In *Visual Global Politics*, edited by Roland Bleiker, 265–71. London: Routledge.

Shorrok, Tim. 2018. “How ‘The New York Times’ Deceived the Public on North Korea.” *The Nation*. Accessed December 15. https://www.thenation.com/article/how-the-new-york-times-deceived-the-public-on-north-korea/.

SIA [Satellite Industry Association]. 2015. “2014 State of the Satellite Industry.” Accessed February 14. http://www.sia.org/annual-state-of-the-satellite-industry-reports/2014-sia-state-of-satellite-industry-report/.

Sinclair, Timothy J. 2012. *Global Governance*. Cambridge: Polity.

Singer, Peter W. 2003. *Corporate Warriors: The Rise of the Privatized Military Industry*. Ithaca: Cornell University Press.

———. 2009. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York: Penguin Press.

Sivanpillai, Ramesh, Brenda K. Jones, and Rynn M. Lamb. 2017. “Accessing Satellite Imagery for Disaster Response through the International Charter: Lessons Learned from the 2011 US Midwestern Floods.” *Space Policy* In Press. Elsevier: 1–8.

Slaughter, Anne-Marie. 2004. *A New World Order*. Princeton: Princeton University Press.

Solomon, Ty, and Brent J Steele. 2016. “Micro-Moves in International Relations Theory.” *European Journal of International Relations* Online.

Sørensen, Estrid. 2009. *The Materiality of Learning: Technology and Knowledge in Educational Practice*. Cambridge: Cambridge University Press.

Soucek, Alexander. 2011. “International Law.” In *Outer Space in Society, Politics and Law*, edited by Christian Brünner and Alexander Soucek, 294–405. Vienna: Springer.

Space Angels. 2019. *Space Investment Quarterly - Q4 2018*. New York: Space Angels.

Sperling, James. 2014a. “Governance and Security in the Twenty-First Century.” In *Handbook of Governance and Security*, edited by James Sperling, 3–13. Cheltenham: Edward Elgar.

———. 2014b. “Regional Security Governance.” In *Handbook of Governance and Security*, edited by James Sperling, 98–119. Cheltenham: Edward Elgar.

Sperling, James, and Mark Webber. 2014. “Security Governance in Europe: A Return to System.” *European Security* 23 (2): 126–44.

Squire, Vicki. 2015. “Reshaping Critical Geopolitics? The Materialist Challenge.” *Review of International Studies* 41 (1): 139–59.

Srnicek, Nick. 2014. “Cognitive Assemblages and the Production of Knowledge.” In *Reassembling International Theory: Assemblage Thinking and International Relations*, edited by Michele Acuto and Simon Curtis, 40–47. Basingstoke: Palgrave.

Srnicek, Nick, Maria Fotou, and Edmund Arghand. 2013. “Introduction: Materialism and World Politics.” *Millennium - Journal of International Studies* 41 (3): 397–397.

Stoler, Ann Laura. 2002. "Colonial Archives and the Art of Governance." *Archival Science*, no. 2: 87–109.

Strauss, Anselm L., and Juliet M. Corbin. 1998. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. *Basics of Qualitative Research Grounded Theory Procedures and Techniques*. 2nd ed. London: SAGE Publishing. http://srmo.sagepub.com/view/basics-of-qualitative-research/SAGE.xml.

Stroikos, Dimitrios. 2016. "China, India in Space and the Orbit of International Society: Power, Status, and Order on the High Frontier." London School of Economics and Political Science.

Susman, Gerald I., and Sean O'Keefe. 1998. *The Defense Industry in the Post-Cold War Era: Corporate Strategies and Public Policy Perspectives*. Edited by Gerald I. Susman and Sean O'Keefe. Oxford: Pergamon.

Tarr, Jeff, and Will Marshall. 2017. "How Satellite Surveillance Is Hauling in Illegal Fishers." *World Economic Forum*. Accessed November 21. https://www.weforum.org/agenda/2017/10/satellites-illegal-fishing-digitalglobe-planet/.

Tucker, Todd N. 2016. "Grounded Theory Generation: A Tool for Transparent Concept Development." *International Studies Perspective* 17 (4): 426–38.

