TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Perceptual Modalities in Offensive Cyberspace Operations: Tools, Practices and Experiences of Targeting

Master's thesis

Student: Konor Sajti

Supervisor: Dr. Rain Ottis

Tallinn 2026

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Tajumisviisid küberründeoperatsioonides: sihtimise tööriistad, tavad ja kogemused

Magistritöö

Üliõpilane: Konor Sajti

Juhendaja: Dr. Rain Ottis

Tallinn 2026

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Konor Sajti

20 May 2026

Acknowledgements

I would like to thank my supervisor, Dr. Rain Ottis and reviewer, Dr. Adrian Nicholas Venables, for their invaluable guidance, feedback and support during this research project. I also thank my friends, colleagues and family for their continued support and encouragement throughout this process, and their generous belief in me.

Abstract

This thesis traces the perceptual modalities of targeting in offensive cyberspace operations (OCO) to understand the ontological and epistemic logics that shape cybersecurity tool design, targeting practice and the violent results of targeting. It finds that targeting is the practice of engineering knowledge and perceptual modalities into tools and operationalising them to produce violence in cyberspace. By mapping the ontology and epistemology of targeting tools, the thesis proposes an analytic framework to understand targeting's sub-optimal practices and violent effects. These findings are used to propose ways to design more efficient and ethical tools, while propagating a receptivity toward the lived experience of targeting – and being targeted – in cyberspace.

This thesis is written in English and is seventy-eight pages long, including five chapters, one figure and three tables.

Lühikokkuvõte

Tajumodused rünnakutes küberruumis: digivaenlase tajumise tööriistad, tavad ja kogemused

See lõputöö jälgib ründevälise küberruumioperatsioonide (OCO) sihtimise tajumismeetodeid, et mõista ontoloogilisi ja epistemilisi loogikaid, mis kujundavad küberturbe tööriistade disaini, sihtimisharjumusi ja sihtimise vägivaldseid tulemusi. Töös leitakse, et sihtimine on praktika, mis seisneb teadmiste ja tajumismeetodite insenerimises tööriistadesse ning nende operationaliseerimises, et tekitada küberruumis vägivalda. Kaardistades sihtimistööriistade ontoloogia ja epistemoloogia, pakub lõputöö analüütilist raamistikku sihtimise suboptiimalsete praktikate ja vägivaldsete mõjude mõistmiseks. Neid järeldusi kasutatakse viisil, mis pakub ettepanekuid tõhusamate ja eetilisemate tööriistade kujundamiseks ning soodustab vastuvõtlikkust sihtimise — ja sihtimise all olemise — elulisele kogemusele küberruumis.

Lõputöö on kirjutatud inglise keeles keeles ning sisaldab teksti 78 leheküljel, 5 peatükki, 1 joonist, 3 tabelit.

List of abbreviations and terms

CIDR	Classless Inter-Domain Routing
IDS	Intrusion Detection System
IP	Internet Protocol
OCO	Offensive Cyberspace Operations
RQ	Research Question
RST	Reset
STS	Science and Technology Studies
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
US	United States, as in United States of America

Table of contents

List of figures

List of tables

1 Introduction

1.1 Motivation

Contemporary cybersecurity tooling has a marked visual and mental aesthetic. In what James Shires calls a ‘cyber-noir’, dark patterns and threatening shapes pervade how cybersecurity is represented in cyberspace. Shires observes “[m]any emerging companies in the cybersecurity industry deliberately play on the popular perception of cybersecurity as a nether region, a gloomy underworld in which the good guys must resort to unconventional tactics to keep at bay a motley group of threats to the digital safety of unsuspecting individuals, businesses, and governments” [1, p. 82]. His comments remind the reader that the image of cyberspace as a blue, or purple, or white, or yellow deck of cute cat videos and dancing figures is only a fragment of how cyberspace is imagined and experienced today. Shires highlights how the visual experience of cyberspace differs for cybersecurity professionals in quite some material ways. This prompts the question of whether there can be multiple perceptual experiences of cyberspace beyond the visual cyber-noir that dominates many of its tools today. It also raises the question whether perception in cyberspace is dominated by a visual modality, or something else.

Assuming that perception is indeed variable, one is similarly urged to question standing ideas and models that obfuscate the role of perception in cyberspace operations. Is perception truly so unitary to be completely uninteresting for research? Is it really so uninteresting that it requires no incorporation into models, like the popular cyber kill chain or MITRE ATT&CK framework? What are the consequences of ignoring perception when it comes to finding, delineating and destroying targets in cyberspace? Driven by these questions, the present research investigates the perceptual modalities of cyberspace targeting to uncover the variegated logics, nature, and practices they produce.

1.2 Research Questions

RQ-1: What perceptual modalities are operationalised in offensive cyberspace targeting?

RQ-2: How do these perceptual modalities affect the practice and experience of targeting?

RQ-3: What are the implications of these observations for the design of offensive cyberspace targeting tools and the ethics of offensive cyberspace operations?

1.3 Research Gap

While there exists some siloed research about reconnaissance in offensive cybersecurity, targeting in military sciences, and target selection in legal treatises, target perception is nearly absent in the literature or discourse of cybersecurity.[1]

1.3.1 Cybersecurity Literature

Cybersecurity professionals often focus on process models of targeting, typically following one or another kind of procedural explanation, like the so-called cyber kill chain or the MITRE ATT&CK framework. These models picture offence as a set of quasi-sequential activities that lead to a desired, or undesired, end state. This presents a narrow view of the practical modalities of offensive cyberspace operations (OCO) and limits the academic study of the subject to general case studies, theories and laboratory simulations [2]. Despite their merits, these studies provide little to no insight into how operators experience their environments or how targeting evolved to be what it is today.

Naturally, a number of studies engage with specific cases of OCO or general overviews of the subject [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]. These studies provide scattered pieces of evidence for how OCOs play out and rarely provide significant insight into the minds and perspectives of operators. Other researchers focus on targeted topics, very often the material consequences, ethics and law of offensive action [13], [14], [15], [16]. These studies rely on legal or techno-scientific discourses with a

[1] Literature was identified by targeted searches with advanced queries in Google Search, Google Scholar, Taylor & Francis, Oxford University Press, and other academic databases. The search terms are logged in Appendix 2.

tendency to oversimplify complex human experiences for the sake of clear-cut rules and design principles.

1.3.2 Military Literature

Military scholarship is preoccupied with the immediate means and effects of offensive operations. The differentiation between kinetic and non-kinetic action, as well as the transition from one to the other, has been a focal point for scholarship [17], [18]. The precision of targeting and the extent of effects have also proven to be noteworthy. Collateral damage has been studied to control unintended effects and manage imprecise targeting [19], [20], while propositions have been made about algorithms to enhance target selection [21]. These studies reflect attempts to make targeting more precise, often conflating precision with humanitarianism [cf. 22]. Finally, as the contrast between cyberspace and the information environment is blurred, there have been calls to re-conceptualise psychological and information operations along the lines of offensive cyber capabilities [23]. While these studies contribute greatly to our understanding of the decision-making mechanisms of cyberspace targeting, they do little to improve our understanding of operator experiences.

1.3.3 Critical Studies

Alongside cybersecurity's exclusive focus on tools and processes and the military's overwhelming attention to targeting and effects, critical security studies investigates perceptual modalities in offensive operations outside cyberspace. Prominently, the historian Antoine Bousquet studies the evolution of military technologies, tactics and thought from the Renaissance to artificial intelligence in the contemporary age [24]. In his book, he argues that targeting has been influenced by an increasingly mechanised and mathematicised logic of perception, which resulted in the dehumanisation and expansion of the military's eye, the 'martial gaze' [24]. This thesis is inspired by Bousquet's work in tracing perception in offensive cyberspace operations through targeting. While many military artefacts – especially unmanned platforms and surveillance technology [25], [26], [27], [28], [29], [30], [31], [32] – have been studied from the perspective of perception, no work presently available interrogates the modalities of perception in offensive cyberspace operations. This leaves room to study perception in cyberspace targeting.

Additionally, several multidisciplinary studies have contributed to our understanding about how tools participate in targeting. Many of these focus on the various policies, products and technologies of Palantir Technologies Inc., a company headquartered in the United States. Palantir has become increasingly notorious as media started reporting on its use by the United States' Immigration and Customs Enforcement and healthcare agencies [33]. Governments view Palantir as a tool of efficiency in the age of big data and global threats [34]. The technology is highly contentious, which has prompted scholars to study how Palantir's selective vision, data transformations, and interactive design violate subjectivity and citizen rights. The company's main product is a triplet of platforms: Gotham is an analytic platform, Foundry is a microservice that connects Gotham to its data pool, and Apollo is the software that automates and delivers data and infrastructure [35]. From a certain perspective, Palantir's stack is a configurable, modular, multilateral group of platforms that enables previously disparate data to be aggregated, queried and analysed from a few interfaces [36]. For instance, Palantir can connect a license plate database with a database of social media profiles to find connections by interfacing data from two sources in a single platform via Application Programming Interface calls. Sarah Brayne's ethnographic study of the Los Angeles Police Department's use of Palantir's Gotham platform described the system as 'dragnet surveillance' where previously disparate data points become connected and correlated via a user-friendly interface [37]. In these 'algorithmic ecologies' of surveillance, big data is converted into actionable signatures for predictive policing [38]. Iliadis and Acker conceptualise Palantir as a 'surveillance platform', where "information standards like administrative metadata [act] as phenomena for structuring social worlds" [35, p. 334]. They argue that the platform's data regulation – essentially, what ontology it uses to integrate and discard new data points – is part of a knowledge production process that "understands the world in a certain way" [35, p. 352].[2] Galis and Karlsson point to the materiality of this ontology, as they explain that Palantir's normative "ideology conceptualized in the code of POL-INTEL defines subject positions through security ideology" [39, p. 2447].

> "This also means making critical choices about how to describe the world, how to generate concepts that differentiate between balancing objective

[2] Ontology in this sense is not the branch of philosophy that deals with knowledge but an artefact that is produced by correlating objects.

> representation, epistemology, and the affordances of code [sic]. The Palantir Gotham E-ontology is about coding a system of classifications based on the world view of the police user." [39, pp. 2446-2447].

Palantir, therefore, is a case study of how technology embeds subjective world views into a targeting system, affecting both user and target. It is this ontology – in combination with an epistemology – that Massumi finds to be the 'operative logic of power', which he argues is a computational mechanism that renders the adversary an object of predictive policing, and thus, a mesh of targetable associations [40]. Amoore calls the product of predictive risk scoring based on aggregated data 'data derivatives' [41]. These derivatives are the means to embed mutable norms and pre-emptive authority into offensive operations via the visualisations of uncertain futures and a shift of decision-making authority to automated outputs [41]. Recognising the extent to which Palantir performs this effect, Tan calls the company and its technology an 'onopticon', an "institutional architect of a new ontological regime" in which targeting tools become "the institutional machinery of preemptive categorization" [42, pp. 1, 4].

Essentially, what Iliadis, Acker, Amoore, Massumi and Tan highlight is how the mere manipulation and platformisation of data result in a system of predictive, preemptive and preventive policing. Disciplinary power is inherent to this system, which violates the subjectivity of the target as an entity anything other than one destined for targeting. This disappearance of the subject is what Rupert Barrett-Taylor used to illustrate the obsession and conflation of modern war with technology-aided targeting [43]. It is what Nordin and Ödin called the new ontology of war – war that is defined by an 'ontic reality' of forming experience through the processing of targets [44]. Collectively, research into Palantir shows that the ontology of the company's platforms exercises violent effects *as part of* targeting. It shows that forced categorisation that the technology's architecture enforces is a means to dissolve the subjectivity of the target into a web of associations. This architecture is defined by the subjective world view of the engineer, and later appropriated and augmented by the targeteer. Ultimately, Palantir

researchers have shown that violence, targeting and the materiality of technology are intertwined in a way that produces violence and new authorities of targeting.[3,4]

It is in this vein that the present research analyses cyberspace targeting tools to unravel the violent practices and effects that they enforce through their socio-technical modalities of perception. Building on the technological understanding provided by cybersecurity engineering and scholarship; utilising the ideas, doctrines, and practices of military thinkers; and relying on the methodological and theoretical toolkit of contemporary critical security, science and technology studies, this thesis investigates the gap between cyberspace targeting and perception – a gap that overshadows how targeting is practiced, and how it is lived through today.

[3] Throughout the paper, 'knowledge' refers to a belief in what one believes to be justified to believe. It is different from guesswork by the virtue of justification, and it is often dependent on some perception of the world around a subject. It is important to note that the thesis does not engage with the idea of knowledge as true belief, rather assumes that more than one subject may form beliefs with different truth values assigned to those beliefs by the subject, and thus, it is not assumed that there is a single system of knowledge that is extant to the subject. For this exclusion of the truth value requirement from knowledge, the paper uses 'knowledges' in the plural multiple times to emphasise how one system of justified belief may be different from another.

[4] Violence refers to the harm caused by one subject to another subject.

1.4 Research Methods

1.4.1 Assumptions

This research analyses professional tools, practices and experiences in cyberspace targeting. It assumes that they reflect and shape the perceptual modalities that inhibit targeting tools. Such tools include network mapping and traffic sniffing technologies, as well as code that can penetrate target networks. It is a further assumption that studying tools reveals the logics and logistics of cyberspace targeting that shape contemporary tool design, and the practices and experiences of targeting. To complete this analysis, two tools of cyberspace targeting – Nmap and Burp Suite – as well as their accompanying textual artefacts – documentation, manuals, handbooks, and websites – are analysed.

1.4.2 Analysing Tools

The analysis of tools is inspired by Science and Technology Studies (STS), an interdisciplinary field that studies the development of technologies and their effects on professional practice and experience. STS has historically been successful in uncovering the social context and social effects of science and technology [45], including the study of socio-technical imaginaries [46], [47], [48], [49], [50], the emergence of socio-technical systems [51], [52], [53], and the formation of techno-scientific knowledge and assemblages [54], [55], [56], [57], [58], [59], [60]. Generally, STS highlights the variability, specificity and complexity of techno-scientific interactions, explaining scientific and technological developments with reference to each other and their wider social context. In STS, “theory is done in the form of case studies”, using case studies as narratives to explain theories with highly contextual observations [57, p. 630]. Its methods often resort to the analysis of tools and technologies with the aim to understand, “from a particular ‘situated’ point of view, [the] material-semiotics in which materials and meanings are woven together” [61, p. 31]. By analysing how tools emerge, interact with and produce science, STS studies how practice forms around scientific artefacts. In this vein, the present research analyses tools to understand the practices and experiences of cyberspace targeting, while querying the conditions of emergence and operationalisation of tools that participate in targeting.

This analysis pays homage to Gilles Deleuze and Félix Guattari's assemblage theory [62], [63], [64], [65], as well as Bruno Latour and Steve Woolgar's actor-network theory [66], [67]. These theories propose network-based models to understand technologies as emergent systems within larger systems of social making and meaning-making. Both theories acknowledge the socio-technical conditions that give rise to artefacts while also framing their use, interpretation, configurations, and engineering [68, p. 93]. They help explain how seemingly static and agentless tools produce the logics, practices and experiences of targeting. Therefore, the thesis maps the actor-networks of cyberspace assemblages onto ontologies and epistemologies of targeting.

1.4.3 Thick Description & Systems Analysis

The study enumerates and describes targeting practice and experiences through a 'thick description' of the modalities of particular targeting tools.[5] This thick description treats perception as a varied experience that can and needs to be studied with attention to detail, variation and context. Therefore, tools are analysed in their context, both in terms of the period of their emergence and in terms of their operationalisation as targeting technologies.

In addition, tools are analysed qualitatively to delineate the targets they perceive and to determine the epistemic techniques and modalities they use to perform targeting. First, the structure of tools is taken into account from a systems science perspective. This enables a deeper analysis and reconstruction of the tools' target ontologies and epistemologies. These respectively refer to the system in which the tools organise knowledge about their targets, as well as the means through which they gain and produce knowledge about them. Second, the target ontologies and epistemologies of tools are used to define their *epistemé* and *targeting domains*, delineating the operational practices they afford. Finally, these affordances are mapped onto social conditions to identify the harms to targets and targeteers in cyberspace targeting. This serves to pinpoint ethical issues and challenges of productivity in cyberspace targeting.

[5] Thick description is the contextual, detailed description of human action that goes beyond mere characterisations and looks for explanations of action, often from emic points of view [69]. Originally proposed by Gilbert Ryle in 1968 [70] and later popularised by Clifford Geertz [71], the approach has been widely adopted in anthropology and sociology to ensure interpretability by providing context for the reader beyond what is purely necessary for abstract theory construction. Importantly, thick description – at least partially – attempts to understand action from the local perspective of the performer and their context as they perceive it, and thus, it is more than the observations of solely the etic researcher [72].

1.5 Sources

This study requires access to two cyberspace targeting tools and their corresponding textual lexicons. They are analysed to discern the design principles, use cases, and affordances that inhibit modalities and reflect perception in cyberspace targeting.[6] These tools and models were selected because they are accessible, widely used in cyberspace targeting, and have detailed textual lexica. Further details are provided about the specific tools and their lexica in the respective sections of Chapter 3.

1.6 Scope

The research concerns tools that participate in intelligence and predatory targeting. The former is defined here as the process through which confidential information is collected about potential targets.[7,8] The latter concerns the process that results in the compromise of the integrity or availability of systems. Both types of targeting must take place in and through cyberspace to be included in this research, which does not concern psychological, information or influence operations, cognitive or narrative warfare, or the kinetic targeting of computer systems. Instead, the study focuses on the targeting of entities in and through cyberspace with tools that are designed to participate in the practice of cyberspace targeting.

1.7 Contribution

The research provides two distinct contributions to the academic study of cybersecurity. For one, it produces a framework to analyse cyberspace targeting tools and practices with respect to targeting domains, target ontologies, targeting practice and violence.

---

[6] Affordance is a property that "shape[s] how people engage with [their] environments" [73], n.p.. They describe the modalities that environments afford to their participants, including both constraints on behaviour and enablers of action. As an example, Lessig has argued that cyberspace is defined by an 'architecture of code' that is constructed by ICT designers and which restricts the possibilities of cyberspace [74, p. 533]).

[7] Some tools of intelligence targeting, like Nmap, may have a limited capacity to cause destruction – for example, through flooding its targets with network packets. Yet, they are primarily aimed at intelligence targeting and not predation, although this function may depend on the intent of the offensive operator.