U.S. Department of State. 2016. "Methodology for U.S. Government Estimates of Illegal Drug Production." Accessed February 12. https://www.state.gov/j/inl/rls/nrcrpt/2016/vol1/253214.htm.

———. 2017. "Country Reports on Human Rights Practices for 2017: Korea, Democratic People's Republic Of."

UN Commission of Inquiry on Human Rights in the Democratic People's Republic of Korea. 2014. "Report of the Detailed Findings of the Commission of Inquiry on Human Rights in the DPRK." Accessed January 25. http://www.ohchr.org/Documents/HRBodies/HRCouncil/CoIDPRK/Report/A.HRC.25.CRP.1_ENG.doc.

UN Office for Outer Space Affairs. 2007. "United Nations Treaties and Principles On Outer Space, Related General Assembly Resolutions and Other Documents." Accessed December 1. http://www.unoosa.org/pdf/publications/st_space_11rev2E.pdf.

UNDP [United Nations Development Programme]. 1994. *Human Development Report 1994*. Oxford: Oxford University Press.

US Government. 2010. "National Space Policy of the United States of America." Accessed January 31. https://fas.org/irp/offdocs/ppd/ppd-4-nsp.pdf).

Varshney, Kush R., George H. Chen, Brian Abelson, Kendall Nowocin, Vivek Sakhrani, Ling Xu, and Brian L. Spatocco. 2015. "Targeting Villages for Rural Development Using Satellite Image Analysis." *Big Data* 3 (1): 41–53.

Voelkner, Nadine. 2011. "Managing Pathogenic Circulation: Human Security and the Migrant Health Assemblage in Thailand." *Security Dialogue* 42 (3): 239–59.

Wagnsson, Charlotte, and Arita Holmberg. 2014. "Conflict Management." In *Handbook of Governance and Security*, edited by James Sperling, 324–42. Cheltenham: Edward Elgar.

Walters, William. 2014. "Drone Strikes, Dingpolitik and beyond: Furthering the Debate on Materiality and Security." *Security Dialogue* 45 (2): 101–18.

Waltz, Kenneth N. 1979. *Theory of International Politics*. New York: Random House.

Wang, Ben Yunmo, Nathaniel A. Raymond, Gabrielle Gould, and Isaac Baker. 2013. "Problems from Hell, Solution in the Heavens? Identifying Obstacles and Opportunities for Employing Geospatial Technologies to Document and Mitigate Mass Atrocities." *Stability: International Journal of Security & Development* 2 (3): 1–18.

Webber, Mark. 2014. "Security Governance." In *Handbook of Governance and Security*, edited by James Sperling, 17–40. Cheltenham: Edward Elgar.

Webber, Mark, Stuart Croft, Jolyon Howorth, and Elke Krahmann. 2004. "The Governance of European Security." *Review of International Studies* 30 (1): 3–26.

Weber, Max. 2002. *Wirtschaft Und Gesellschaft: Grundriß Der Verstehenden Soziologie*. Tübingen: Mohr Siebeck.

Wedeen, Lisa. 2010. "Reflections on Ethnographic Work in Political Science." *Annual Review of Political Science* 13 (1): 255–72.

Weiss, Thomas G. 2012. *What's Wrong with the United Nations and How to Fix It*. Cambridge: Polity.

———. 2013a. *Global Governance: Why? What? Whither?* Cambridge: Polity.

———. 2013b. *Humanitarian Business*. Cambridge: Polity.

Weiss, Thomas G., and Rorden Wilkinson. 2014. "Rethinking Global Governance? Complexity, Authority, Power, Change." *International Studies Quarterly* 58 (1): 207–15.

———. 2015. "Introduction: Drivers and Change in Global Governance." *Ethics & International Affairs* 29 (4): 391–95.

Whitman, Jim. 2007. "Global Governance and Twenty-First Century Technology." In *Technology and Security: Governing Threats in the New Millennium*, edited by Brian Rappert, 89–110. Basingstoke: Palgrave Macmillan.

Wibben, Annick T. R. 2011. *Feminist Security Studies: A Narrative Approach*. London: Routledge.

Wilkinson, Rorden. 2002. "Global Governance: A Preliminary Interrogation." In *Global Governance: Critical Perspectives*, edited by Rorden Wilkinson and Steve Hughes, 1–12. London: Routledge.

Willmott, Oliver. 2010. "The Decline of the Foreign Correspondent." *New Statesman*.

Winner, Langdon. 1980. "Do Artifacts Have Politics?" *Daedalus* 109 (1): 121–36.

Witjes, Nina, and Philipp Olbrich. 2017. "A Fragile Transparency: Satellite Imagery Analysis, Non-State Actors and the Making of International Security Issues." *Science and Public Policy* 44 (4): 524–34.

Wittes, Benjamin, and Gabriella Blum. 2015. *The Future of Violence - Robots and Germs, Hackers and Drones: Confronting the New Age of Threat*. New York: Basic Books.

Woolgar, Steve, and Javier Lezaun. 2013. "The Wrong Bin Bag: A Turn to Ontology in Science and Technology Studies?" *Social Studies of Science* 43 (3): 321–40.

Worth, Robert F. 2012. "Can American Diplomacy Ever Come Out of Its Bunker?" *New York Times Magazine*. Accessed February 3. https://www.nytimes.com/2012/11/18/magazine/christopher-stevens-and-the-problem-

of-american-diplomacy.html?ref=us&_r=0.

Wyn Jones, Richard. 1999. *Security, Strategy, and Critical Theory*. Boulder: Lynne Rienner Publishers.

Zürn, Michael. 1998. *Regieren Jenseits Des Nationalstaates: Globalisierung Und Denationalisierung Als Chance*. Berlin: Suhrkamp.

Zwitter, Andrej. 2015. "Big Data and International Relations." *Ethics and International Affairs* 29 (4): 377–89.

Zwitter, Andrej, and Roberto Zicari. 2017. "Big Data Zum Nutzen von Gesellschaft Und Menschheit." In *Unsere Digitale Zukunft: In Welcher Welt Wollen Wir Leben?*, edited by Carsten Könneker, 41–43. Heidelberg: Springer.

Appendix

Table 3: List of Interviews

No.	Interview Details
1	Face-to-face interview, D.C. area, 2 persons, March 2017. Both informants have profound experience with the commercial, research and advocacy dimension of satellite imagery.
2	Face-to-face interview, D.C. area, March 2017. Informant is an expert open-source and satellite imagery analyst.
3	Face-to-face interview, D.C. area, February 2017. Informant is an expert satellite imagery analyst.
4	Face-to-face interview, D.C. area, March 2017. Informant is an expert satellite imagery analyst and human rights specialist.
5	Face-to-face interview, D.C. area, February 2017. Informant is an accomplished expert on the commercial, advocacy and historical dimension of satellite imagery.
6	Face-to-face interview, D.C. area, March 2017. Informant is a security expert and experienced satellite imagery analyst with extensive knowledge about the history and development of the craft.
7	Face-to-face interview, D.C. area, March 2017. Informant is a satellite imagery analyst and an expert on the advocacy dimension.
8	Face-to-face interview, D.C. area, March 2017. Informant is a nuclear scientist, environmental expert and experienced satellite imagery analyst.
9	Face-to-face interview, D.C. area, March 2017. Informant is an expert on the research and advocacy dimension of commercial satellite imagery.
10	Chat interview, March 2017. Informant is a self-taught satellite imagery analyst.
11	Face-to-face interview, D.C. area, March 2017. Informant is an expert on the historical dimension of commercial satellite imagery.
12	Face-to-face interview, D.C. area, March 2017. Informant is an expert on space regulations and politics including satellite imagery.
13	Face-to-face interview, D.C. area, March 2017. Informant is an expert on satellite imagery analysis with a focus on advocacy and communications.
14	Face-to-face interview, D.C. area, February 2017. Informant is a security expert and experienced satellite imagery analyst.
15	Face-to-face interview, D.C. area, March 2017. Informant is a nuclear expert and open-source satellite imagery analyst.
16	Face-to-face interview, D.C. area, March 2017. Informant is a human rights expert and satellite imagery analyst.
17	Face-to-face interview, Bay Area, 3 persons, April 2018. Informants are satellite imagery analysts and were interviewed as part of a research and training session on satellite imagery analysis.
18	Face-to-face interview, Bay Area, April 2018. Informant is an expert satellite imagery analyst.
19	Face-to-face interview, Bay Area, April 2018. Informant is a human rights expert with profound experience in open-source satellite imagery analysis including its advocacy and legal dimension.
20	Face-to-face interview, Bay Area, April 2018. Informant is a nuclear and missile expert and satellite imagery analyst.
21	Face-to-face interview, Bay Area, April 2018. Informant is a commercial satellite imagery expert.