[8] Here, confidential information refers to not only what is formally labeled as such, but also any information that is used to produce violent knowledge that has the capacity to enable targeting. For instance, knowing a domain name and its corresponding IP address can be public and unprotected per se, but transformed into knowledge that is used for targeting. Thus, public information can become confidential when used to produce targeting violence.

This framework is validated via a thick description of two widely used tools, which helps understand the typical practices and experiences of cyberspace targeting. It surfaces muted experiences and critically examines the impact of dominant mental models on operational aggression in cyberspace. Through this, it provides an opportunity to critically examine accounts that subsume targeting in the wider cyber kill chain, while also locating the architectural affordances that shape the practices of targeting. As a corollary, this analysis highlights critical issues for the ethics of cyber targeting and provides actionable recommendations to improve these tools in an ethical and socially responsible manner.

1.8 Validation

The findings of this research are validated by a thorough analysis of primary sources from tool creators and users. These sources document lived experiences as first-hand accounts from their authors, which supports the assumption that they reflect at least part of how targeting is experienced. Furthermore, as the thesis builds theories from a thick description of tools and a close reading of primary sources, its epistemic value is derived from the internal consistency of its grounded theories.[9] The ultimate test is whether or not the theoretical findings can consistently explain the perceptual modalities of cyberspace targeting.

1.9 Limitations

This research is based on the analysis and thick description of two open source cybersecurity targeting tools. While it is acknowledged that cybersecurity practice happens in proprietary and secretive contexts too, the research resorted to the analysis of publicly available tools to ensure replicability and transparency. It is admitted that the present analysis of artefacts could be improved on by analysing practices through other means, such as participant observation. Participant observation could ensure a more comprehensive actor-network mapping, the integration of a larger number of primary

[9] It is standard practice in anthropology to generate a theory that provides an explanation for a local phenomenon, while not aiming to explain the same phenomenon across cultures, locales, or times. In contrast to inductive reasoning, this implies an abductive method of qualitative research [75], [76], [77], following the abductive traditions of anthropology, history and critical technology studies [78], [79]. Abduction does not aim to generalise its findings and acknowledges the possibility of diverging analyses for tools other than the analysed technologies.

accounts of targeting, and incidental observations about practice that may not have been documented in textual sources. Finally, the analysis of more tools could have broadened the perspective of the paper, potentially enriching its findings. Importantly, the primary aim of this research is to show that a study of perceptual modalities can provide valuable insight into the previously under-explored topic of cyberspace targeting.

1.10 Outline

This chapter has outlined the key analytic theories and methods of data collection, as well as the scope and limitations of the paper. It defined the issue and explained the research questions in light of the research gap.

Chapter 2 continues by reviewing key terminology and explaining the underlying theories of the paper. It discusses how modalities link to perception in the context of cyberspace, explaining the theoretical underpinnings of assemblage and actor-network theory as they relate to the literature on military and cyberspace targeting. Chapter 2 lays the theoretical foundations of the rest of the paper.

Chapter 3 reveals the findings of the paper, providing a thick description of two targeting tools and their corresponding modes of targeting. Through the analysis of Nmap, it discusses the emergence and structure of intelligence targeting, including its ontology and epistemic techniques. Subsequently, Burp Suite demonstrates how violent logics are engineered into targeting tools and how the rationale of predatory targeting inherits the epistemic tinkering of technoscientific rationality.

Chapter 4 interprets findings, explaining how the tools affect targeting practices and the experiences of violence in cyberspace. The chapter outlines the analytic framework that guided this research, with the potential to be replicated across other tools and contexts. Later sections highlight the practical implications of the findings about architectural biases and targeting practice. They identify key points for intervention in tool design and explain how targeting produces hidden violence. Chapter 4 closes with remarks on the design, operational, and ethical implications of the analysis.

The final chapter concludes the paper by outlining a possible generalisation of the findings and identifying room for future research.

2 Literature Review

The modalities of perception in offensive cyberspace operations define the practice and experience of targeting. The following literature review delineates a number of core concepts to avoid confusion about perceptual modalities. It also provides a background on the study of modalities and perception, delimits a method of analysing tools, and extracts insights from military studies on perception and targeting. Firstly, individual and contextual aspects of modalities are discussed, primarily borrowing insights from critical accounts of philosophy and neuroscience. This section is aimed at defining core terms, such as modality, perception, cognition and mental models. Second, actor-network theory and anti-essentialism are introduced to provide a methodical link between phenomenology and the study of tools. This section argues that tools can be studied as embedded systems in human environments and produce insight about the modalities they afford. Finally, studies of military targeting are discussed to understand the process of targeting, its technological evolution, and its violence in modern war. Ultimately, this chapter lays the theoretical and methodical foundations of later chapters that discuss the phenomenology of cyberspace tools through socio-technical systems of targeting.

2.1 Studies of Perception

2.1.1 Perception in Targeting

Perception influences targeting not only in the physical world but also in cyberspace. Perception is the process by which sensory information is organised and interpreted to make sense of the environment in which the sensor is located. Perception channels data through modalities to cognition, which is the mental process of acquiring knowledge about the world. This knowledge formation is dependent on both the data incoming from perception, as well as the modalities that shape and limit perception. Perception is related to cognition, but not necessarily to conscious experience. Consciousness is not a precondition for perceptual experience, since perception may occur even without the observer being conscious of the presence of the perceived object [80], [81].

2.1.2 Modalities

Modalities are the modes in which we experience the world, and perceptual modalities in particular are the modes in which subjects experience the world through sensation. The *modalities of targeting* are part of the epistemology of cyberspace targeteers through which they perceive their operating environment and generate knowledge about its targets. *Epistemic techniques* reveal how the practice and experience of targeteers are ordered by modalities, which are embedded in technologies. Such epistemic techniques include, for example, network scanning, which relies on technologies that enable communications over packet-switching digital networks. Because network scanning is a particular epistemic technique that generates a particular knowledge, the modal affordances of network scanning tools influence the knowledge generation of this mode of targeting. Since both epistemic techniques and perceptual modalities are *affordances* of targeting technologies, these tools influence the practice of targeting, including knowledge generation, manoeuvring and hiding. Such practice also produces harms and violence that mark the experience of targeting. In other words, targeting tools are proxies that help understand how modalities afford perception, and how that tool-shaped perception influences the practice and experience of targeting.

As perception depends on perceptual modalities, studying the modalities of targeting is fundamental to understanding targeting practice and experience. Generally speaking, perceptual modalities are the ways in which one experiences the world. Modalities in philosophy are understood as the ways in which something can be true or false, i.e. the ways of possibility and necessity [82]. This entails the study of logical conditions [83]. Linguistic accounts often study grammar and tense (‘tense-aspect modality’), as well as “qualifications of state of affairs” or utterances as modalities [84, p. 1]. In the present context, modalities are viewed as ways to experience the world as part of perception. Among the many perceptual modalities, sensory modalities are traditionally viewed as consisting of hearing, seeing, touching and more. These modalities restrict how subjects get access to the world, and therefore, influence their perceptions.

Modalities are, however, not simple or monolithic but often changing and variable, as history and anthropology have shown. This suggests that modalities may exist where the traditional five senses are not immediately apparent. Both historical and anthropological research point to how modalities can be studied alternatively. Sensory history, for

instance, studies perception as situated experience, seeking to uncover how humans of the past experienced, for example, hearing or smelling things [85]. This offers several advantages, revealing aspects of the past that would be missed otherwise and contributing to an "understand[ing of] people from the past on their own terms" [86, p. 419]. Thereby, historical research shows that modalities are chronologically atypical.

Anthropological research contributes to this by demonstrating that modalities are culturally and spatially variable. Recognising the Western cultural particularism of the 'five senses', anthropologists have shown that perceptual modalities go beyond the five senses [87]. In addition, they have used multimodal analysis to upset and diversify existing assumptions about perception [87]. They argued that the findings of a modal research depend on the modalities the research itself involves. This has prompted anthropologists to co-produce experiences through multimodality with their subjects [88], [89], [90], while also using alternative modalities to communicate through documentaries, exhibitions, and art [91], [92]. In summary, history and anthropology highlight the variability and complexity of perceptual experience. They encourage an exploration of perceptual modalities in targeting as situated experience.

2.1.3 Mental Imagery & Mental Models

What does a targeteer 'see' in cyberspace? To make the objects of perception somewhat less abstract, cyberspace operators have resorted to *mental models* to depict, improve, organise, transfer and operationalise their *mental images* of their targets and targeting environments. This affects how they organise and represent knowledge about their targets in so-called target ontologies, as well as how they generate knowledge via the use of epistemic techniques. Collectively, the processes and artefacts that generate and represent this system of knowledge are called the *episteme* of targeting. One such episteme in intelligence targeting is the network, which uses associations to create its target ontology, operationalises tools to gather information in, through and about networks, and uses mental models and corresponding mental images to represent knowledge visually as graphs. Therefore, the *episteme* of network scanning tools is the network. To understand how targeteers perceive cyberspace, one needs to understand how they form, revise and represent mental images through mental models.

Mental models are the primary means by which cyber operators synthesise their experience of cyberspace. They are structured representations of knowledge about the world that help individuals and communities understand and predict real-life events from inductive and abductive experience. While cybersecurity is teeming with mental models that structure the targeteer experience,[10] the forthcoming discussion focuses on mental models that form selected epistemes of targeting – networks and vulnerability signatures in particular. These mental models are representations of the perceptions of cyberspace operators of their targets and operating environments. Mental images serve as proxies to understand this perceptual experience [93]. Hence, to understand perception in cyberspace, mental images need to be understood, even as they are formed of non-physical objects. This is not logically impossible, as mental imagery is not bound to physical sensory experience. Mental images are often formed of objects in the world, even when direct external sensory input is unavailable. For example, "[i]f you close your eyes and visualize an apple, what you experience is mental imagery", writes Nanay [94], n.p.. Mental imagery often refers to "representations […] of sensory information without a direct external stimulus" [95, p. 590]. Thus, mental imagery is the part of human experience that cannot be captured by a characterisation of sensation [96]. This means that the study of mental images in cyberspace needs to explore perception beyond sensation. For example, mental images in cyberspace may include abstract models – like a network – and their visual representations – a corresponding graph – derived from data produced by the non-sensory modalities of cyberspace targeting. This complex of images, models and modalities is conceptualised as the *episteme* in Chapter 3.

2.1.4 Summary

This section has argued that perception influences cyberspace targeting, which can be studied through modalities. Modalities are the ways in which one experiences the world. Yet, because they are often changing and variable, they also contribute to the emergence of varied practices and experiences, which can be studied through mental models as the imprints of the mental imagery of cyberspace operators.

[10] Examples include the cyber kill chain, the unified cyber kill chain, the MITRE ATT&CK framework, and the Diamond Model.

2.2 Subjects, Objects, Agency

In a superficial definition, a subject can be said to be an agent who experiences the presence of another thing – an object – in their perceptual field. In this study, the targeteer is understood as a subject who perceives an object in cyberspace. Concomitantly, the object is anything the targeteer perceives as a metaphysical entity other than itself, or in a stricter sense, anything that the targeteer perceives as a target. However, since the present research relies on an analysis of tools for the identification of perceptual modalities, these non-human technologies need to be treated as subjects to understand their effects on perception. Without granting some agency to tools, it is impossible to understand how they shape, mediate and modify the human targeteer's perception. Therefore, tools are conceptualised as subjects in targeting because they construct and operate on a targeting ontology of non-physical, non-human and not-so-human objects – such as users, profiles, computer systems, network packets, and exploit payloads. Since agency is a requirement for subjectivity [97], it is a requirement for targeting tools as well. Therefore, targeting tools are conceptualised as non-human agents in order to be accepted as subjects.

Non-human objects can be perceived as agents because they participate in the production of agency in a relational and distributed way in so-called actor-networks. Initiated by Bruno Latour and Steve Woolgar in their ethnographic study of a biology lab in the United States, the researchers had shown how scientists and their testing and writing machines "began to take on the appearance of a system of literary inscription" as they co-produced scientific facts through particular practices of inscription [66, p. 52]. This research prompted Latour to illustrate his methodology of actor-network theory in his 1986 book, *Science in Action*. Based on his observations in *Laboratory Life*, Latour proposed to study science and technology always "in action" or "in the making", not as a product, but rather as a process of meaning-making and knowledge-production [98]. His method follows the production of science as a process, and maps the observed interactions between human and non-human actors in real-life settings [98]. Later, Latour clarified some of the tenets of this approach [67], four years after John Law's 1992 article on the core features and principles of the theory [99]. As Law explained:

> "[Actor-network theory is] a body of theoretical and empirical writing which treats social relations, including power and organization, as network effects. The

> theory is distinctive because it insists that networks are materially heterogeneous and argues that society and organization would not exist if they were simply social. Agents, texts, devices, architectures are all generated [i]n, form part of, and are essential to, the networks of the social. And in the first instance, all should be analyzed in the same terms" [99, p. 379].

Law aggregated the findings of actor-network theorists in the form of some core arguments. Firstly, he pointed to how these theorists conceptualised science as a social product of a highly social and political process [99, p. 381]. They suggest, in Law's account, that "the social is *nothing other than patterned networks of heterogeneous materials*" [99, p. 381] (emphasis in the original), in other words, the product of networked interactions between human and non-human things. Accordingly, Law summed, "the task of sociology is to characterise these networks in their heterogeneity, and explore how it is that they come to be patterned to generate effects like organizations, inequality and power" [99, p. 381]. He illustrates this with a vivid example:

> "For instance, I speak to you through a text, even though we will probably never meet. And to do that, I am tapping away at a computer keyboard. At any rate, our communication with one another is mediated by a network of objects – the computer, the paper, the printing press. And it is also mediated by networks of objects-and-people, such as the postal system. The argument is that these various networks participate in the social. They shape it. In some measure they help to overcome your reluctance to read my text. And (most crucially) they are necessary to the social relationship between author and reader" [99, p. 382].

Based on the methods of actor-network theory, and its insistence on the non-human object as an actor in the social production of knowledge, the present research also treats non-human tools that participate in the production of violent knowledges in targeting as networked agents with subjectivity.

2.3 Tools & Socio-Technical Systems

The forthcoming analysis of non-human actors and their networked relationships with human agents utilises the principles of systems science. This allows for an analysis of

targeting tools as parts of complex actor-networks of targeting with the primary function to produce useful knowledge for targeteers. As such, targeting tools are studied as components of knowledge systems, embedded in wider socio-technical systems of targeting. This section explains the key components and dynamics of these systems.

First, targeting tools participate in the knowledge production of targeting, while also enacting certain knowledges to do targeting. In other words, they are instantiations of *technologies* that perform *techné.* According to David E. Tabachnick:

> "While sometimes used interchangeably, episteme means 'scientific knowledge' and techne means 'technical knowledge'. Where episteme may be 'knowledge for the sake of knowledge', techne is instrumental or oriented towards the deliberate production of something" [100].

Techné, or technique, is knowledge to produce something particular, while technology – in the contemporary sense – is not more than the enactment of *techné* in complex assemblages of actor-networks. It is "making something into something it is not" [101]. Consequently, technologies produce things through techniques. When technologies are co-opted as in Latour and Woolgar's laboratory environment, they become parts of actor-networks that inscribe knowledge into artefacts, generating knowledge by the production of knowledge-carrying artefacts, such as scientific papers or notes. In this way, *techné* produces *epistemé,* which, in the context of targeting, manifests as techniques of targeting generate violent knowledges of practice and experience.

Tools are artefacts that implement some *techné.* In Tim Ingold's account, technique signifies "the embodied skills of human agents", while technologies comprise of "the operational principles embodied in the external apparatus of production" [102, p. 342]. Arguably, for him, the evolution of tools represents the "*objectification* of technique in the form of technology" [102, p. 342] (emphasis in the original). Following this line of thinking, the present research treats targeting tools as instantiations of targeting techniques that produce knowledges for targeting. A single tool can produce various *knowledges* because its calibration and positionality determine more than one system of knowledge (see in Chapter 3).

In addition to understanding them as knowledge producing systems, studying tools as systems can also contribute to an understanding of their emergence and behaviours,

which then produce particular perceptual modalities, targeting practice and experiences of targeting. According to Bousquet and Curtis, certain key concepts of complexity theory can aid a systems science approach to studying targeting [103]. In their reading, complexity theory benefits from system science's anti-reductionism – that the whole is merely the sum of its parts – and non-linearity – the idea that the disproportionality of input-output pairs in these complex systems are resistant to analysis [103, pp. 45-46]. They see these principles as justifications to introduce qualitative analysis into the analysis of systems [103, p. 46], and thus to introduce social science to the analysis of tools and technologies. They also recognise system science's move away from Newtonian homeostatic closure to open systems that "have boundaries that are porous and shifting, and exchange information and energy with their environment" [103, p. 47]. These open systems are contingent on their environments, evolve to learn, and adapt to survive [103, p. 47]. They also self-organise, whereby an autonomous choreography of low-level entities gives emergence to larger, more complex systems without a centralised authority [103, p. 47]. Accordingly, *anti-reductionism* cautions against the understanding of systems – such as the tool-target-targeteer triad – as simplex. It also prompts an *anti-essentialist* inquiry that recognises the study of technological effects as socio-political processes, and as such, understands tool and system design as the product of a cultural and political negotiation [104]. Along these lines, Matthew Ford, for example, shows, through the history of various British and American munition and small arm design communities, how the functionalities of weapons are shaped primarily not by their physical essence but rather by the interaction of various communities participating in the design process [105]. While this research concerns less the socio-*cultural* negotiation of tool design, it does concern the socio-*technical* construction of targeting ontologies and epistemologies in tool design.

In summary, *non-linearity* justifies qualitative approaches to analysing complex systems, while *open systems* and *self-organisation* explain at a high level why the actor-networks of targeting are contingent on their conditions of emergence, on practices of targeting, hiding and manoeuvre, and on the coupling of systems in modular tool architectures and complex operating procedures. These core concepts from system science and complexity theory, therefore, help explain the interactions, couplings, dependencies, co-produced effects and co-emergence of tools, targets and targeteers. In particular, as Chapter 3 illustrates, targeting tools interact with designers to construct

target ontologies as they co-emerge from the process of design, engineering and testing. They also couple with operator skills and knowledges to augment their respective shortcomings, while they use their co-produced effects to hide and manoeuvre around defenders and their defensive apparatus. In essence, then, cyberspace targeting is always co-emergent with and co-produced by targeteers, targeting tools, targets, and operating environments as these actors influence each other's perceptions.