22	VoIP interview, March 2018. Informant is an expert on the commercial and advocacy dimension of satellite imagery.
23	Face-to-face interview, Bay Area, 2 persons, April 2018. Informants are experts on the commercial and analytical dimension of satellite imagery and interviewed as a part of a hackathon event on satellite imagery.
24	Face-to-face interview, Bay Area, April 2018. Informant is an expert on commercial satellite imagery.
25	Face-to-face interview, Bay Area, April 2018. Informants is an expert on commercial satellite imagery.
26	Face-to-face interview, Bay Area, April 2018. Informant is an expert on space and satellite imagery.
27	Face-to-face interview, Bay Area, April 2018. Informant is an expert on space and satellite imagery.
28	Face-to-face interview, D.C. area, March 2017. Informant is an expert on satellite imagery in development, human rights and humanitarian contexts.
29	Face-to-face interview, D.C. area, 2 persons, March 2017. Informants are junior satellite imagery analysts in development contexts.
30	Face-to-face interview, D.C. area, March 2017. Informant is an expert the legal dimension of commercial satellite imagery.
31	Face-to-face interview, D.C. area, March 2017. Informant is an expert on space and satellite imagery.
32	Face-to-face interview, D.C. area, March 2017. Informant is an expert satellite imagery analyst with a focus on environmental and advocacy work.
33	VoIP interview, March 2017. Informant is an experience satellite imagery analyst and an expert on environmental advocacy.
34	VoIP interview, February 2017. Informant is an expert on the political dimension of satellite imagery.
35	Face-to-face interview, Spain, December 2014. Informant is a government expert on satellite imagery.
36	Face-to-face interview, Boston, 2 persons, July 2015. Informants are self-taught imagery experts with particular experience in human rights advocacy.
37	VoIP interview, July 2015. Informant is an expert on commercial satellite imagery.
38	VoIP interview, June 2015. Informant is an expert on human rights advocacy and satellite imagery.
39	VoIP interview, October 2014. Informant is an expert satellite imagery analyst.
40	VoIP interview, September 2014. Informant is a nuclear and environmental expert and satellite imagery analyst.
41	VoIP interview, September 2014. Informant is an expert open-source and satellite imagery analyst.
42	VoIP interview, August 2014. Informant is a security expert and open-source and satellite imagery analyst.
43	VoIP interview, August 2014. Informant is an expert satellite imagery analyst.
44	Face-to-face interview, Germany, January 2017. Informant is a non-proliferation expert and satellite imagery analyst.
45	Face-to-face interview, D.C. area, February 2017. Informant is an expert on space politics and regulations as well as the commercialization of satellite imagery.
46	Face-to-face interview, D.C. area, February 2017. Informant is an expert on commercial, political and regulatory aspects of satellite imagery.
47	Face-to-face interview, D.C. area, 2 persons, March 2017. Both informants are experts on commercial, non-governmental and government uses of satellite imagery.
48	VoIP interview, July 2018. Informant is an expert on government and commercial satellite imagery in development and humanitarian contexts.

49	VoIP interview, June 2018. Informant is an expert on open-source analysis and commercial satellite imagery in human rights contexts.
50	VoIP interview, July 2018. Informant is an expert on open-source analysis and commercial satellite imagery in non-proliferation contexts.

English Summary

Over the past two decades, the commercialization of high-resolution satellite imagery has put the former intelligence technology within reach for non-governmental organizations, journalists and researchers. This fueled expectations that they become increasingly involved in security governance efforts, help promote global transparency from space, and monitor of security threats including nuclear proliferation, human rights violations, humanitarian crises and environmental degradation. The thesis qualifies claims that the commercialization of satellite imagery unambiguously increases global transparency and promotes peace and security. It argues that the positive appraisal of non-governmental remote sensing is based on an understanding of technology as neutral and controllable so that they are believed to be a technological extension of the good intentions of non-governmental actors to reduce uncertainty and secrecy in global politics. Challenging this assessment, the thesis draws on socio-material approaches to security that take seriously the role of technology and matter in security governance. Building on 50 qualitative interviews as well as supplementary documents, it comprehensively explores non-governmental remote sensing to investigate (a) how human and technological factors interact to problematize security, (b) what types of non-government remote sensing have emerged and (c) what kind of transparency is produced and what are its security implications.