2.4 Targeting

Targeting is a process of generating knowledge for intentional violence, materialised or not. Yet, since it relies on tools and target systems, targeting can be also analysed through systems science, specifically focusing on the structures and functionalities of targeting tools. Given the variability and complexity of targeting tools, targeting as a process is also highly varied. Therefore, a systems analysis of targeting tools, coupled with a qualitative analysis of the descriptions of targeting procedures and experiences, can be used to understand the phenomenon of targeting, specifically the practices and experiences it produces. For this purpose, this section reviews existing studies of targeting as a process, its material dependencies, and the violence it produces. The forthcoming chapter will elaborate on how tools produce specific processes, practices and experiences of targeting. It will argue that, ultimately, targeting is the practice of engineering violent knowledges and perceptual modalities into tools and operationalising them to produce experiences of violence in cyberspace.

2.4.1 Targeting as a Process

Targeting is described by Antoine Bousquet as the coalescence of perception with military effects [24], [106]. He describes 'the functional constituents of the martial gaze' as the steps of perception consisting of sensing, imaging and mapping. Following these steps of perception, Bousquet identifies aiming, ranging, tracking and guiding as the four 'successive orders of targeting' [106]. His tracing of these phases in the history of military technologies shows the historical expansion of the military's desire and ability to sense targets; record, disseminate, and interpret sensory data; and represent, orient and localise war in spatial terms relative to targets and targeteers [24, p. 18-19]. By highlighting the progressive rationalisation and mechanisation of targeting technologies – including perception – he shows how violence rooted in military

targeting becomes a planetary activity of hunting for predictable vulnerabilities [24, pp. 17, 191]. Thus, the study of targeting reveals a "visual faculty that is exhaustively solicited, augmented and incorporated within an array of sociotechnical assemblages of military violence" [106, p. 62]. Through the tools of sensation, imaging, mapping, and targeting, Bousquet shows how the perceptive functions of weapon systems reveal the violent logics of military perception. These functions transpire into less obviously violent technologies too, such as mundane network scanners and web crawlers, as this study argues.

Moreover, targeting reveals itself as a process as it extends various temporalities. Cyberspace targeting's temporalities resemble the 'operational time' of operational military targeting that Astrid H. M. Nordin and Dan Öberg identify [44]. Describing "the repetitive battle-rhythm of military targeting [...] no longer principally characterised by encounters through fighting [but through targeting]", they explain how war today is largely defined by how its objectives are translated to tactical gains [44, pp. 392-394]. As this translation happens through operational targeting, Nordin and Öberg explain it is no longer the target or the targeting effects that are critical to modern war, but the formation of "target-sets, target-systems or matrices" through the process of targeting [44, p. 404]. As a moral consequence, "the process subsumes all possible things as targets" and creates a form of targeting violence that is not based on exchange (of fires), but on the inclusion of targets in the processes and artefacts of targeting [44, p. 404].

Targeting as a process produces not only practices but also artefacts that shape how violence is produced in the modern battlespace. This is so partially due to the structural ideologies that drive automation [43], and partially due to the 'epistemic infrastructures' that incidentally arise from 'target practice' [107]. Rupert Barrett-Taylor argues that "war itself has become incidental to an obsession with managerialism" as datafication and algorithmic mediation chased a reductive "technocratic, process-obsessed managerial ideology" in targeting [43, p. 1]. He argues that these "digital technologies perpetuate an illusion of optimised warfare", which then claims to reduce the human cost of war despite its aggravated violence [43, p. 1]. Jutta Weber supports this claim by arguing that the US government's 'disposition matrix', its main kill list, ingrains a 'targeting methodology' in both targeting practice and its material artefacts [108]. She

points to how “computational actors make the messy targeting process more opaque and less traceable” by appealing to sanitised statistical calculations, database structures, and processing algorithms [108, p. 1]. According to Weber, these artefacts and the practices of targeting evoke the logic of technoscience and a culture of preemptive technosecurity that “actively shape the politics of targeted killing” [108, p. 1]. These ideologies – managerialism, technoscience, technosecurity – produce practices that derive from and inform how material artefacts are designed and operationalised in targeting.

2.4.2 The Materiality of Targeting

In addition to the ideologies of managerialism and technoscience that influence the process of targeting, material epistemic infrastructures also participate in targeting. Jon R. Lindsay was a participant observer anthropologist embedded with American special forces in Iraq between 2007 and 2008. In his study of special military operations, Lindsay uncovered how the affordances of the digital environment that surrounded US Navy SEAL operators and their support units had created ‘data friction’, which prompted a certain form of target practice [107]. For Lindsay, data friction denoted the annoyance caused by hard-to-use or malfunctioning information systems. For SEAL teams, it decelerated information flows, obscured provenance, and amplified a violent culture of ‘direct action’, in addition to downgrading more humanist approaches of civil-military cooperation. In this way, digital affordances contributed to the formation of an information ecosystem that favoured particular practices and logics of kinetic targeting. In this ecosystem, ‘epistemic infrastructures’ were part of the targeting apparatus of US SEAL teams and included computer workstations, files, PowerPoint presentations, and metadata, among others, which collectively amplified and directed a practice of violent targeting. With his work, Lindsay has shown how the materiality of targeting is inseparable from its tools and practices, even when much of targeting takes place in cyberspace. This finding prompts the current research to interrogate the materiality of targeting through the study of cyber tools, beyond an analysis of the processes and techniques that conventionally denote targeting.

Finally, Bousquet’s study of the trajectory of military perception in weapon systems illustrates how art and science co-produced military perception in, what can be deemed, early dual use technologies [24]. Easiest to understand, the use of vision as a perceptive modality is apparent in the military techniques of ranging, aiming and guiding of

physical weapon projectiles. Other less known techniques include photogrammetry, whose invention is attributed to the French military engineer Aimé Laussedat by Bousquet [24, p. 89]. Photogrammetry is the use of photographs to create maps of military terrains proportional to reality. These maps are then used to range weapons, while conformal maps enable aiming from large distances. It is not only vision, however, that acts as a modality of military perception. Through various acoustic and radiational tools, such as the sonar and the radar, militaries have been contracting other modalities in service of the 'martial gaze' [24, p. 138]. While the 'martial gaze' is semantically linked to vision, in Bousquet's account, it refers to the military's longing for a capability to sense, image, map and target its enemies through various modal configurations. In conclusion, Bousquet has shown not just that it is possible to study the modalities of perception in the practice of targeting, but also that these modalities are variable and bound to material artefacts.

2.4.3 The Violence of Targeting

It is not only the action taken as a result of targeting that can be considered harmful or violent, but also the process and actor-network of targeting as they enable violence. This violence is organised through an arrangement of logistical infrastructures that marshal tangible and intangible resources at the service of targeting. Critical to the logistics of military perception is the rationalisation of the martial gaze and the distancing of the moral agent from the dulls and dirt of war. Bousquet shows how the progressive rationalisation of military perception enabled increasingly inhumane targeting [24]. As Western militaries inherited the fascination of the Renaissance with measurement, this fascination later escalated into demoralised calculative logics of violence [24, p. 17]. As early battle plans of Italian gun-powder sieges merited from the drawings of Venetian architects, military acts of violence became sanitised of violence, while the lethality and perception have been brought ever closer to each other [24, ch. 1]. Supporting this theory, Malm's ethnography with the operational planning staff of the Swedish Armed Forces finds that bureaucratic and cultural conditions have "managed, suppressed and neutralised [military violence] through operational work" [109].

Besides these organisational and cultural conditions, however, technological innovation also assists the distancing of the moral agent from the sites of military violence. As Elish argues, the US Air Force's concept of 'remote split' – spatially separate but

virtually connected networks of human analysts and operators operating armed unmanned aerial vehicles abroad – represents this unison [27]. In Elish's explanation, with the distancing of combat from control, the US Air Force regiments "new forms of authorized evidence and expertise" that rely on both "an extensive network of humans and machines", as well as on human labour increasingly separated from war and the experience of warfighting [27, pp. 1103-4]. Essentially, Elish shows that socio-technical assemblages integrate minds, men and machines in a seamless web of co-constitutive parts that both distance and magnify human experiences in war.

Furthermore, the layers of perception in the modern battlespace also shape the sense of moral agency and degrade guardrails against moral prohibitions of killing [110]. Blackmore recalls that very early Nazi imagery of robotic aircraft directly led to the development of the V-1 and V-2 ballistic missiles [110, p. 196]. These missiles inherited the military's long-term dream of "automatic, programmable, and autonomous" killing that could exert precise violence without risking (one's own) soldiers' lives [110, p. 196]. Modern technologies, like artificial intelligence, also shape battlefield morality. Schwartz argues that the calculative logics of targeting transpire into contemporary military systems of artificial intelligence where complex moral decisions are reduced to technological calculations [111]. Therefore, the way in which the logistics of military perception is organised complicates the ethics behind the tools that rely on perceptive modalities. It is, thus, important to unfold the historical and socio-technical assemblages that contribute to the emergence of particular logics of military ethics. Understanding how dominant modes of perception couple with technologies in the cyber realm, therefore, leads to a more transparent understanding of the ethical issues behind cyber targeting.

2.5 Summary

Following early philosophies of phenomenology, modern advancements in psychology, neuroscience, and multi-modal historical and ethnographic studies have shown that perception depends on modalities. As these modalities are changing and variable, it is worth asking whether they generate particular mental images of targets in cyberspace. Arguing that they do, the above discussion suggested that mental images of

non-physical objects leave their imprint on the mental models of cyberspace targeteers, as part of the knowledge producing practices of targeting.

To conceptualise targeting tools and non-physical targets in cyberspace, it has been argued that non-human objects can be conceived of as actors. Using the theory and method of mapping actor-networks, these actors can be better understood as agents in the social production of knowledges. These non-human actors are best analysed as systems that interact, couple, and co-emerge with human roles and actors, while co-producing the violent effects of targeting. Surfacing some selected principles of complexity theory, it has been argued that non-linearity and self-organisation explain how and why non-human actors, like targeting tools, become agents in producing the perceptual modalities, practices and experiences of cyberspace targeting.

Finally, targeting as a historically changing temporal process and material practice has been reviewed. This established that targeting as a process and experience is not universal, and that targeting engineers and operationalises violent knowledges through tools. These tools reproduce particular perceptual modalities that rationalise violence, distance the operator from their own violent effects, and ingrain violence in tools of professional practice. Collectively, the literature review has shown that targeting tools are non-human actants that have the capacity to carry and produce violent knowledges and practices of cyberspace targeting. The following chapter shows how this actually proves to be the case.

3 Findings

3.1 Intelligence Targeting

3.1.1 Nmap as a Paradigmatic Tool of Targeting

In order to understand targeting as a process, system, and modality, this section analyses a popular network scanning tool, Nmap. Nmap is a software that identifies computer systems on computer networks by manipulating network packet headers. The tool was first released on September 1, 1997 by its designer Gordon Lyon and has been a popular tool ever since [112], [113]. It is a tool that reflects and constitutes the practice of cyberspace targeting, therefore, it reveals its modalities and manoeuvres. Through conceptualising Nmap as an actor in various actor-networks, it is argued that Nmap co-constitutes its targeting environment with its designer and user, while altering the perception of its users. This conceptualisation helps understanding Nmap's target ontology and its targeting practice. This analysis provides not only insight into how Nmap works, but also into the life world of offensive cyberspace operators, as well as into defensive practices that arise from the violent logics of cyberspace targeting.

The analysis is based on Nmap's online documentation as of March 10-11, 2026, presented on the Nmap website (nmap.org/book). This documentation can be used to unearth the discourses, logics and practices of targeting because it is produced by the tool's designer, who is its user in one person. This author presents historical narratives, personal recollections, design rationales, real-world use cases, and designer-authored tips and tricks, making the documentation a primary source. Additionally, the documentation is ostensibly aimed at educating other users, and thus, also acts as a discursive artefact that represents knowledge. Analysing this artefact allows for an understanding of how Nmap functions and what its operators experience while using it.

3.1.2 Nmap as a System

Analysing Nmap as a system of interconnected features allows for setting a common vocabulary when defining and relating Nmap's affordances. As a tool of intelligence targeting, Nmap's features revolve around its function to perceive confidential information and to manoeuvre in cyberspace. The options that afford the operator to manoeuvre in cyberspace allow it to orient Nmap toward targets, define its speed of operation, set its manner of approach, while calibrating its deceptive capabilities. This creates the positionality that the tool requires to perceive its targets and evade defences. Additionally, Nmap specifies its targets via command-line arguments, as "[e]verything on the Nmap command-line that isn't an option (or option argument) is treated as a target host specification" [114]. These arguments define the target ontology of the tool. Collectively, the calibration and target specification features of Nmap fine-tune the violence intelligence targeting. While these features are simple, the process of targeting is more complex.

3.1.3 Nmap's Process of Targeting & Target Ontology

The Nmap documentation defines an iterative sequence of steps that an operator is recommended to take during targeting [115]. Nmap targeting starts with a human-defined seed list – a list of targets that must be correctly formatted. Providing the seed list of targets is inherently the task of the human who limits the scope of targeting in order to reduce the effects of the tool's automatic violence, as well as to save resources during targeting. The exact scope is defined by the users the tool caters for. For example, network administrators, penetration testers, and offensive operators seek different levels of damage and efficiency, and hence they calibrate the tool differently [116].

The first step of calibration comes with target selection, which includes verifying the seed list of targets. In the words of the author, "Nmap automates many aspects of network scanning, but you still must tell it which networks to scan" [115]. While target specification may include Internet Protocol (IP) addresses and Classless Inter-Domain Routing (CIDR) notation, the documentation suggests that "[i]n many cases" operators are given a list of domain names belonging to a "company" [115]. This is because targeting often starts with the awareness not of networks but of organisations. Because

Nmap is incapable of recognising social targets according to its target ontology (see Section 3.1.4), it needs a human to translate the social rationale of targeting into machine-readable target lists. This translation – or verification – presumes authoritative knowledge at the initialisation of targeting, which begins when the human operator verifies the seed list. This step of target selection defines legitimate targets as, for example, organisations. Given that the tool's architecture prevents it from recognising organisations as targets on the command-line, human assistance is needed to traverse, what is termed here, 'targeting domains'. These domains refer to specific target ontologies and corresponding epistemologies, or collectively: the targeting domain's episteme. For example, the target ontology of Nmap consists of strictly four types of entities: domain names, IP addresses, port numbers, and CIDR notations. Nmap uses various epistemic techniques, including numerous scanning methods to produce knowledge about these targets. While an organisation is admittedly a possible target of offensive cyberspace operations, it is not recognised by Nmap, and thus, it falls outside of its targeting domain. In the case of a company, Nmap is blind because of its target ontology, only capable of perceiving IP addresses, ports and networks but not an organisation. Therefore, the tool needs the *techné* – the knowledge to do – of the human operator to verify its seed list. This techné is essentially one of targeting domain traversal, where a set of ontology and epistemology is used to generate seeds for another. This is necessitated by the tool's perceptual architecture, which engineers a certain logic of targeting into the tool.

Nmap itself performs certain limited forms of boundary traversal when it shifts its perception from host-based targets to ports or applications. These shifts are qualitatively different as they recognise entity types and enlist epistemic techniques different from the preceding targeting domain. In other words, Nmap defines sub-domains for its main targeting domain. In the first layer, the tool scans hosts identified by IP addresses, while in the following stages it looks for ports and applications based on port numbers and application names, respectively.

Nmap starts mapping the network by identifying *active* hosts, which is a universal qualifier in Nmap's target ontology: inactive hosts are not targets. In a way that defines the ontology, Nmap's recognition of targets is defined by its epistemology. This epistemology contains a list of techniques that can send, receive and manipulate packets

and display the results on the command-line interface in textual format. Because the modality of Nmap's targeting is packet-based, the epistemology of Nmap is constituted of techniques that elicit responses from targets. Because of this, Nmap recognises only entities that are responsive to the sending of network packets.

Once Nmap finishes targeting hosts, it shifts to its second sub-domain. This sub-domain recognises four port 'states': open, closed, open|filtered, closed|filtered [117], and uses the episteme of port scanning. "Ports are simply a software abstraction, used to distinguish between communication channels. Similar to the way IP addresses are used to identify machines on networks, ports identify specific applications in use on a single machine" [117]. The episteme of port scanning consists of knowledge of so-called port 'states' and the epistemic techniques that help determine those states. They are based on network protocols that are inherent to packet-switching network communications, affording Nmap to read port states from packet headers.

The Nmap documentation notes that the "most interesting" ports are open ports: the ones that are accessible ("active") and connected ("listening"). While in the case of host scanning, responsiveness is the qualifier of target selection, in port scanning, ports have to be connected too. A port is connected ("listening") when an application is assigned to the port on a host system. Port states form a hierarchy of value based on accessibility and connectivity. Accessible ports – 'open' ports – provide (near-)certain information about the application residing behind them. 'Closed' ports, in turn, reveal that the port is accessible but does not connect to an application on the host. Open ports are ultimately valuable because they provide a gateway to potentially vulnerable applications and do not obstruct communication with compromised systems. Their value is derived from their accessibility and connectivity. Closed ports show that the queried host is online and provide some information for yet another sub-domain that aims to gather information about Operating System configurations ('OS detection'). Closed ports are accessible but cannot provide connection at the moment of scanning. The documentation notes, however, that this might change with time: closed ports may be opened. It recommends periodically returning to port-scanning these closed ports. This shifted temporality in which actual non-recognition lives synchronously with the potential of future targeting is a feature of anticipatory targeting, which both the literature and the section on predatory targeting later critique.

The third and fourth port states are called ‘filtered’ and ‘unfiltered’. They require specialised techniques to elicit information about the target. When detected, both states suggest interference with the transmission channel, describing the probability of accessing or connecting to a target port. They “frustrate attackers because they provide so little information” [117], forcing Nmap to “retry several times just in case” [117]. While the almost zero information emitted from filtered ports suggests human interference, unfiltered ports are often identified by protocol affordances that emit some information. These ports require specialised techniques, including “other scan types such as Window scan, SYN scan, or FIN scan [that] may help resolve whether the port is open” [117]. The qualitative difference between filtered and unfiltered ports, thus, is their level of information emission. Since information can be elicited from unfiltered ports only through alternative scan types, these scan types are alternative targeting modalities that allow for the recognition of previously unperceived targets. Therefore, the modalities of Nmap are identical with its scanning techniques. Given that scans are differentiated by the configurations of network protocol packet fragments they send, by extension, the targeting modalities of network scanning tools are identical with their techniques of packet manipulation.

3.1.4 Nmap’s Target Epistemology

As packet manipulation is the unique targeting modality of network scanning tools, it is instructive to analyse the targeting rationale of these tools too. Targeting rationale stands for the reasons behind certain operational and design choices that constrain the ontology and epistemology of targeting in a given targeting domain. This section discusses how the epistemology of targeting appears, in other words, what modalities are operationalised in tools. Because there are multiple targeting rationales co-habiting a single tool and its operational context, multiple modalities necessarily imply that a targeting tool has not a single epistemic system, but a system of systems. This complex, nested system of rationales is dubbed by critical theorists as the logics of targeting – the plural form highlighting the multiplicity of reasons that go into the design choices and battlefield effects of operational targeting tools. It follows that Nmap’s logics of targeting are multivariate: consisting of various ontic and epistemic systems.

The environment of Nmap features a set of epistemic conditions in which targeting is always characterised by some level of uncertainty. The easiest point to understand

Nmap's experience of uncertainty is to review how it defines 'filtered' and 'unfiltered' port states. These genotypes of ports signify moments when Nmap is unsure about whether a target port is 'open' or 'closed'. 'Filtered' and 'unfiltered' ports both reveal information about targets, indicating with equal or nearly equal probability that a port is open or closed. In essence, a scan that results in a verdict of open and closed ports is a scan that carries knowledge with the numerical probability value of 1 (certainty). Results of filtered and unfiltered ports then indicate an undetermined port state, and thus, the probability of knowledge about the state is near half of certainty, which effectively translates to equal probability or indistinguishability. This means that in the probabilistic world of cyberspace targeting, knowledge is a product of abductive reasoning. Consequently, any view that propagates an objective deterministic perception of targets in cyberspace must contend with the fact that knowledge derived from targeting is probabilistic.

Another way to evidence Nmap's lack of confidence about port states is to recall its recurring theme of characterising networking filtering (the assumed environmental causes of filter/unfiltered port states) as noise [118]. Noise in information science "represents the randomness or uncertainty in a signal through which information is transmitted" [119, p. 106]. Therefore, noise is inherently tied to some level of uncertainty. The fact that Nmap perceives network filters as noise reveals its frustration with the uncertainty they create for its port scanning modality. Uncertainty is, thus, the epistemic condition of targeting because it is partially induced by environmental factors outside the control of the targeteer or the tool. Consequently, the game of the targeteer is always about increasing their sense of certainty by repositioning themselves in their environs.

Nmap's targeting modalities are greatly determined by the tool's positionality. The six port states that Nmap recognises are not intrinsic properties or necessary emissions of the targets, but are the results of "how Nmap sees them" [117], in other words, of Nmap's targeting modalities. For instance, the documentation notes, Nmap determines different states depending on where it scans the target network from and how it is calibrated [117], [120]. This "demonstrates that what we are calling a port state is not solely a property of the port itself [sic]; [it] only reflects what Nmap saw when running from a particular machine, with a defined set of options, at the given time" [118]. Port

states are thus not facts, but perspectives. They completely depend on the positionality, modality and calibration of a targeting tool. This positionality is partially deterministic, but due to its complexity largely unpredictable. This unpredictability is what the probability calculus of Nmap tries to resolve with the introduction of additional port states, effectively making them phenotypes – genotypes instantiated by their environs. These port states beyond open and closed reveal information about the targeting environment. Consequently, how Nmap produces knowledge about its environment and to what extent its targeting modalities are functional depend on its positionality. In the space of a targeting domain that is conceptualised as non-physical, positionality assumes relative qualities. These qualities can be best studied through abstract terms, such as those provided by network science.

3.1.5 Nmap's Target Episteme: The Network

Antoine Bousquet notes that targets need to be localised in space-time for the martial gaze to acquire full sight of the targets while rationally calculating avenues of approach [24, p. 120]. Without 'fixing' targets in a known grid of reference, militaries cannot guide projectiles to their targets. Similarly, in cyberspace, targeteers need to locate their targets in a referential system. For this purpose, cyberspace targeting has historically chosen to enroll the discipline of network science, where spatial measures are less defining. A network-based epistemology equips Nmap with the tools to measure accessibility and connectivity without recognising spatial properties. Accessibility is tied to the modality of packet-based communications, while connectivity is mapped by means of studying networked targets. For Nmap, networks define the underlying target ontology of the tool, its core modalities of targeting, its manoeuvres and even its logic of targeting. Collectively, they and the conceptual model of the network define the perceptual field of Nmap. Therefore, studying how networks are imagined, explored, and utilised by the tool is a means to understand the network-based paradigm of intelligence targeting.

The reductive nature of Nmap's network image generates a perceptual field that relies on and re-creates a particular representation of the world as a network. Nmap defines networks based on hosts, where nodes are computers connected by edges that represent open communication channels. Because of its network-based epistemology and host-based ontology, Nmap perceives only responsive hosts on a computer network.

This means, if a computer is completely inactive on a path in a local network of computers, it does not respond to Nmap scans, and thus, is not mapped by Nmap as part of the network. Hence, Nmap's field of vision can be described by the networks it is able to scan. This highlights the perceptual limitations of network packet-based modalities, differentiating Nmap from other targeting tools whose targeting domains span socio-technical networks.[11] The packet-based modality also restricts Nmap's image of the network since it relies exclusively on a particular concept of adjacency to image its surroundings. Adjacency in IPv4 networks determines if a node is reachable from another node. In Nmap's universe, adjacency refers to the ability to scan a range of IP addresses that share the same leading bits, using CIDR notation [116]. It focuses on IP address similarity rather than physical or logical proximity. This means that Nmap's mental image of the network is radically different from other alternatives. Consequently, Nmap's conception of adjacency, which is derived from its response-based modality and host-based episteme, defines its image of the target. By highlighting Nmap's restrictive and restricted perceptual field, one can appreciate how particular mental models restrict perception. To understand how these restrictions are engineered into code, one needs to appreciate the socio-technical conditions from which targeting tools emerge.

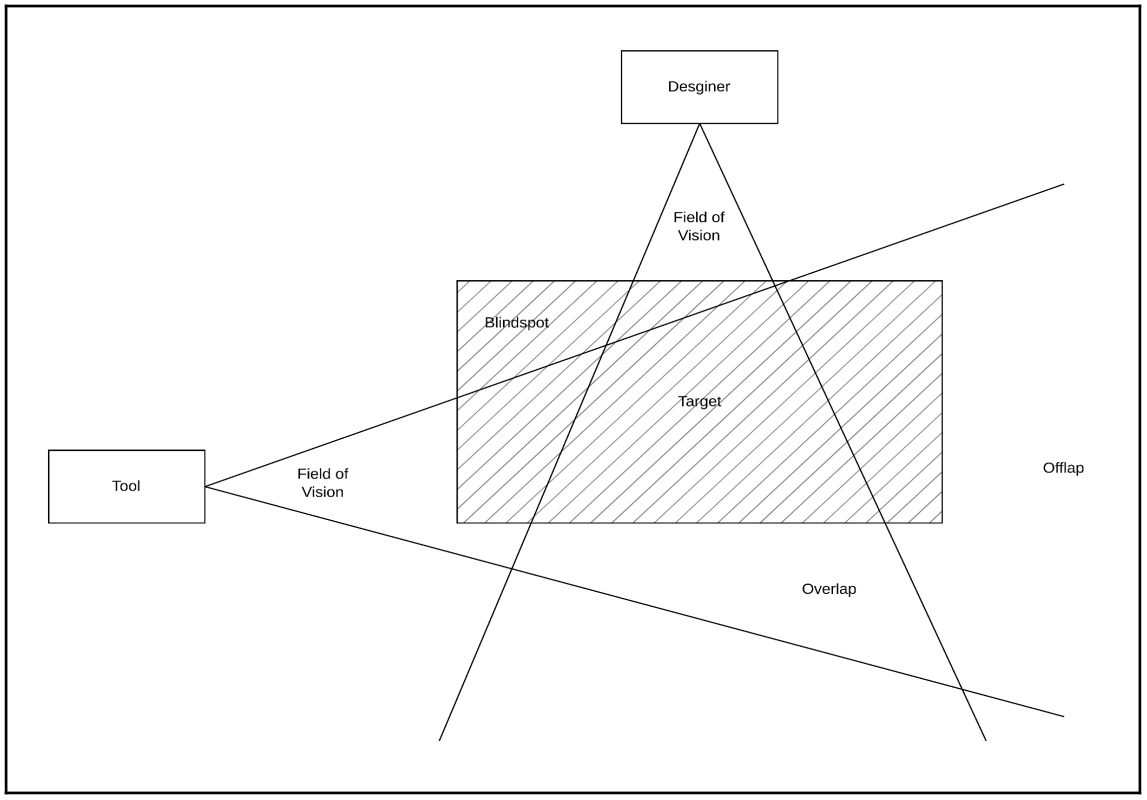
3.1.6 The Socio-Technical Construction of Targeting

Antoine Bousquet notes the inherent role of architects as perspectival engineers in the genesis of modern targeting [24]. Early Renaissance military engineers relied on the drawings and studies of architects to understand the disposition of objects in three dimensional space. To operationalise this knowledge, these engineers devised – in collaboration with architects – devices to formalise the calculable aspects of space in mathematical representations [24]. This mathematicisation was necessitated by the technological developments of 16th-century warfare. As long-range guns appeared in the battlefields of Italy, the men of the Renaissance needed a technique to calculate the optimal location of long-range weapons relative to a target. The technique that emerged relied on the geometric combination of ranging and measuring perspective, which enabled the mapping of targets in relation to other known objects. As a core feature, perspective emerged as an indispensable piece of information in modern warfare.

[11] Consider tools that are capable of identifying and differentiating other types of target nodes, such as social media profiles or physical structures.

Perspective helps explain how the perceptual fields of targeting tools emerge, as Nmap appropriates the lineage of perspectival weapons at the cognitive level. At the level of cognition, both the designer and the tool-in-the-making have a vantage point, or perspective. Both are treated as correlated actors, despite their in-the-moment co-emergence. (Tool emerges as the designer designs, while the designer emerges as a distinct persona only as the tool materialises.) In this setup, the tool, the designer and a target are positioned relative to each other. To use the metaphors of the visual sensorium, they see each other from their own vantage points. The two subjects (tool and designer) perceive their object (the target) from their own unique perspectives. In the visual metaphor, their fields of vision are defined by the angular lines of their perspectives and the distance of the horizon. The three together – two lines and the horizon – construe a slice, which is equal to the corresponding actor's 'field of vision'. Occasionally, as both are directed at the target, these slices will intersect, forming an *overlap*, and disjoin in an *offlap*. In the overlap, both perceive the target, while in the offlap, only one does. In this way, the tool and designer couple their perspectives to complement and reinforce each other about their shared recognition of the target.

Figure 1 – Illustration of the Social-Construction of Nmap's Target Ontology



Given an overlap, if a target is detected, the tool and designer reinforce their knowledge of the target. However, when an offlap occurs, the two actors come into conflict: one perceives an object where the other perceives nothing. This difference either produces new knowledge for one party by introducing a new entity into the common field of vision (the union of the two sets), or uses the superior power of one actor to force the other into excluding the new entity from the common field of vision. Effectively, disagreement coupled with power imbalance creates a bias. If the bias is introduced by the designer to the tool, we speak of a human bias. If the bias is introduced by the tool to the designer, it is a case of architectural bias. To illustrate this, imagine that, in the process of engineering Nmap, the designer fails to implement a new functionality to distinguish ports from each other – for whatever reason. Because the tool cannot perceive the difference between ports, the designer also excludes it from its field of vision during the design and while using the tool. In this way, the architecture of the tool introduces a bias to the human's cognition. In the other – easier – case, the human designer simply decides not to gather information about domain names, and thus, exclude domain names as legitimate targets. In the consequent code, domain names will not be recognised as acceptable values and thus will be rejected by the tool.

Finally, given the two-dimensionality of the visual metaphor, a third option alongside overlap and offlap can occur. In this case, both fields of vision miss part of their environment, including possibly parts or the whole of their target. If this is the case, a blindspot is introduced and otherwise valid entities in space will be set for non-recognition. Here, it is important to recognise the temporality of the ontology-construction: once the ontology is constructed – once entities are accepted and rejected for recognition – it is not changed for that given state of the ontology. Putting it differently, an unlearning system will not adapt to its changing target set and horizon because architectural and human biases limit its field of vision.

The presented visual metaphor explains how the alignment of fields of vision produces restrictive design decisions and how misalignment reinforces human and architectural biases, including blindspots. Because in all these configurations, the model produces omissions, the modalities of socio-technical targeting will always produce biased targeting domains.

3.1.7 The Violence of Intelligence Targeting

Nmap's network-based episteme and architectural biases aggravate its violence against subjectivity – the process of individuation and socialisation, or in other words, how one emerges as distinct from but related to their environments. Nmap's particular image of the network enacts violent modes of targeting by reducing complex objects into nodes and edges, or where this is not possible, erasing them completely from the targeteer's field of vision. Both harm the targeteer, because they deprive her of information that could be useful for targeting. In addition, the same acts of reduction and elimination harm targets too, as they become uniformly targetable despite their otherwise meaningful differences. Nmap violates the integrity of its targets by erasing some of their relationships or erasing objects from the targeting space. They also prevent the target from relating itself to illegitimate targets, thereby making itself illegitimate for targeting as well. For example, a database can be seen as a legitimate target, unless it is identified by its relation to a hospital. This illustrates how the erasure of real-world associations in an abstract episteme can result in violence.

3.1.8 Cyberspace Manoeuvres: Subversion, Mimicry, Distortion

For Nmap, manoeuvres in cyberspace are necessitated by defensive tooling that could potentially compromise the stealth of its operations. One such tool is the intrusion detection system (IDS), capable of countering Nmap's targeting modalities and shaping its offensive behavior by manipulating packets that Nmap uses to infer information about its targets. For example, by spoofing packets, IDS can mislead Nmap to think that certain ports are closed when in fact they are open.[12] For this reason, it is critical for a tool of intelligence targeting to identify defensive tooling and evade them via manoeuvres.

[12] Linux *iptables* is an example of a defensive tool that manipulates the environmental affordances of an ordered cyberspace to deceive Nmap-like targeteers. *Iptables* can forge TCP reset (RST) packets to claim ports are closed, and thus deceive Nmap's port-scanning. As a reminder, Nmap's port-based targeting sub-domain recognises six port states, of which the 'closed' type is returned when Nmap receives reset (RST) packets from its targets. This tells the tool the application is accessible but unconnectable, and thus, unworthy of targeting. However, when RST is returned by a deceptive firewall, like *iptables*, the case is not that the application is unreachable, but that it will not service Nmap due to firewall rules. In this theatre of deception, the firewall forges a packet at the level of Nmap's core episteme. Nmap's epistemology, its modes and means of targeting rely on packet-based network communications. Because this mode of communication stores information in packets, it allows Nmap to read and manipulate packets, and thus, infer knowledge about its targets. The ability to read and manipulate packets is the affordance of the regulatory regime of TCP/IP networking.

Nmap identifies IDS by flagging anomalous nodes on a network edge. Because IDS typically sit on the only path between the scanner and many internal hosts, Nmap treats them as high-betweenness nodes and looks for anomalous response patterns to infer how many hosts lie behind them. Drawing on network-science expectations for scale-free networks (cf. [121], [122], [123]), Nmap flags responses that deviate from statistical norms. Detecting these anomalies lets the tool identify the IDS or firewall for what it is, enabling intelligence-driven manoeuvre in the subsequent phases of targeting.

When it comes to manoeuvre, Nmap offers two categories of techniques to "subvert" IDS's perceptual field [124]. The first category includes slowing scanning, evading known IDS rules, and avoiding "easily detected Nmap features" [124]. These techniques mimic the behaviour of 'normal' hosts.[13] In essence, these techniques hide Nmap's approach by reducing emitted signals, making it appear as other benign objects. The second set of techniques confuses the IDS through distortion, by altering Nmap's observable shape on the network. [14] By scattering probes, the tool makes itself appear originating from a multitude of networks. This alters the single-node shape an IDS would expect from a scanner, confusing its perception and evading its defences. Specifically, this happens through decoys, proxying, scattering probes, and fragmenting packets. Decoys and proxies allow the tool-operator complex to blend into network communication noise. Because "Nmap can construct a scan that appears to be coming from dozens of hosts across the world" [124], it appears as any legitimate source. Scattering probes and fragmenting packets achieve a similar effect by manipulating packets at the session level instead of the network layer. Finally, some techniques combine mimicry and distortion by appearing as a multitude of 'normal' hosts. Spoofing manipulates outbound packet source IPs to confuse the IDS, by "framing innocent parties, casting doubt in the administrator's mind about the accuracy of his IDS" [124]. Idle scans and DNS proxies, in turn, route requests through other machines, expanding on spoofing by allowing Nmap to receive responses.

[13] Mimicry is the evolutionary behaviour of a system that by time becomes closely resemblant of another system. It is commonly observed in nature where, for example, certain butterfly species grow wing-features that mimic other unpleasant prey of their predators. Once the predator experiences displeasure with the mimicked prey, it stops attacking the mimicker as well [134].

[14] Shape in topology refers to the spatial arrangement of a network's nodes when those nodes are mapped onto a geometric space [125]. As many IDS rules expect scanners to have a single-node shape, scanners can evade detection by altering their network shape. This means changing which nodes appear active and how they are distributed (for example, making probes appear to come from many dispersed hosts rather than one source).

The effectiveness of these manoeuvres relies on how well they can appropriate the perceptual modalities of the defensive apparatus. For Nmap and the IDS, the modalities of targeting involve the ability to read and manipulate network packet headers. The IDS catches or confuses Nmap by inspecting network packet headers, while Nmap uses the same headers to infer information about its targets and subvert the IDS. Both mimicry and distortion are part of this packet manipulation paradigm. Therefore, subversion techniques and defensive systems appropriate the perceptual modalities of each other, generating momentary, positional experience of targeting and evolving images of targets. Perceptual modalities of targeting, therefore, co-create targeting practices and experiences through offence-defence interactions. This interaction is discussed in the following section.

3.1.9 Producing Knowledge Through Targeting

The offence-defence interactions of intelligence targeting define the political economy of cybersecurity with respect to targeting. This economy is characterised by the circular production of offensive knowledge, its appropriation for defensive purposes, and its re-appropriation by offence again. Effectively, intelligence targeting can be understood as an economy of knowledge production and exchange, where offensive targeting is legitimised as necessary in a calculative logic defensive adversary emulation.