In order to pursue the research objectives, the thesis both introduces a conceptual framework and draws on grounded theory methods to organize data collection and analysis. This directly addresses a lack of coherence and accessibility of socio-material approaches and makes explicit the theoretical assumptions and empirical foci that otherwise remain hidden. Grounded theory methods, it is argued, are a suitable complement to socio-material approaches to security with respect to its empirical sensitivity, data-driven theorizing and acceptance of diverse data sources. In short, the conceptual part of the thesis takes a pragmatist perspective to devise research-practical guidelines for the study of technology in security governance.

Adopting a socio-material perspective shows how the problematization of security is co-produced by human and technological factors. The potentials and constraints of commercial satellite imagery co-determine which and how security threats are eventually addressed by non-governmental actors and what kind of transparency is pursued. The thesis traces the force of technology throughout the process of satellite imagery analysis, i.e. during imagery acquisition, interpretation and reporting. Effectively, it demonstrates the techno-political limits to the promise of global transparency. The available imagery alone already constrains the space of possible security problematizations. Once imagery is acquired, the interpretation also constitutes a socio-material process. Analysts define material proxies. They translate matter into security threats so that immaterial threats and structural violence are invisible to non-governmental remote sensing.

Still, it becomes difficult for the observed to discursively escape the hierarchy of material evidence. In essence, the material and visual dimensions of non-governmental remote sensing render security problematizations as intuitively legitimate and credible.

The potentials and constraints of satellite technology also take effect in defining different modes of non-governmental remote sensing. These modes differentiate along two dimensions that are characterized by the goals of non-governmental actors as well as if they actualize the imagery or data potential of remote sensing. Building on the diversity of empirical data, the thesis draws up a typology of four distinct ways how non-governmental actors integrate commercial satellite imagery into their operations. Security think tanks often use satellite imagery to monitor known security threats and produce public information. Human rights NGOs rather seek to advocate for human rights and create a sense of accountability. Both, however, rely on the visual dimension of a handful of satellite images to convince the public and policymakers of the urgency and credibility of insecurities. Humanitarian actors and environmental groups, on the other hand, usually cover large areas of interests that are affected by disasters or environmental degradation. As a result, they tend to actualize the data potential of remote sensing as they are interested in the geographic distribution of accessible roads, affected populations, illegal logging or the extent of oil spillage. Although remote sensing presents its users with the same set of socio-material potentials and constraints, the variation is a result of how non-governmental actors react to and actualize them.

Finally, the thesis challenges prevalent ideas about the effects of transparency promised by non-governmental remote sensing. It argues that non-governmental remote sensing leads to forced transparency. NGOs, think tanks and satellite imagery analysts declare transparency a virtue. They understand it as the amount of publicly available information about a security threat. Taken together, transparency is idealized as a quantifiable virtue that should be maximized. The relatively easy access and global reach of remote sensing allows small groups of actors to pursue this goal on a broad scale. In turn, a lack of transparency is rendered suspicious so that non-governmental users feel justified to force transparency if the required information is not voluntarily provided. Effectively, this blurs the lines between transparency and surveillance. The finding calls for a reassessment of the consequences of non-governmental remote sensing that in addition to the benefits of transparency examines the risks and implications of the maximization of transparency. Among other things, the thesis demonstrates how commercial satellite imagery contributes to risks that reinforce remote governance practices which disproportionally affect non-Western countries, draws the observers into the security situations and complicates diplomatic crisis management.

The thesis establishes how human and technological factors co-produce non-governmental remote sensing. As a result, neither the virtuous nor forced transparency are foregone conclusions but dependent on which and how the potential and constraints of satellite imagery are actualized and stabilized.

Nederlandse Samenvatting

In de afgelopen twee decennia heeft de commercialisering van hoge resolutie satellietbeelden deze voormalige inlichtingendienstentechnologie beschikbaar gemaakt voor niet-gouvernementele organisaties, journalisten en onderzoekers. Dit heeft verwachtingen gewekt dat zij steeds meer betrokken raken bij inspanningen op het gebied van veiligheidsbeheer, mondiale transparantie met betrekking tot de ruimte hebben bevorderd, en toezicht houden op veiligheidsdreigingen zoals nucleaire proliferatie, schending van mensenrechten, humanitaire crises, en de achteruitgang van het milieu. Dit proefschrift toetst beweringen dat de commercialisering van satellietbeelden eenduidig mondiale transparantie vergroot en veiligheid en vrede stimuleert. Het betoogt dat de positieve beoordeling van niet-gouvernementele remote sensing is gebaseerd op een opvatting van technologie als neutraal en controleerbaar, zodat dit wordt beschouwd als een technologisch verlengstuk van de goede bedoelingen van niet-gouvernementele actoren om onzekerheid en geheimhouding in de mondiale politiek te verminderen. Om deze beoordeling te beproeven, baseert deze dissertatie zich op socio-materiële benaderingen ten aanzien van veiligheid met het doel om de rol van technologie en materie in veiligheidsbeheer serieus te nemen. Op basis van 50 kwalitatieve interviews en aanvullende documenten, analyseert dit proefschrift uitvoerig niet-gouvernementele remote sensing om te onderzoeken (a) hoe menselijke en technologische factoren op elkaar inwerken om veiligheid te problematiseren, (b) welke soorten niet-gouvernementele remote sensing zijn ontstaan en (c) welke soorten van transparantie worden gecreëerd en welke implicaties deze hebben voor veiligheid.

Om deze onderzoeksdoelen na te streven, introduceert deze dissertatie een conceptueel raamwerk en baseert zich op gefundeerde theoriebenadering om dataverzameling- en analyse te ordenen. Het proefschrift identificeert direct een gebrek aan samenhang en toegankelijkheid van socio-materiële benaderingen en legt theoretische aannames en empirische focuspunten bloot die normaliter verborgen blijven. Gefundeerde theoriebenadering, luidt het betoog, is een gepaste toevoeging op socio-materiële benaderingen ten opzichte van veiligheid wat betreft empirische en datagedreven theorievorming en aanvaarding van verscheidene databronnen. Kortgezegd, het conceptuele deel van de dissertatie hanteert een pragmatistisch perspectief om onderzoekspraktische richtlijnen op stellen voor de studie van technologie binnen veiligheidsbeheer.

Het aannemen van een socio-materiaal perspectief laat zien hoe de problematisering van veiligheid deels wordt geschapen door menselijke en technologische factoren. De mogelijkheden en beperkingen van commerciële satellietbeelden bepalen mede welke en de manier waarop niet-gouvernementele actoren veiligheidsdreigingen aanstippen en welke soorten van transparantie

zij nastreven. Dit proefschrift volgt de kracht van technologie tijdens het proces van satellietbeeldenanalyse, dat wil zeggen tijdens beeldverwerving, interpretatie en rapportage. Het demonstreert dat het techno-politieke de belofte van mondiale transparantie beperkt. De beschikbare beelden alleen al beperkingen de ruimte van veiligheidskwesties. Zodra de beelden zijn verkregen, vormt ook de interpretatie daarvan een socio-materieel proces. Analisten definiëren materiele proxies. Zij vertalen materie in beveiligingsdreigingen zodat immateriële bedreigingen en structureel geweld onzichtbaar zijn voor niet-gouvernementele remote sensing. Desalniettemin wordt het moeilijk voor de degenen die geobserveerd worden om discursief te ontsnappen aan de hiërarchie van materieel bewijs. In wezen maken de materiële en visuele dimensies van niet-gouvernementele remote sensing veiligheidskwesties tot intuïtief legitiem en geloofwaardig.