Nmap justifies its offensive applicability by depicting itself as an agent of defence by translating offensive practices into defensive knowledge. It proposes to interpret offensive capability as useful knowledge for defensive purposes, practicing adversity temporarily and with limitations to adopt the offender's framework of violence while gaining defensive knowledge.

> "One of the best methods of understanding your network security posture is to try to defeat it. Place yourself in the mind-set of an attacker and deploy techniques [sic] against your networks" [126].

At a meta level, appropriating the knowledge of a targeting tool, or its accompanying adversarial practices, requires appropriating the ontologies and epistemologies inherent in adversary ecosystems. Because these ecosystems possess numerous biases and blindspots, they also transmit some of this negative baggage to the defenders. This perpetuates the violent logics of targeting by transmitting violent ontologies and

epistemologies into defence. For example, using Nmap to scan networks commits to a recognition of legitimate targets defined by Nmap. It forces the benevolent scanner to see the world through Nmap's perceptual field, ignoring what Nmap would ignore. Hence, the knowledge exchanges of cybersecurity trade knowledge at the cost of unrecognised violence. This exchange fundamentally defines the political economy of cybersecurity as it intertwines knowledge production with the practices of targeting, the requirements of vigilant cyber defence, and the design of tools.

Tools that defend against intelligence targeting appropriate the latter's modalities to deceive the targeteer. The techniques of defensive deception are the results of appropriating adversarial knowledges, as engineers effectively co-opt the episteme of the adversary to design defensive tooling. For example, they study how Nmap detects port states and design their systems to deceive these scans. In turn, when Nmap's designer integrates the analytic results of its scans against new IDS rules to evade them, they appropriate the knowledge of defence and co-opt its modalities to counteract its perceptual field. In this vein, targeting violence is co-produced and mutually experienced by both tools, while mimicry appears as a transactional and co-dependent phase of tool design. In this circular system of feedback and learning, an ecosystem of contending tools and techniques emerges to constitute targeting in the ecology of cybersecurity. Importantly, because of their co-dependence and mutually deceptive practices, both offenders and defenders rely on each others' knowledges in a concert that enacts practices of targeting, as well as additional security practices. These include a calculative logic of cyber defence, which aims to reduce risk by reducing threat exposures. This calculus commonly involves the so-called 'attack surface', the net of opportunities where successful attacks are expected from. A common way to do this is to patch vulnerable systems and eliminate unnecessary applications, thereby reducing a system's attack surface. When Nmap aids this, it performs security practices that aim to recognise outliers, which Muller has noted is the primary driver to practice vigilance in cybersecurity [127]. When Nmap is used to recognise outliers, it becomes an apparatus of vigilance, and in one, a means to practice cyber defence. This means security practice becomes performative and iterative, inseparably intertwined with practices of targeting. Theorising the drivers behind this practice – such as the proposed calculative logic – offers an opportunity to ground practices in tools, like Nmap, that embody and operationalise that calculus. For example, by flagging anomalous hosts and behaviours,

Nmap converts intelligence targeting into remediation, making scanning a routine practice of vigilance. Therefore, appropriated knowledge is not merely a copy of adversary knowledge, but a new form of knowledge that is coupled with defensive concepts at its core. For example, a standard penetration testing report, although listing key offensive actions, qualifies for a defensive artefact because it contains countermeasures, recommendations, or patchable vulnerabilities. This means that even when defenders appropriate adversary information, they produce a different kind of knowledge, using distinct methods and pursuing different goals. Consequently, defensive knowledge production may produce outputs that are harder for offenders to repurpose, while also shaping offensive tactics by informing defensive design. This creates incentives for offenders to innovate stealth and deception to counter newly informed defences. The political economy of knowledge production and exchange explains how defence and targeting co-produce cybersecurity.

3.1.10 Summary

The analysis of Nmap established it as a paradigmatic tool of intelligence targeting that functions not merely as a passive instrument but as an active socio-technical actor that co-constitutes the environment of cyberspace targeting. Nmap operationalises a specific network-themed episteme and a target epistemology that relies on the ability to manipulate network packet headers. Its target ontology recognises four types of targets and qualifies them based on responsiveness, connectivity and accessibility. This makes the target ontology restricted to hosts, ports, and networks, rendering social entities like organisations invisible unless translated by a human operator through the practice of ‘domain traversal’. Nmap’s episteme enforces a circular logic where only responsive entities are recognised, perpetuating biases and blindspots that filter and reduce complex social realities to abstractions. These shortcomings are introduced during the construction of targeting tools, where the ‘martial gaze’ is engineered through the alignment of designer intent and tool affordances into targeting. This limits the perceptual field of the tool and the targeteer and produces various manoeuvring tactics that aim to subvert defensive logics. As the choreography of offence-defence unfolds, the practice of targeting becomes increasingly entangled with inimical knowledge exchanges. This political economy enacts a form of violence that dissolves subjectivity

and frames the acquisition of knowledge through targeting as necessary for the production of security.

3.2 Predatory Targeting

3.2.1 Predatory Targeting as a Process

A successive order of intelligence targeting is predatory targeting, which uses the knowledge generated by intelligence targeting to compromise the integrity or availability of computer systems.[15] Although the aim of targeting is ultimately to compromise a system, in the present working definition, targeting ends when compromise begins.[16] On the 'cyber kill chain' [127], [128], predatory targeting spans reconnaissance, weaponisation and delivery, although the kill chain itself would assume each step to break away from the activities of the previous step. The kill chain, thus, effectively removes perception from the phases of targeting following reconnaissance. This is a misleading characterisation of cyberspace targeting, which, from reconnaissance to delivery, involves certain perceptive modalities transient to these phases. Therefore, this study does not isolate perception or targeting to reconnaissance only.

3.2.2 Burp Suite & The Web Application Hacker's Handbook

The following analysis of predatory targeting concerns the structure, targeting domain, target ontology, modes and logics of targeting, and its violence through an analysis of a popular web application penetration testing tool, Burp Suite.[17] Burp Suite is a computer software with a graphical user interface that allows for the mapping and testing of web applications from the client side. It is composed of several modules that specialise on different aspects of targeting a web application. Burp Scanner, for example, lets its user retrieve content from websites [129], while Burp Intercept captures hypertext transport protocol (HTTP) packets [130]. Burp Intruder is another module that manipulates these packets semi-automatically to perform various 'attacks' at scale [131]. Collectively, these modules enable web application mapping and testing, supporting Burp Suite's

[15] Intelligence targeting does not involve the compromise of security controls that are aimed at ensuring the confidentiality of information. For example, decrypting an encrypted file would not be part of intelligence targeting, as its main purpose is not the identification of targets but the breach of confidential information.

[16] These targeting functions resemble the successive orders of targeting Antoine Bousquet describes as aiming, ranging, tracking and guiding [108].

[17] For the present analysis, Burp Suite's Community Edition was used, which excludes modules and functionalities that the Pro version offers.

claim for being "[t]he most widely used web application security testing software" [132].

In addition to Burp Suite as a tool, the analysis relies on written materials, including Burp Suite's documentation and Dafydd Suttard and Marcus Pinto's 2008 *The Web Application Hacker's Handbook*. This book claims to be "a practical guide to discovering and exploiting security flaws in web applications" [133, p. xxv]. Throughout the book, the authors use Burp Suite as the primary tool to showcase their methods of predatory targeting. This is not by coincidence, Suttard created the tool between 2003 and 2006 [133], [134], which is now maintained by PortSwigger [134], a company more than fifty per cent owned by Stuttard [135]. PortSwigger also maintains an online academy that claims to replace the third edition of The Web Application Hacker's Handbook online [136]. Given the apparent propagation of people and ideas related to Burp Suite across the book, the company, its website and academy, the present research treats the collection of these artefacts as a lexicon of primary sources. These primary sources provide not only descriptions of the tool, but also of the practices and experiences of targeting from the firsthand account of the tool's creator. As the book and the academy both perform educational functions, they also transmit knowledge from the tool creator to aspiring targeteers. Akin to Nmap and its documentation, Burp Suite and its information ecosystem can be treated as primary sources to understand predatory targeting.

3.2.3 Attacks or Targeting?

What is the difference between attack and targeting? Can one exist without the other, or are they always inherently tied together? Both intelligence and predatory targeting may be parts of computer network exploitation (CNE) and computer network attack (CNA), albeit only predatory targeting is a necessary component of both. Predatory targeting – the generation and elimination of attack hypotheses (see below) – is necessary for both. CNE's primary purpose is "covert intelligence gathering and espionage", while CNA focuses on affecting the integrity or availability of computer systems [137, p. 386]. Both rely on the compromise of a computer system – either for intelligence or predatory purposes – and thus, are different from intelligence targeting that does not necessarily involve system compromise. Nmap as an intelligence targeting tool may scan a network, locate its targets, and gather information about them without compromising any part of

the target system.[18] Hence, intelligence and predatory targeting are disjoint sets, just like CNE and CNA. CNE or CNA always involve predatory targeting, while intelligence targeting may sometimes be a precursor to both. Differently put, predatory targeting concerns the means to achieve the *objective* of CNE and CNA (compromise), while intelligence targeting concerns their *object of interest* (the target).

This is important to delineate because what is considered to be an 'attack' in the Burp Suite lexicon overlaps with both CNE and CNA, and thus, predatory targeting, but not with intelligence targeting. The Handbook broadly considers attacks as "the practical steps that you can take to probe and attack an application's logic" [133, p. 349].

> "Any serious attacker, therefore, needs to pay serious attention to the logic employed in the application being targeted, to try to figure out the assumptions that designers and developers are likely to have made, and then to think imaginatively about how those assumptions may be violated" [133, p. 350].

The essence of an attack – or predatory targeting – for Burp Suite is thus the testing of hypotheses about the possibilities to violate the assumptions designers embed into their systems. This game of assumptions is what differentiates predatory targeting from intelligence targeting in terms of targeting rationale. It also necessitates a considerable qualitative difference between the target ontology and targeting modalities of predatory targeting compared to those of intelligence targeting. This difference manifests most visibly in how intelligence targeting focuses on mapping networks of targets, while predatory targeting is preoccupied with mapping networks of hypotheses onto so-called 'vulnerability signatures'.

3.2.4 Burp Suite's Target Ontology

The targeting ontology of Burp Suite consists of web application functionalities, such as a login form or file submission feature. Probing these components eliminates attack hypotheses and generates knowledge for weaponisation that calibrates payloads to exploit vulnerabilities. Predatory targeting, in general, is thus aimed at producing knowledge, where reconnaissance generates hypotheses, probing eliminates them, weaponisation calibrates knowledge into payloads, and delivery carries it to targets.

[18] For the sake of simplicity, the functionalities of Nmap that could incidentally degrade targets are ignored here.

Tracing this chain shows that targeting is more than reconnoitering a target system; it is a series of knowledge generating activities transient across the phases preceding the moment of exploitation.

The Handbook's chapter on attacks against access controls reveals the knowledge and ontology at play in predatory targeting. Firstly, attacks against access controls require a targeting sub-domain that catalogues identities, roles, access controls, functionalities, data, and resources. In an attack that is aimed at breaching a user's account, the target is not merely defined by its username, but also by its role, rights, accesses and powers in the target system. Consequently, the targeting sub-domain is embedded into the higher-level targeting domain of applications. As targets diversify, these lower-level ontologies scale at least linearly, proliferating the ontology of predatory targeting rapidly. By necessity, predatory targeting tools proliferate quickly in functionality and variance.

3.2.5 Burp Suite's Epistemology & Process of Targeting

Targeting by Burp Suite includes the two cycles of mapping and probing. In mapping, hypotheses are formed about target system functionalities and vulnerabilities. This phase includes manually navigating a web site for features and elements, crawling or spidering a web page for resources, and harvesting data for analysis. In the subsequent phase of probing, Burp Suite calibrates payloads, sends them sequentially, and measures resulting changes in application behaviour to eliminate and validate hypotheses. This hypothesis testing results in a set of attack hypotheses that enable predatory effects in the later phases of the cyber kill chain.

The mapping cycle of predatory targeting is aimed at generating hypotheses about vulnerabilities. According to the lexicon, each vulnerability carries a 'vulnerability signature', a unique fingerprint that identifies an array of entry points, attack paths, and weaknesses for a given functionality [133, p. 487]. This signature lies at the centre of attack hypotheses, tested in the probing cycle.

> "The final stage of the mapping process is to identify *the various attack surfaces* exposed by the application, and the potential vulnerabilities that are commonly associated with each one" [133, p. 91] (emphasis added).

Surfaces are the outer boundaries of objects [138, p. 197], and attack surfaces are sets of gateways that allow an attacker to enter a system, but they are not vulnerabilities themselves. In this way, attack surfaces exist *without* vulnerabilities momentarily; at the moment, they are not more than *potential* entry points to a system. This transitionary state of the attack surface – that it is the mental imagery of a path, rather than an actual attack – is what necessitates the hypothesis-based modality of predatory targeting.

Vulnerabilities and attack surfaces merge into vulnerability signatures when hypotheses about the weaknesses of a functionality and its indicative behaviours are tested in probing, and thus become 'associated' with vulnerabilities. Mapping the attack surface of a target application is thus inseparable from probing it for vulnerabilities. This inseparability is what differentiates the mapping of predatory targeting from the mapping of intelligence targeting. Predatory targeting emerges with the critical step of merging attack surfaces with vulnerabilities, which happens through probing.

Probing involves steps to validate hypotheses about vulnerability signatures. It is aimed at confirming that a given entry point provides a viable attack path that exploits a weakness in a certain functionality. Probing – in the context of web applications – is the process of sending requests to a web application and assessing its responses. It is part of the epistemology of predatory targeting as it aims to eliminate hypotheses in search of attack paths. However, this knowledge generation is not entirely cumulative or terminal; it is generated by sequential repetitions of probes and hypotheses. Both mapping and probing, therefore, involve circular steps – crawling after crawling after crawling – and both can turn to each other multiple times as hypotheses are discarded and new ones are sought for.

3.2.6 Burp Suite as Epistemic Infrastructure

Probing happens in iterations either because there are multiple hypotheses to be tested, or because there are multiple targets. In the simplest example, enumeration is a probing technique offered by Burp Suite to place markers and corresponding payloads in elements of URLs or HTTP requests [133], [139], forcing the targeted application to violate the assumptions of its designers. Many web designers would, for instance, ingrain a logic in their system to identify certain files by sequential numbers. For any application that returns these documents at a simple HTTP request with the URL

parameter of '&file=1' for the first file and '&file=10' for the tenth file, an attacker could force the application to return all files stored by enumerating parameter values one by one. What happens is an attacker forming a hypothesis about the application's behavior – that it returns files by sequential URL parameter values – to identify a weakness. Therefore, probing involves making guesses about system weaknesses and manipulating them to identify vulnerabilities.

Beyond sending probes, the cycle of probing also validates hypotheses. This relies on a technoscientific apparatus of cognitive tasks and material artefacts. Cognitive tasks involve human 'intuition', for example, as targeteers assume the hats of their opponents to guess their design assumptions.

> "Every web application is different. Attacking an application effectively involves using various manual procedures and techniques to understand its behavior and probe for vulnerabilities. It also *entails bringing to bear your experience and intuition* in an imaginative way" [133, p. 471] (emphasis added).

Testing for path traversal vulnerabilities or exploiting access controls illustrate how hypotheses are formed and eliminated based on the targeteer's perception of design assumptions. Path traversal illustrates how "user controlled data" passed to "file system operations" can cause behaviours to "traverse out of the starting directory and access files from elsewhere on the server file system" [133, p. 337]. In certain misconfigured systems, requesting resources from the target is possible by querying for a payload "../../../../../../../../../../../etc/passwd" that instructs the underlying server to navigate its file system in a way unthought of by the application's designers. This results in the compromise of sensitive files that were not intended for public eyes, such as the passwd file of a Linux system that includes confidential user account identifiers.

The attack illustrates how probing is calibrated and how attack hypotheses are tested. Firstly, the targeteer enters various payloads, say, in the address bar of their browser, which instructs the server to retrieve files from its file system. Often, this process involves many steps of trial and error as the tester submits variations and encodings of the payload to see which one exerts behavioural change. This calibration involves positioning, as well as manipulating payloads. Positioning in this case refers to finding application components that are likely to return files when probed, while manipulation

includes acts to permute or encode payloads in attempts to fool system controls. These manipulations are afforded by Burp Suite's epistemic infrastructure that allows to define payloads as hypotheses about the states of a system, given certain inputs. This testing involves observing response behaviours and assessing whether or not they support or refute a hypothesis. When it is determined that a certain payload validates the hypothesis, the payload is saved as weaponised knowledge for subsequent exploitation. For example, a simple payload targeting the above-mentioned file locator path would include numbers from one to many, testing application responses until the state that returns no files is reached. Because payloads carry state values that identify hypotheses as true or false, they act as knowledge workers, with Burp Suite providing the underlying epistemic infrastructure for such work. This infrastructure lets targeteers define testable hypotheses with payloads and calibrate payloads with start and end points in HTTP requests and send these requests to multiple parts of a target application.

To calibrate probing, Burp Suite allows its operator to choose one or more of multiple input types for its probing cycles, as well as a mode of targeting. These input types include regex patterns, characters, numbers, dates, bits and more [140]. Modes include the 'sniper' mode, which lets users cycle through a number of values at a single given entry point, while the 'battering ram', 'pitchfork', and 'cluster bomb' modes combine multiple fields with different datasets and input types [133], [140]. These modes let the targeteer test multiple or complex hypotheses in a single automated probing cycle. However, because they use combinations to produce hypotheses, they also generate unwanted amounts of noise that make targeting less discriminatory. Therefore, for precise probing, the Handbook recommends identifying "the attributes of the server's responses that you are interested in analyzing" [133, p. 494]. This is presumably aimed at fine-tuning payloads to reduce the number of hypotheses and the volume of their noise. When the Handbook recommends identifying 'the attributes' of the target, it suggests mapping its attack surface without a vulnerability. Consequently, precision in predatory targeting is achieved by the appropriate identification of attack surfaces *before* payloads are sent. This implies that ethical discrimination in targeting requires not only appropriate target selection and the weighing of effects against benefits, but also a careful consideration of attack surfaces and the identification of corresponding attack hypotheses. Probes against only the obvious entry points of a target are likely to miss meaningful vulnerabilities that could be potentially less damaging and more

discriminatory to exploit. However, how the attack surface is perceived by the targeting system depends on its perceptual field, which is strictly limited by the system's target ontology. Ethical and responsible targeting, thus, requires the continuous evaluation of target ontologies to identify overlooked attack surfaces.

3.2.7 Sequentiality as the Logic of Predatory Targeting

While Nmap's network-based epistemology is characterised by its topology, Burp Suite's probing is characterised by its *sequentiality*. Network mapping sends packets to targets to reveal their accessibility and connectivity, and then maps these targets over network paths. Burp Suite, in turn, sends sequential payloads in probes that test various states and hypotheses, aimed at enumerating vulnerability signatures.

Sequentiality in probing marks the logic of predatory targeting. It clearly manifests in the calibration of probes, as payloads are defined by lists and input types. In access control attacks, for example, the list often consists of a sequence of usernames or passwords. These usernames or passwords are sent to the targeted authentication mechanism that accepts or rejects them based on its input filters. This is also called a brute-force attack, because it relies on exhausting the hypothesis space with all possible payload variations. Furthermore, sequentiality depends on mechanisms of filtering and sorting, determined by the affordances of the targeting tool. Similar to how Nmap's target ontology is constructed socio-technically by overlaps and offlaps of perspectives, Burp Suite's target perception is defined by its hypothesis space – the set of all possible hypotheses. These are products of the designer's perception of the hypothesis space and the architectural affordances of the tool-in-emergence. Therefore, the sequential logic compels targeteers to use predetermined target ontologies – limited by sorted and filtered lists, limiting the perceptual field of the predatory targeteer. This creates similar blindspots and biases as Nmap's perspectival eye, although through the morphospace of attack hypotheses.

Burp Suite's generation of vulnerability signatures through sequential hypothesis testing and empirical validation resembles the paradigm of technoscientific rationality. It is characterised by science that "has become an entrepreneurial and pragmatic project in which technology assumes a lead role in the development of innovative solutions [sic], characterized by a strong interest in the unpredictable, in processes of emergence, and in

the unknown" [108, p. 12]. In technoscience, complex problems are solved through "formalized and systematized tinkering as well as the use of trial and error, bottom-up search heuristics and post-processing" [108, p. 12].

Burp Suite's sequential probing is exactly this kind of systematised tinkering, where hypotheses are not resolved in a precise targeted manner, but by trial and error. This creates a sense of empirical validation as the subject can claim knowledge from etic observations. As Weber notes, this 'technoscientific rationality' is dangerous, as it sanitises socially produced knowledge to legitimise targeting by appealing to what appears to be a scientific – and thus unquestionable – rationality [108]. It is a mistake, however, to assume that what is produced by empirical testing is pure truth, as the filtering and sorting that goes into hypothesis validation in technoscience is social and political. Given the sociotechnical construction of Burp Suite's targeting domain – the determinism of its ontology and epistemology – the tool itself is always partly social and political, too.

3.2.8 The Violence of Predatory Targeting

Predatory targeting – and the phases of reconnaissance, weaponisation and delivery of the cyber kill chain – are ridden with violence, due to the biases, blindspots and injustices built into and reproduced by targeting tools. Recognising this violence is a step forward to a more ethical and responsible design and use of targeting tools.

Beyond direct harm from successful compromise, predatory targeting enacts violence and creates pretexts for future violence. Predatory targeting is no less violent than that of intelligence targeting (see section 3.1.5). Predatory targeting violates the principles of discrimination by hoarding, correlating and ignoring information about its targets. Discrimination cannot be fine-tuned with calibration completely because the tools' perceptual fields are determined by architectural choices.

Burp Suite exemplifies two related modes of violent practice: hoarding ('harvesting') and probing. Harvesting "extract[s] useful or sensitive data from the application using specific crafted requests" and shifts enumeration from binary hits to content extraction [133, pp. 472, 484].

Harvesting is violent because it amasses data irrespective of ownership or context, enabling misuse through indiscriminate aggregation. This can be widely unethical without proper constraints [141], [142], [143], [144], [145], as hoarding of publicly available information violates the subjectivity of the data subjects. This not only includes privacy, but also the right to be free from algorithmic decision-making or mass targeting across social interactions [22], [146], [147], [148], [149]. Hoarding, therefore, violates the subject mostly because it is indiscriminate and has the potential for aggravated misuse. Furthermore, harvesting biases target selection by filtering data (later weaponised in probing). Using extractors, Burp Suite pulls data from specific fields of an application (e.g., 'SessionId', 'OrderType'), predetermining the hypothesis space of the tool, shifting its focus from meaningful targets to ones found by chance.

Even more sinister than harvesting, Burp Suite's targeting domain produces violence through probing by eliminating hypotheses and driving behavioural indicator searches. Burp Suite labels observations that carry knowledge about vulnerability signatures "hits" [133, p. 476]. Probing recognises hits that are consistent with attack hypotheses but ignores weaknesses that are not, constructing a list of targets where ignored hypotheses are de-prioritised compared to vulnerability signatures that produced hits. If the logic of targeting is to use force discriminately and only as long as it is needed, the prioritisation of targets has the potential to exclude some from the kill list in favour of others. This architectural affordance potentially contributes to the aggravation of discriminatory violence, as different priority target lists result in different sequences of violence.

The second form of probing violence relates to the creation of behavioural indicators. Since targeteers may not always know what to expect from an application, and thus, may miss a hit, a technique appeared to generate targets from 'unknown unknowns':

> "[Targeteers may] not know in advance precisely how to identify hits. Rather than monitoring the application's responses for a specific indicator of success, [targeteers] generally need to capture as much detail as possible in a clear form, so that this can be easily reviewed to identify cases where [an] attack string has triggered some anomalous behavior within the application, which merits further investigation" [133, p. 487].

The technique prompts targeteers to probe for responses, record outputs, and analyse behavioural anomalies, and correlate them with other datasets to produce indicators. This 'diagnostic screening' employs a techno-scientifically rational epistemology to infer knowledge from 'unknown unknowns', which Erik Reichborn-Kjennerud's 'epistemological history' traces to the conditions and logics of knowledge generation through the history of US military targeting [150, pp. 9-10]. Reichborn-Kjennerud shows that diagnostic screening's trial-and-error mode of targeting has been historically ripped off of its violent genealogy to conceal how tinkering with targeting logics had produced unnecessary violence on the path to precision targeting. The problem is that this mode of targeting carries over to cybersecurity, as behavioural indicators replace attribute-based detections (see, [127], [128], [151]). The example of Burp Suite shows that trial-and-error mode of targeting results in filtering and discrimination, which produces targeting knowledge not based on careful considerations of what is and is not a legitimate target and how targeting may produce harm but on how systematised and operationalised suspicion identifies targets by anticipatory correlation. This suspicion-based targeting gives rise to a world where targeting's logics become increasingly opaque, and its effects ever more unethical [41], [152]. In this world, "the mass production and processing of data from the ever-expanding digital ecosystem, various techniques of capture, abstraction, and modeling now iteratively correlate and represent the entire world as fluid sets of relationships in which the enemy and the operational environment are seen as spatiotemporal continuums" [150, p. 9]. Therefore, targeting tool design that enacts anticipatory logics could result in less transparent and ethical targeting systems and operating procedures.

3.2.9 Automation and Knowledge in Predatory Targeting

The analysis of behavioural indicators requires large memory and complex computations to correlate data, which relies on automations and various degrees of human-machine interactions. Automation eases or replaces human labour by offloading perceptual, mnemonic or epistemological labour, which signify the knowledge economy of predatory targeting.

In an article about SAGE, an early computer-based targeting system of the Cold War, Jeremy Packer and Joshua Reeves show that Cold War fears of human mistakes about missing nuclear launches prompted the automation of tasks previously done by humans, namely sensing, remembering, and identifying threats [153]. They explain that "SAGE developed out of an anthropophobic rationality: namely, the belief that military observation and response mechanisms must eliminate the possibility for human error" [153, p. 313]. The system automated the tasks of sensing, remembering and knowing the enemy, effectively joining the perceptual phases of targeting into a single process of human-machine interaction. Tools like Burp Suite evidence how these cybernetic ideas morphed into a techno-scientific drive toward predictive behavioural modeling (cf. [154]), as the tool aims to make "extremely laborious" tasks less "prone to mistakes" [133, p. 471]. Burp Suite leverages the logic of sequentiality to automate probing with deterministic algorithms, offloading human labour to the machine in an attempt to spare time, resources, and avoid human errors. In this, the predatory targeting logic behind automations is not dissimilar to the desire of SAGE to avoid semiotic failures, making automation a common desired feature of predatory targeting as it lends naturally to a sequential episteme.

Automation shifts the relationship of humans to knowledge and machines by decreasing alleviate labour, coincidentally requiring humans more cognitive labour. This contributes to knowledge development at the individual level by deskilling pentesters to concentrate on proper inputs, while subsequently reskilling targeteers to generate new hypothesis spaces as exploit developers. Both of these trends contribute to knowledge exchanges and dynamics that favour higher level knowledges, while also intensifying labour at certain sites. The ascendance of widely available artificial intelligence technologies illustrates how these trends transform targeting practice already, offloading certain cognitive tasks from humans to machines [155], [156].

3.2.10 Summary

Burp Suite represents the paradigmatic tool of predatory targeting in which the purpose to construct vulnerability signatures regiments a range of epistemic techniques that rely on a modality to recognise ‘hits’and eliminate hypotheses via probing. Burp Suite’s target ontology is designed to couple attack surface discovery with vulnerability signatures by matching entry points and attack patterns with functional weaknesses. In two cyclic phases of targeting, the tool generates a hypothesis space of possible weaknesses from the attack surface it maps, which are then tested and eliminated via probing. Probing is the main epistemic technique of Burp Suite, integrating the logic of sequentiality into a techno-scientific rationality of testing hypotheses via systematised and automated tinkering. This shuffles the dynamics of knowledge production and perceptual labour between knowledge workers, who therefore assume new roles with the machine taking on more tasks in the mapping phase and the human operator in the calibration step of the probing phase. The deskilling of the operator and the sequential tinkering of probing results in violence as targeting tools hoard, filter, and correlate data in ways that reproduce biases, erase subjectivity, and create pretexts for further harm. This process institutionalises anticipatory suspicion, turning aggregated signals into opaque indicators that justify anticipatory suspicion and perpetuate cycles of unnecessary targeting. Burp Suite, thus, evidences how socio-technical biases enter predatory targeting, driving violent effects and practices of systematised tinkering.

4 Discussion

The thick description of Nmap as an intelligence targeting tool and Burp Suite as a predatory targeting tool in the previous chapter outlines (1) an analytic framework for cyberspace targeting; (2) a theory of the socio-technical construction of biases and blindspots in targeting tool design; (3) a theory of violent knowledge production and exchange through targeting; and (4) descriptions of the practices and experiences of violence, hiding and manoeuvre in targeting. This section interprets these findings and translates them into operational, ethical and design take-aways.

4.1 A Framework for the Analysis of Cyberspace Targeting

This thesis has analysed two targeting tools and the corresponding targeting epistemes in a framework that can be adapted for similar analysis elsewhere. The framework consists of the steps of (1) mapping the target ontology of a tool; (2) enumerating and characterising the epistemic techniques of targeting; (3) identifying the episteme of targeting; (4) identifying the rationale of targeting from the episteme, epistemic capabilities and ontic affordances of the tool; (5) matching the rationale of targeting with practices observed in targeting, manoeuvre and hiding; and (6) identifying the experiences of violence produced during targeting. Table 1 illustrates these components with key research questions and examples from Chapter 3.

Table 1 – Key Questions Guiding the Analytic Framework

Step	Key Questions	Examples
1 - Ontology	What is recognised as a target? How are targets related? What is unseen?	Nmap recognises hosts and ports as targets. It does not recognise ‘unresponsive’ hosts. Burp Suite recognises target functionalities and data fields that are consistent with its attack hypotheses.
2 - Epistemology	How are targets accessed? How is data gathered and processed?	Nmap uses packet header manipulation to access its targets. Burp Suite uses mapping techniques and probing to generate, test and eliminate hypotheses.
3 - Episteme	What is the underlying mental	Nmap uses the image of the

	model that is used to characterise the target (set)?	network as its core episteme, relating non-spatial targets with the logic of topology. Burp Suite works with imaginary vulnerability signatures that associate functional weaknesses with attack surfaces.
4 - Rationale	What logics are represented in the episteme of the targeting system? How is targeting rationalised by these logics?	Nmap's network-based episteme drives a mathematicised logic of topology, as well as a political economy of cybersecurity knowledge production and exchange. Burp Suite relies on sequentiality to systematically tinker with hypotheses and target system functionalities, allowing it the cloak of empiricism and efficiency.
5 - Practices	What practices of targeting, hiding and manoeuvre emerge from the episteme and rationale of targeting?	Since Nmap perceives its targeting environment in terms of networks, it exploits and suffers from the affordances of networks. It uses header manipulation to mimic sources and make itself appear as a distributed network. Burp Suite is limited by its sequentiality in how it calibrates probing.
6 - Experiences	What experiences (or effects) does targeting produce for the target and the targeteer?	Nmap's focus on reachable hosts, packet-based scanning techniques and network-based representations make it forget other legitimate targets and orient it toward IPv4 sub-nets. Nmap violates target subjectivity with disassociation, which Burp Suite achieves via hoarding, probing and anticipatory hypothesis generation.

The research has validated the proposed analytic framework with the thick description of two widely used cyberspace targeting tools. It performed the analysis as per Figure D and observed the dynamics, logics, practices and experiences of targeting. Future research can make use of and extend this framework by applying it to other tools either comparatively or as standalone studies.

4.2 The Socio-Technical Construction of Targeting Systems

The analysis of Nmap and Burp Suite demonstrates that targeting systems are not merely neutral instruments but socio-technical assemblages that reflect their conditions of emergence and operationalisation. These conditions are characterised by the co-constitution of targeting logics in human-machine interactions. As evidenced by the "overlap" and "offlap" of the designer's and the tool's fields of vision, the target ontologies of these systems are socially constructed artefacts that hard-code specific biases and blindspots. Nmap's reliance on a network-based episteme rooted in topology, and Burp Suite's adherence to a sequential, hypothesis-driven logic, illustrate how the perspectival engineering of these tools dictates what entities are recognised as legitimate targets while rendering others invisible. This socio-technical assemblage ensures that the tool does not simply reflect the environment but actively shapes the perceptual field of the operator. By embedding a specific logic of violence in target practice – whether through the reduction of complex social entities to IP addresses, or through the filtering of behavioural indicators – violence permeates targeting.

There are a number of system design implications that follow from these findings. They cover analytic practices, design team structures, enforceable governance protocols, and a potential for neural systems. Firstly, targeting tools and designers couple perceptual fields to complement and reinforce each other about their shared recognition of the target. This means there are no unbiased tools, necessitating an analysis and mitigation of architectural and human biases in targeting, as well as their politicisation. Analytic techniques exist to mitigate biases as early as the problem definition phase of the design process,[19] as do governance structures that can reduce blindspots. These are easier to fix in learning systems, where ontologies are dynamically calibrated to perceive previously unrecognised entities. Learning systems include technological solutions, like neural networks, as well as socio-technical interventions. For example, protocols to integrate user feedback about unrecognised targets and targeting practices periodically could build more agile socio-technical learning processes. Similarly, learning techniques and

[19] Intelligence practitioners have long relied on so-called 'structured analytic techniques' (SATs) to mitigate biases [157], [158], [159], although the effects of these await further scientific validation [160]. Multiple accounts exist that highlight the pitfalls of SATs [161], [162], [163], [164]. Structured analytic techniques in the design and analysis of cyberspace targeting could include Cross-Impact Matrix analysis to identify the impact of epistemic techniques on ontologies and vice versa; Morphological Analysis to ideate about alternative modalities and targets; Hypothesis Generation and Diagnostic Reasoning in predatory targeting; and Key Assumptions Check throughout the design and testing phases.

protocols could be established at the designer level to prompt humans to periodically and methodically review their targeting assumptions.

Finally, tool designers must consider socio-technical power games as well, since the negotiation between tool and designer about perceptive modalities is decided by the relative power of the two. To upset the imbalance, the integration of modalities needs an empowered design-engineering team, most urgently in terms of skill, but also potentially in terms of time, trust and knowledge. Design-engineering teams need to recognise they may be disadvantaged in face of a powerful and complex tool. If an inexperienced designer faces the challenge to design or tweak a complex and powerful codebase, there is a possibility that no new modalities will be added because the tool's perceptual field will dominate. To construe new modalities, thus, the designer team needs to outpower the tool, for example, by enlarging the team or involving senior developers.

These findings are translated into actionable advice for system designer-engineering teams in Table 2. They suggest that targeting system design-engineering is a socio-technical management process, requiring management tools and techniques to balance specific dynamics, biases and blindspots, specific to cyberspace targeting tools.

Table 2 - Actionable Advice for Targeting System Design-Engineering

Advice 1	Cyberspace operators need to study and mitigate the architectural and human biases of targeting, recognising that what and how they perceive in cyberspace is deeply socio-technical. Structured analytic techniques and analyses similar to this research could help the process.
Advice 2	Design-engineer teams need to regularly and critically analyse the tools they are building not only in terms of efficiency, but also in terms of their onto-epistemic limitations. Human biases have to be mitigated, while also appraising the effects of a tool on the shared perceptual field of targeting.
Advice 3	Targeting design and operations need to involve continuous learning, which can make use of technical systems – like neural networks – as well as human systems, like protocols that demand user-feedback integration and regular targeting assumptions check.
Advice 4	Management needs to consider the socio-technical power games as inherent parts of the design and engineering of targeting tools. Design-engineering managers need to identify and strategically mitigate power imbalance, for example, by re-allocating human and cognitive resources when a powerful and complex tool is being (re)designed.

4.3 The Violence of Knowledge Production & Sanitisation

The thesis has argued extensively that the violence of targeting surpasses its predatory effects as it generates and exchanges violent knowledges. This points to moral hazards and ethical considerations about the violence of knowledge production and its sanitisation in cyberspace targeting. The cycle involves three consecutive sites of violence: knowledge extraction, sanitisation, and the re-use of violent knowledge. These are illustrated in Table 3 below. In cyberspace targeting the process can be observed in how tools translate offensive practices into defensive knowledge, including the knowledge to design defensive tooling with appropriated targeting modalities.

Table 3 - The Mechanisms of Violent Knowledge Production

Mechanism	**Questions**
Knowledge Extraction	What knowledge is produced and how?
Violent Foundations	What or who experiences violence at the moment of knowledge extraction?
Erasure	How is the violence of extraction erased?
Recurrence due to Ignorance	How does the ignorance of the original violence and erasure produce more violence?