De mogelijkheden en beperkingen van satelliettechnologie hebben ook invloed op de vorming van verschillende modi van niet-gouvernementeel remote sensing. Deze modi vallen te onderscheiden in twee dimensies die gekarakteriseerd worden door zowel de doelen van niet-gouvernementele actoren als de wijze waarop zij de afbeeld- en datamogelijkheden van remote sensing realiseren. Door voort te bouwen op een diversiteit aan empirische data, construeert dit proefschrift een typologie van vier verschillende manieren waarop niet-gouvernementele actoren commerciële satellietbeelden hebben geïntegreerd in hun verrichtingen. Veiligheidsdenktanks maken veelal gebruik van satellietbeelden om toezicht te houden op bekende veiligheidsdreigingen en om openbare informatie te creëren. Mensenrechten-ngo's kiezen er liever voor om te pleiten voor mensenrechten en om een gevoel van verantwoordingsplicht te creëren. Beide zijn echter afhankelijk van de visuele dimensies van een beperkt aantal satellietbeelden om zowel een breed publiek als beleidsmakers te overtuigen van de spoed en geloofwaardigheid van onveiligheden. Humanitaire actoren en milieuorganisaties aan de andere kant nemen doorgaans aandachtsgebieden voor rekening die zijn getroffen door rampen of achteruitgang van de natuur. Ten gevolge daarvan neigen zij om de datamogelijkheden van remote sensing te realiseren alsof zij belang hebben bij een geografische distributie van toegankelijke wegen, getroffen bevolkingen, illegale houtkap, of de omvang van olielekkage. Hoewel remote sensing gebruikers presenteert met een vergelijkbare set aan socio-materiële mogelijkheden en beperkingen, zijn de verschillen een uitkomst van hoe niet-gouvernementele actoren hierop reageren en hoe zij deze realiseren.

Tenslotte toetst dit proefschrift gangbare opvattingen over de effecten van transparantie die wordt beloofd door niet-gouvernementeel remote sensing. Het betoogt dat non-gouvernementeel remote sensing zorgt voor afgedwongen transparantie. Ngo's, denktanks, en satellietbeeldanalisten roepen transparantie uit tot een deugd. Zij vatten het op als het geheel van publiekelijk beschikbare informatie over een veiligheidsdreiging. Als geheel wordt transparantie

geïdealiseerd als een kwantificeerbare deugd die gemaximaliseerd dient te worden. Het betrekkelijke gemakkelijke toegang tot en mondiaal bereik van remote sensing stelt kleine groepen van actoren in staat om deze doelen op grote schaal na te streven. Aan de andere kant wordt een gebrek aan transparantie gezien als verdacht, zodat niet-gouvernementele gebruikers zich gerechtvaardigd voelen om transparantie af te dwingen als de vereiste informatie niet vrijwillig wordt verschaft. Dit zorgt ervoor dat de grenzen tussen transparantie en surveillance vervagen. De onderzoeksuitkomsten roepen daarom op tot een herwaardering van de gevolgen van niet-gouvernementeel remote sensing die in aanvulling op de voordelen van transparantie ook de risico's en implicaties van de maximalisering van transparantie in acht neemt. Deze dissertatie toont onder andere aan dat de manieren waarop commerciële satellietbeelden bijdragen aan risico's die bestuurspraktijken op lange afstand versterken en daarom ook onevenredig non-Westerse landen aantasten, observanten in veiligheidssituaties betrekken en diplomatiek crisisbeheer bemoeilijken.

Dit proefschrift stelt vast hoe menselijke en technologische factoren deels non-gouvernementele remote sensing tot stand brengen. Als gevolg daarvan zijn noch de deugdelijkheid noch de gedwongen transparantie een uitgemaakte zaak, maar zijn deze afhankelijk van de manier waarop de mogelijkheden en beperkingen van satellietbeelden worden gerealiseerd en gestabiliseerd.

Author Biography

Philipp Olbrich (Paderborn, Germany, 1987) obtained a B.Sc. in Social Sciences from the University of Cologne. He continued to graduate with a M.A. (with honors) in East Asian Economy and Society from the University of Vienna in 2015. After working as a researcher for the Austrian Institute for International Affairs, he started as a Ph.D. candidate at the Department of International Relations and International Organization at the University of Groningen. During his Ph.D. he pursued his research interests concerning the role of technology in global security and the conflict on the Korean peninsula. In doing so, he participated in over a dozen international academic conferences and published five peer-reviewed journal articles and a number of book chapters and policy papers. For more than three years, he was the Managing Editor of the Journal of International Humanitarian Action (2016–2019).