Defenders effectively extract value from offensive knowledge by enacting targeting practices and designing tools that inherit targeting modalities. In the process, the temporary enactment of violence appears as a method of knowledge production, legitimising offensive knowledge and perception through their defensive services by portraying them as the only paths to security. This knowledge is later sanitised of their violent origins through sanitising technologies that disallow non-violent perceptions of cyberspace. Sanitisation happens through the abstraction of offensive practices into a linear calculation of risk (threat x likelihood), the erasure of victims and their prohibitive associations, and the legitimisation of violence through red team contracts that frame targeting as temporary, controlled, harmless exercises. Thereby, the violent logics of targeting become cloaked behind the calculative logic and knowledge economies of cybersecurity, depicting aggression as neutral, temporary exchanges and conversions. Nmap's self-legitimisation and Burp Suite's techno-scientific rationality are specific instances of this sanitisation. Moreover, although appearing clean of

violence, offensive knowledges imprint specific images of enmity in defenders, biasing their perceptual fields with the onto-epistemic limitations of targeting. Appropriated targeting epistemes commit defenders' perceptual fields to a set of legitimate targets via epistemic techniques and infrastructures. These are engineered into the tools of targeting, which operationalise particular perceptual modalities to perform targeting. This is morally hazardous as these practices blindfold violence by depicting socio-technical targeting systems as neutral, inconsequential, unbiased and comprehensive perceptual machines. Consequently, an ethical framework of targeting limits the inherited violence of targeting by considering its perceptual limitations.

4.4 Practices and Experiences of Targeting

Targeting tools operate in so-called targeting domains defined by the triplet of episteme, epistemology and ontology. The triplet collectively produces the perceptual field of the socio-technical targeting system, which influences how targets are perceived, approached and accessed by targeteers. This implies that the practices of targeting – specifically following engineered processes, interacting with machines, manoeuvring and hiding – are fundamentally determined by the architecture of tools.

The targeting process is defined by a sequential logic and predetermined target ontologies that limit the operator's perceptual field to what the tool's architecture permits. Given the static nature of the ontologies and epistemologies these tools employ, the process of targeting is also restrained to a finite set of practices. Often, these sets are not sufficient, and therefore, targeting necessitates domain traversal within and across tools, necessitating human translation between social rationales and machine ontologies. Such human-machine interactions are further constrained by architectural affordances. They also define the experience of targeting with uncertainty. Architecture ingrains an experience of lost agency in targeteers, as well as new dynamics of human-machine knowledge exchanges. With automation, these exchanges increasingly shift perceptual labour from humans to machines, potentially involving further machine biases. Automation in tools like Burp Suite also offloads perceptual, mnemonic, and epistemological labour (e.g., repetitive probing), while intensifying the need for human cognitive labour. This shifts the labour dynamic as operators become deskilled in repetitive tasks but reskilled as exploit developers who generate new assumption sets.

Human-machine interactions are thus inherent in cyberspace targeting not merely because perceptual modalities depend on the translation of digital signals to semiotic meaning, but also because target processing requires further steps of perceptual, mnemonic, and epistemological labour, as well as acts of social translation.

Targeting involves manoeuvres, as targeteers move through cyberspace, trying to evade defences while positioning themselves to increase their knowledge of targets. Sometimes manoeuvres can have more mundane functions too, for example, to calibrate timing and resource usage during targeting. Defensive manoeuvres, on the other hand, are aimed at hiding the fact of targeting by anticipating and subverting targeting perception to foil detection, identification, and pursuit. Because one hiding party enlists the modalities of the other, hiding is the complementary – or 'constitutive obverse' – of targeting. Therefore, to understand hiding tactics, one needs to understand the perceptual modalities of targeting. Nmap and Burp Suite both employ hiding tactics, such as disinformation, mimicry and distortion through fragmentation, deceleration, proxying, and decoys. Yet, as defensive tools learn these tactics, they appropriate the perceptual modalities of offenders to detect targeting. This compels the targeteer to reposition, through which targeteers learn more about their targets, since many of the epistemic techniques reviewed rely on perspective.[20]

The co-constitutive nature of the offence-defence choreography reveals an interactive process whereby the effectiveness of hiding depends on continuous testing and interaction between offensive and defensive tools. Manoeuvre and hiding are therefore co-dependent. The development of offensive manoeuvres drives the evolution of hiding techniques, and vice versa. This creates a circular ecosystem where security and insecurity are mutually experienced and produced. For the defender, the attacker's manoeuvre creates a sense of insecurity that manifests in self-scanning and attempts to reduce attack surfaces. For the attacker, the defender's hiding creates frustration and insecurity, arising from the inability to achieve a clean, deterministic view of the target. The relationship is not static; it is a dynamic equilibrium of constant adaptation. As defenders improve their hiding capabilities (e.g. better camouflage), attackers must refine their manoeuvres (e.g. new probing techniques), leading to an endless cycle of escalation and innovation in cybersecurity. It implies that operational training for hiding

[20] For example, Nmap's port states are perspectives rather than facts, and Burp Suite's hypotheses are slices of a morphospace rather than exhaustive sets of possibilities.

requires interactive environments where targetees learn how their manoeuvres impact their success.

4.5 Ethical, Operational and Design Implications

The ethical implications of these findings centre on the violence embedded within the socio-technical assemblages of targeting systems. This violence concerns harm caused by targeting either to the target or the targeteer. Harm to the target includes the violation of subjectivity through dissolution, mimicry, and forced categorisation, as the target is subsumed in the violence that treats it as merely an object of the martial gaze. Furthermore, by treating public information as confidential, and by hoarding data irrespective of ownership, these systems enact a form of epistemic violence that obscures the human cost of cybersecurity practices. Harm to the targeteer involves biases and blindspots introduced by a tool's perceptual field, target ontology, targeting techniques and underlying episteme. Furthermore, knowledge exchanges between offenders and defenders transmit the biases and injustices of offensive ontologies into defensive frameworks. Conclusively, targeting produces a variety of harms that disadvantage actors in the operating environment, and more generally, in cybersecurity as a professional field of practice. An ethical approach toward cyberspace targeting would take these findings to design tools that transmit fewer biases and enforce operational practices that mitigate targeting violence.

Operationally, the convergence of offence and defence creates a political economy of cybersecurity where the distinction between offender and defender becomes increasingly porous, driven by the mutual mimicry of targeting modalities. This operational reality suggests that security practices are no longer merely about protecting assets but about appropriating adversarial knowledges. The dynamic forces operators into a state of perpetual vigilance, attempting to anticipate adversary practices by detecting anomalous behaviours. The need for anomaly analysis gives rise to automation workflows that shift the human's role from active perception to the management of opaque systems where biases and blindspots remain unacknowledged. These limitations shape the operational reality of targeting as they limit the perceptual field of targeteers. Therefore, analysing the perceptual modalities of cyberspace targeting tools is not only an ethical criticism, but also a way to identify suboptimal and

undesired practices, experiences and effects that have been previously under-explored in both literature and practice.

From a design perspective, the findings necessitate a critical intervention into the architectural determinism that hard-codes specific ontologies and epistemes into targeting tools. Tools like Burp Suite and Nmap demonstrate that design choices shape the perceptual fields of operators, limiting the range of legitimate targets. Future tool development must, therefore, explore reflexive mechanisms that acknowledge the social construction of targets and resist the reduction of complex social entities to singular abstractions. This could ensure that the architecture of cybersecurity tools does not inadvertently enforce a rigid logic of enmity. Rigidity can be resolved with tools that evolve into dynamic systems that can learn from their environments, update their ontologies, and calibrate their violence. Learning could happen through both technological solutions and human-machine cooperation. Finally, tool design should incorporate the reflexive study of practices to understand architectural affordances. By doing so, these targeting tools can achieve better operational efficiency, less socio-technical bias, a more complete targeting coverage, and a more thoughtful set of operational rules of engagement that rest not in normative presumptions but in reflexive observations about the actual tools, practices and experiences of sensing the target.

5 Conclusion

5.1 Summary

Cyberspace targeting produces violence through engineering sanitised knowledges into tools and operationalising them in targeting practices. By mapping the ontology and epistemology of targeting tools across intelligence and predatory targeting, the thesis proposed an analytic framework to understand how targeting tools prompt sub-optimal practices and lead to violent effects. It studied the affordances of tools that connect human fields of action to machine modalities to understand how they define the epistemes of intelligence and predatory targeting. Through these modalities, it formed a theory of targeting that interprets engineering and operational practices in terms of socio-technical targeting. Collectively, the framework analysed the ethical, operational and design challenges of engineering violent knowledges into tools.

5.2 Contribution

This thesis contributed to existing research about cyberspace targeting by providing a thick description of particular tool design and usage practices. It also outlined several theories, including a theory of socio-technical construction of targeting, as well as a model to understand adversarial knowledge appropriation as part of the political economy of cybersecurity. The analysis furthermore expanded on historical narratives and first-person accounts of designers and users to explain targeting rationales and experiences. This included an analysis of perceptual fields and manoeuvring practices in cyberspace targeting that reveal room for design improvements. Targeting rationales also hint at ethical considerations that both design and operational practice can merit from. With its grounded theory, tool analysis, thick description, and deep-running ethical and design critique, this study contributed to existing literature with both theory and actionable advice. It expanded on previous literature about cyberspace targeting that focused solely on the effects and processes of targeting. While it drew on similar analyses of another targeting technology, Palantir, the thesis introduced a novel and unique framework to examine hitherto peripheral tools and practices of offensive cyberspace operations.

5.3 Generalisation of Findings

While this research has been highly particular to the tools and practices analysed, the narrative use of case studies in science and technology studies allows for some generalisation, although with flexibility for accrual research.

Firstly, the thesis divided cyberspace targeting into two mutually exclusive categories: intelligence and predatory targeting. The differentiation can be used consistently by including systems and fields of action in intelligence targeting that are aimed at gaining knowledge without any particular direct effect on a target, and assigning others with effects upon exploitation to predatory targeting. The differentiation is meaningful because it encourages a recognition and dissection of targeting as an assemblage of systems and practices. It opens possibilities for analysis beyond existing frameworks that leave considerable gaps about targeting tools and practice. By recognising the two modes of cyberspace targeting as different, it is possible to map the steps, effects and experiences of targeting in more granular detail. By looking beyond 'reconnaissance', it becomes possible to appreciate the perceptual modalities and experiences of targeting beyond this step. It is a recommendation therefore to analyse cyberspace targeting in the future as consisting of intelligence and predatory targeting – possibly part of computer network exploitation (CNE) and attack (CNA), but also distinct from them.

Secondly, the method of identifying perceptual modalities proved to be useful in revealing the epistemic techniques and ontological catalogues of targeting systems, as well as the logic, rationale and scientific thinking engineered into targeting. Studying these provides a ground to examine practices of targeting, as well as their ethical, operational and design implications. Therefore, future tool design aiming to reduce violent effects and expand perceptual fields needs to explore a wider range of perceptual modalities, as has been done in this research.

Thirdly, targeting can be conceptualised as a knowledge economy arising from an actor-network of human and non-human knowledge producers, knowledge workers, epistemic techniques and infrastructures, and antagonistic subjects. Treating targeting as a knowledge producing process, reveals the dynamic interactions that exist between tools and operators on both the offensive and defensive sides. Studying these dynamics

through the knowledge exchanges of targeting actors has the potential to unravel hidden logics about perceptual design, such as specific mechanisms of manoeuvre and hiding.

Fourth, the thesis outlined a theory of the socio-technical construction of targeting, positing that biases and blindspots emerge during tool design. In this process, tool and designer modalities compete to produce a dominant perceptual field, which is later engineered into the tool. Both tools and the derivative practices of targeting inherit an imprint of this competition, involving a power imbalance between codebase and designer. This implies practically that tool design requires careful governance and management to balance perceptual shortcomings.

Finally, although Nmap's and Burp Suite's violence may be particular, the mechanisms of extraction and sanitisation of violence in targeting could be a cross-cutting topic for future case studies. Unless tools are built with transparency about their design assumptions, engineering constraints and architectural biases, the knowledge produced in targeting will be derived from and sanitised of some form of violence. This carries moral hazard, risks operational inefficiency, and perpetuates impaired design.

5.4 Future Work

Future work on cyberspace targeting may benefit from shifting the focus from legalistic discourses of what is right or wrong to target and technical manuals of how to scan targets to phenomenological accounts of targeting. As this study has illustrated through the analysis of targeting tools and lexicons, studying perception in cyberspace is possible. Other approaches could involve the direct study of practices, as well as more comprehensive analyses of documentary material. Furthermore, ethnographic, experimental and design research is needed to validate design recommendations in practice, which may lead to more granular findings. While expanding the scope to secretive contexts – like state and criminal networks – could reveal unexpected results, keeping the discussion focused on commercially available tools and public practices would ensure transparency and wider applicability. Finally, expanding the analysis to other tools – both intelligence and predatory – could yield further results, including more precise descriptions of architectural affordances. Although this is promising, any such analysis requires an accompanying thick description of context and practices to ensure tools are analysed as embedded in their socio-technical and discursive context.

References

[1] J. Shires, “Cyber-noir: Cybersecurity and popular culture,” *Contemp. Secur. Policy*, vol. 41, no. 1, pp. 82–107, Jan. 2020, doi: 10.1080/13523260.2019.1670006.

[2] G. Huskaj, “The current state of research in offensive cyberspace operations,” in *18th European Conference on Cyber Warfare and Security (ECCWS 2019), 4-5 July 2019, Coimbra, Portugal*, Academic Conferences and Publishing International Limited, 2019, pp. 660–667. Accessed: Oct. 01, 2025. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1337484

[3] J. P. Farwell and R. Rohozinski, “Stuxnet and the future of cyber war,” *Survival*, vol. 53, no. 1, pp. 23–40, Feb. 2011, doi: 10.1080/00396338.2011.555586.

[4] J. S. Caso, “The rules of engagement for cyber-warfare and the Tallinn Manual: A case study,” in *The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent*, IEEE, 2014, pp. 252–257. Accessed: Oct. 01, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6917470/

[5] M. Connell, “Deterring Iran’s use of offensive cyber: A case study,” CNA Analysis & Solutions, Arlington, USA, 2014. Accessed: Oct. 01, 2025. [Online]. Available: https://apps.dtic.mil/sti/html/tr/ADA617308/

[6] W. R. Detlefsen, “Cyber attacks, attribution, and deterrence: Three case studies,” US Army Command and General Staff College, Fort Leavenworth, USA, 2015, Accessed: Oct. 01, 2025. [Online]. Available: https://apps.dtic.mil/sti/html/tr/AD1001276/

[7] A. Gamero-Garrido, “Cyber conflicts in international relations: Framework and case studies,” MIT Political Science Department, Cambridge, MA, USA, 2014, Accessed: Oct. 01, 2025. [Online]. Available: https://dspace.mit.edu/handle/1721.1/141695

[8] M. B. Gazula, “Cyber warfare conflict analysis and case studies,” PhD Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2017. Accessed: Oct. 01, 2025. [Online]. Available: https://dspace.mit.edu/handle/1721.1/112518

[9] M. Gordon, “Lessons from the front: a case study of russian cyber warfare,” 2015, Accessed: Oct. 01, 2025. [Online]. Available: https://apps.dtic.mil/sti/html/tr/AD1040762/

[10] T. Grant, I. Burke, and R. Van Heerden, “Comparing models of offensive cyber operations,” *Leadership Issues Cyber Warf. Secur. Cyber Warf. Secur.*, vol. 2, p. 35, 2015.

[11] E. P. Oliver, “A case study in cyber warfare,” in *Conflict and Cooperation in Cyberspace: Challenges National Security*, 2010, pp. 127–60.

[12] P. Pernik, *Preparing for Cyber Conflict: Case Studies of Cyber Command*. International Centre for Defence and Security (ICDS), 2018. Accessed: Oct. 01,

2025. [Online]. Available: https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf

[13] S. B. Aquino, "Shifting from kinetic to cyber: A cyber diplomacy literature review," *Int. J. Cyber Dipl.*, vol. 3, no. 1, pp. 3–11, 2022.

[14] H.-P. Vogel and F. Al-Dabbagh, "Unintended Consequences and Spillover Effects in Offensive Cyber Operations: A Systematic Literature Review," *Int. J. Cyber Threat Intell. Secure Netw.*, vol. 1, no. 01, pp. 25–30, 2024.

[15] W.-L. Cheng, "Collateral effects and unintended repercussions in offensive cyber operations: A Systematic Literature Review," *Int. J. Cyber Threat Intell. Secure Netw.*, vol. 2, no. 03, pp. 6–11, 2025.

[16] E. Larsson, "Collateral damage from offensive cyber operations—A systematic literature review," *J. Cybersecurity Priv.*, vol. 5, no. 2, p. 35, 2025.

[17] T. Grant and H. Kantola, "Targeting in all-domain operations: choosing between cyber and kinetic action," in *Proceedings, 20th European Conference on Cyber Warfare & Security (ECCWS 2021), online, paper*, 2021, pp. 139–148. Accessed: Feb. 24, 2025. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=wCo4EAAAQBAJ&oi=fnd&pg=PA139&dq=An+Introduction+to+Cyber+Analysis+and+Targeting

[18] R. Shandler, M. L. Gross, and D. Canetti, "A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United Kingdom, and Israel," *Contemp. Secur. Policy*, vol. 42, no. 2, pp. 135–162, Apr. 2021, doi: 10.1080/13523260.2020.1868836.

[19] R. Fanelli and G. Conti, "A methodology for cyber operations targeting and control of collateral damage in the context of lawful armed conflict," in *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 2012, pp. 1–13. Accessed: Feb. 24, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6243983/

[20] S. Backman, "Normal cyber accidents," *J. Cyber Policy*, vol. 8, no. 1, pp. 114–130, Jan. 2023, doi: 10.1080/23738871.2023.2281675.

[21] K. Kim, S. Oh, D. Lee, J. Kang, J. Lee, and D. Shin, "A study on cyber target importance quantification and ranking algorithm," *Appl. Sci.*, vol. 12, no. 4, p. 1833, 2022.

[22] M. Zehfuss, "Targeting: Precision and the production of ethics," *Eur. J. Int. Relat.*, vol. 17, no. 3, pp. 543–566, Sep. 2011, doi: 10.1177/1354066110373559.

[23] M. Sartonen, A.-M. Huhtinen, and M. Lehto, "Rhizomatic target audiences of the cyber domain," *J. Inf. Warf.*, vol. 15, no. 4, pp. 1–13, 2016.

[24] A. Bousquet, *The Eye of War: Military Perception from the Telescope to the Drone*, Minneapolis, Minnesota, USA: University of Minnesota Press, 2018.

[25] A. Bousquet, "Becoming (im)perceptible: from scopic regimes to the martial gaze," in *Drone Aesthetics: War, Culture, Ecology*, Beryl Pong and Michael Richardson, Eds., London, UK: Open Humanities Press, 2024, pp. 32-45.

[26] I. Chaar-López, “Drone technopolitics: A history of race and intrusion on the US-Mexico border, 1948-2016,” PhD Thesis, 2018. Accessed: Jan. 15, 2025. [Online]. Available: https://deepblue.lib.umich.edu/handle/2027.42/146090

[27] M. C. Elish, “Remote split: A history of US drone operations and the Distributed Labor of War,” *Sci. Technol. Hum. Values*, vol. 42, no. 6, pp. 1100–1131, Nov. 2017, doi: 10.1177/0162243917731523.

[28] D. Gregory, “‘The rush to the intimate’: Counterinsurgency and the cultural turn,” *Radic. Philos.*, no. 150, 2008, Accessed: Jan. 07, 2025. [Online]. Available: https://www.radicalphilosophy.com/article/the-rush-to-the-intimate

[29] D. Gregory, “From a view to a kill: Drones and late modern war,” *Theory Cult. Soc.*, vol. 28, no. 7–8, pp. 188–215, Dec. 2011, doi: 10.1177/0263276411423027.

[30] D. Gregory, “The everywhere war: The everywhere war,” *Geogr. J.*, vol. 177, no. 3, pp. 238–250, Sep. 2011, doi: 10.1111/j.1475-4959.2011.00426.x.

[31] L. Lee-Morrison, “Drone warfare: Visual primacy as a weapon,” Lund Univ., Lund, SE, 2015, Accessed: Mar. 21, 2025. [Online]. Available: https://lup.lub.lu.se/search/publication/7766431

[32] T. Wall and T. Monahan, “Surveillance and violence from afar: The politics of drones and liminal security-scapes,” *Theor. Criminol.*, vol. 15, no. 3, pp. 239–254, Aug. 2011, doi: 10.1177/1362480610396650.

[33] B. Gutman, “Palantir’s surveillance empire: A story of American policing, Patriotism, and Profit.” 2021. Accessed: Nov. 16, 2025. [Online]. Available: https://www.researchgate.net/profile/Benjamin-Gutman-3/publication/353352542_Palantir’s_Surveillance_Empire_A_Story_of_American_Policing_Patriotism_and_Profit/links/613eaee701846e45ef44fbeb/Palantirs-Surveillance-Empire-A-Story-of-American-Policing-Patriotism-and-Profit.pdf

[34] M. Lanzing, “Traveling technology and perverted logics: conceptualizing Palantir’s expansion into health as sphere transgression,” *Inf. Commun. Soc.*, vol. 27, no. 15, pp. 2617–2633, Nov. 2024, doi: 10.1080/1369118X.2023.2279557.

[35] A. Iliadis and A. Acker, “The seer and the seen: Surveying Palantir’s surveillance platform,” *Inf. Soc.*, vol. 38, no. 5, pp. 334–363, Oct. 2022, doi: 10.1080/01972243.2022.2100851.

[36] L. Ulbricht and S. Egbert, “In Palantir we trust? Regulation of data analysis platforms in public security,” *Big Data Soc.*, vol. 11, no. 3, p. 20539517241255108, Sep. 2024, doi: 10.1177/20539517241255108.

[37] S. Brayne, “Big data surveillance: The case of policing,” *Am. Sociol. Rev.*, vol. 82, no. 5, pp. 977–1008, Oct. 2017, doi: 10.1177/0003122417725865.

[38] L. Munn, “Seeing with software: Palantir and the regulation of life,” *Stud. Control Soc.*, vol. 2, no. 1, 2017, Accessed: Feb. 10, 2026. [Online]. Available: https://researchers.westernsydney.edu.au/en/publications/seeing-with-software-palantir-and-the-regulation-of-life/

[39] V. Galis and B. Karlsson, “A world of Palantir – ontological politics in the Danish police’s POL-INTEL,” *Inf. Commun. Soc.*, vol. 27, no. 13, pp. 2438–2456, Oct. 2024, doi: 10.1080/1369118X.2024.2410255.

[40] B. Massumi, *Ontopower: War, powers, and the state of perception*. Durham, North Carolina, United States: Duke University Press, 2015.

[41] L. Amoore, "Data derivatives: On the emergence of a security risk calculus for our times," *Theory Cult. Soc.*, vol. 28, no. 6, pp. 24–43, Nov. 2011, doi: 10.1177/0263276411417430.

[42] H. Tan, "Digital Guantanamo: The ontological regime of the onopticon-A near-future theoretical intervention via Palantir technology," 2025, Accessed: Nov. 16, 2025. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5317823

[43] R. Barrett-Taylor, "The reductive nature of military process," *Digit. War*, vol. 6, no. 1, p. 10, Nov. 2025, doi: 10.1057/s42984-025-00106-6.

[44] A. H. M. Nordin and D. Öberg, "Targeting the ontology of war: From Clausewitz to Baudrillard," *Millenn. J. Int. Stud.*, vol. 43, no. 2, pp. 392–410, Jan. 2015, doi: 10.1177/0305829814552435.

[45] U. Felt, R. Fouché, C. A. Miller, and L. Smith-Doerr, "Introduction to the Fourth Edition of The Handbook of Science and Technology Studies," in *The Handbook of Science and Technology Studies*, 4th ed., Cambridge MA, USA: MIT Press, 2017, pp. 1–26.

[46] M. Kuchler and G. Bridge, "Down the black hole: Sustaining national socio-technical imaginaries of coal in Poland," *Energy Res. Soc. Sci.*, vol. 41, pp. 136–147, Jul. 2018, doi: 10.1016/j.erss.2018.04.014.

[47] L. L. Delina, "Whose and what futures? Navigating the contested coproduction of Thailand's energy sociotechnical imaginaries," *Energy Res. Soc. Sci.*, vol. 35, pp. 48–56, Jan. 2018, doi: 10.1016/j.erss.2017.10.045.

[48] K. Mikami, "State-supported science and imaginary lock-in: The case of regenerative medicine in Japan," *Sci. Cult.*, vol. 24, no. 2, pp. 183–204, Apr. 2015, doi: 10.1080/09505431.2014.945410.

[49] S.-H. Kim, "The politics of human embryonic stem cell research in South Korea: Contesting national sociotechnical imaginaries," *Sci. Cult.*, vol. 23, no. 3, pp. 293–319, Jul. 2014, doi: 10.1080/09505431.2013.860095.

[50] S. Jasanoff and S.-H. Kim, "Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea," *Minerva*, vol. 47, no. 2, pp. 119–146, Jun. 2009, doi: 10.1007/s11024-009-9124-4.

[51] N. Cristianini, T. Scantamburlo, and J. Ladyman, "The social turn of artificial intelligence," *AI Soc.*, vol. 38, no. 1, pp. 89–96, Feb. 2023, doi: 10.1007/s00146-021-01289-8.

[52] E. Coiera, "Putting the technical back into socio-technical systems research," *Int. J. Med. Inf.*, vol. 76, pp. S98–S103, 2007.

[53] O. Coutard and S. Guy, "STS and the city: Politics and practices of hope," *Sci. Technol. Hum. Values*, vol. 32, no. 6, pp. 713–734, Nov. 2007, doi: 10.1177/0162243907303600.

[54] H. Collins, R. Evans, and M. Weinel, “STS as science or politics?,” *Soc. Stud. Sci.*, vol. 47, no. 4, pp. 580–586, Aug. 2017, doi: 10.1177/0306312717710131.

[55] G. Downey and T. Zuiderent-Jerak, *Making and Doing: Activating STS Through Knowledge Expression and Travel*. MIT Press, Cambridge, MA, USA, 2021. Accessed: Apr. 18, 2026. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=Kyk5EAAAQBAJ&oi=fnd&pg=PR9

[56] L. Garforth, “In/visibilities of research: Seeing and knowing in STS,” *Sci. Technol. Hum. Values*, vol. 37, no. 2, pp. 264–285, Mar. 2012, doi: 10.1177/0162243911409248.

[57] J. Law, “On sociology and STS,” *Sociol. Rev.*, vol. 56, no. 4, pp. 623–649, Nov. 2008, doi: 10.1111/j.1467-954X.2008.00808.x.

[58] J. Law, “Knowledge places,” *Link. STS Soc. Sci. Transform. Soc.*, 2011, Accessed: Apr. 18, 2026. [Online]. Available: http://heterogeneities.net/publications/Law2011KnowledgePlaces.pdf

[59] G. Ottinger, “Changing knowledge, local knowledge, and knowledge gaps: STS insights into procedural justice,” *Sci. Technol. Hum. Values*, vol. 38, no. 2, pp. 250–270, Mar. 2013, doi: 10.1177/0162243912469669.

[60] H. Radder, “The politics of STS,” *Soc. Stud. Sci.*, vol. 28, no. 2, pp. 325–331, Apr. 1998, doi: 10.1177/030631298028002005.

[61] J. Law, “1 STS as method,” *Handb. Sci. Technol. Stud.*, vol. 31, 2016, Accessed: Apr. 18, 2026. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=4GTUDQAAQBAJ&oi=fnd&pg=PA31

[62] G. Deleuze and F. Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia*, 2004th ed. New York, NY, USA: Continuum, 1988.

[63] E. W. Holland, “Deleuze and Guattari’s’ A Thousand Plateaus’,” 2013, Accessed: Nov. 16, 2025. [Online]. Available: https://www.torrossa.com/it/resources/an/5203642

[64] R. Pringle and D. Landi, “Re-reading Deleuze and Guattari’s A Thousand Plateaus,” *Ann. Leis. Res.*, vol. 20, no. 1, pp. 117–122, Jan. 2017, doi: 10.1080/11745398.2016.1204138.

[65] S. Bowden, “Assembling agency: Expression, action, and ethics in Deleuze and Guattari’s A Thousand Plateaus,” *South. J. Philos.*, vol. 58, no. 3, pp. 383–400, Sep. 2020, doi: 10.1111/sjp.12384.

[66] B. Latour and S. Woolgar, *Laboratory Life: The Construction of Scientific Facts*, 1st ed. Beverly Hills, CA, USA: Sage Publications, Inc., 1979. doi: 10.2307/j.ctt32bbxc.

[67] B. Latour, “On actor-network theory: A few clarifications,” *Soz. Welt*, pp. 369–381, 1996.

[68] A. Bousquet, “Welcome to the machine: Rethinking technology and society through assemblage theory,” in *Reassembling International Theory*, M. Acuto and

S. Curtis, Eds., London: Palgrave Macmillan UK, 2014, pp. 91–97. doi: 10.1057/9781137383969_11.

[69] B. Malinowski, “Ethnology and the study of society,” *Economica*, no. 6, p. 208, Oct. 1922, doi: 10.2307/2548314.

[70] G. Ryle, “Thinking and reflecting,” *R. Inst. Philos. Suppl.*, vol. 1, pp. 210–226, 1968.

[71] G. Clifford, “Thick description: Toward an interpretive theory of culture,” *Interpret. Cult. Sel. Essays*, vol. 3, pp. 5–6, 1973.

[72] T. Mostowlansky and A. Rota, “Emic and etic,” *Open Encycl. Anthropol.*, Nov. 2020, doi: 10.29164/20emicetic.

[73] D. Boyd, “Social network sites as networked publics: Affordances, dynamics, and implications,” in *A networked self*, Routledge, 2010, pp. 47–66. Accessed: Dec. 02, 2024. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.4324/9780203876527-8/social-network-sites-networked-publics-affordances-dynamics-implications-danah-boyd

[74] L. Lessig, “The law of the horse: What cyber law might teach,” *Harv Rev*, vol. 113, p. 501, 1999.

[75] K. Earl Rinehart, “Abductive analysis in qualitative inquiry,” *Qual. Inq.*, vol. 27, no. 2, pp. 303–311, Feb. 2021, doi: 10.1177/1077800420935912.

[76] J. Reichertz, “Induction, deduction, abduction,” *SAGE Handb. Qual. Data Anal.*, pp. 123–135, 2014.

[77] I. Tavory and S. Timmermans, *Abductive analysis: Theorizing qualitative research*. University of Chicago press, 2022. Accessed: Oct. 26, 2025. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=5OYvBAAAQBAJ&oi=fnd

[78] P. Atkinson, “The spirit of abduction,” *Contemp. Sociol. J. Rev.*, vol. 47, no. 4, pp. 415–417, Jul. 2018, doi: 10.1177/0094306118779812b.

[79] V. Bajc, “Abductive ethnography of practice in highly uncertain conditions,” *Ann. Am. Acad. Pol. Soc. Sci.*, vol. 642, no. 1, pp. 72–85, Jul. 2012, doi: 10.1177/0002716212438197.

[80] J. Berger, B. Nanay, and J. Quilty-Dunn, “Unconscious perceptual justification*,” *Inquiry*, vol. 61, no. 5–6, pp. 569–589, Aug. 2018, doi: 10.1080/0020174X.2018.1432413.

[81] P. W. Halligan and J. C. Marshall, “Supernumerary phantom limb after right hemispheric stroke,” *J. Neurol. Neurosurg. Psychiatry*, vol. 59, no. 3, p. 341, 1995.

[82] A. Mallozzi, “What is absolute modality?,” *Inquiry*, vol. 0, no. 0, pp. 1–26, doi: 10.1080/0020174X.2023.2221670.

[83] J. Hintikka, *The modes of modality*. Cornell University Press, 1979. Accessed: Oct. 26, 2025. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=ie6J_XoVJYEC&oi=fnd&pg=PA65

[84] J. Nuyts, “Modality: Overview and linguistic issues,” *Expr. Modality*, vol. 1, p. 1, 2008.

[85] W. Tullett, “State of the field: Sensory history,” *History*, vol. 106, no. 373, pp. 804–820, 2021, doi: 10.1111/1468-229X.13246.

[86] R. C. Rath, “Hearing American history,” *J. Am. Hist.*, vol. 95, no. 2, pp. 417–431, 2008.

[87] S. Pink, “Multimodality, multisensoriality and ethnographic knowing: social semiotics and the phenomenology of perception,” *Qual. Res.*, vol. 11, no. 3, pp. 261–276, Jun. 2011, doi: 10.1177/1468794111399835.

[88] S. Down and M. Hughes, “When the ‘subject’ and the ‘researcher’ speak together: Co-producing organizational ethnography,” *Organ. Ethnogr. Stud. Complex. Everyday Life*, pp. 83–98, 2009.

[89] L. Enria, “Co-producing knowledge through participatory theatre: reflections on ethnography, empathy and power,” *Qual. Res.*, vol. 16, no. 3, pp. 319–329, Jun. 2016, doi: 10.1177/1468794115615387.

[90] M. Presnell, “Postmodern ethnography: From representing the other to co-producing a text,” *Interpret. Approaches Interpers. Commun.*, pp. 11–43, 1994.

[91] M. R. Westmoreland, “Multimodality: Reshaping anthropology,” *Annu. Rev. Anthropol.*, vol. 51, no. 1, pp. 173–194, Oct. 2022, doi: 10.1146/annurev-anthro-121319-071409.

[92] E. Yılmaz, “Your turn as an example of multi-modal, ethnographic and collective documentary,” *J. Soc. Sci.*, vol. 8, no. 16, pp. 124–137, 2024.

[93] C. J. Dance, J. Ward, and J. Simner, “What is the link between mental imagery and sensory sensitivity? Insights from aphantasia,” *Perception*, vol. 50, no. 9, pp. 757–782, Sep. 2021, doi: 10.1177/03010066211042186.

[94] B. Nanay, “Mental imagery,” in *The Stanford Encyclopedia of Philosophy*, Winter 2021., E. N. Zalta, Ed., Metaphysics Research Lab, Stanford University, 2021. Accessed: Sep. 28, 2025. [Online]. Available: https://plato.stanford.edu/archives/win2021/entries/mental-imagery/

[95] J. Pearson, T. Naselaris, E. A. Holmes, and S. M. Kosslyn, “Mental imagery: functional mechanisms and clinical applications,” *Trends Cogn. Sci.*, vol. 19, no. 10, pp. 590–602, 2015.

[96] M. Arcangeli, “The two faces of mental imagery,” *Philos. Phenomenol. Res.*, vol. 101, no. 2, pp. 304–322, Sep. 2020, doi: 10.1111/phpr.12589.

[97] B. Rettler and A. M. Bailey, “Object,” in *The Stanford Encyclopedia of Philosophy*, Spring 2026., E. N. Zalta and U. Nodelman, Eds., Metaphysics Research Lab, Stanford University, 2026. Accessed: Apr. 04, 2026. [Online]. Available: https://plato.stanford.edu/archives/spr2026/entries/object/

[98] B. Latour, *Science in action: How to follow scientists and engineers through society*. Harvard university press, 1987. Accessed: Apr. 04, 2026. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=sC4bk4DZXTQC&oi=fnd&pg=PA

19&dq=Science+in+Action&ots=WdkIAtdaTD&sig=a_9mksGC3DlEDBa7Sk5SiCe7drk

[99] J. Law, “Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity,” *Syst. Pract.*, vol. 5, no. 4, pp. 379–393, Aug. 1992, doi: 10.1007/BF01059830.

[100] D. E. Tabachnick, “Techne, technology and tragedy,” *Techné Res. Philos. Technol.*, vol. 7, no. 3, 2004.

[101] R. Meagher, “Technê,” *Perspecta*, vol. 24, pp. 159–164, 1988, doi: 10.2307/1567132.

[102] K. R. Gibson and T. Ingold, *Tools, Language and Cognition in Human Evolution*. Cambridge, UK: Cambridge University Press, 1993.

[103] A. Bousquet and S. Curtis, “Beyond models and metaphors: complexity theory, systems thinking and international relations,” *Camb. Rev. Int. Aff.*, vol. 24, no. 1, pp. 43–62, Mar. 2011, doi: 10.1080/09557571.2011.558054.

[104] K. Grint and S. Woolgar, *The machine at work: Technology, work and organization*. John Wiley & Sons, 2013. Accessed: Nov. 02, 2025. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=7c1FAAAAQBAJ&oi=fnd&pg=PA1958

[105] M. Ford, *Weapon of Choice: Small Arms and the Culture of Military Innovation*. Oxford, UK: Oxford University Press, 2017.

[106] A. Bousquet, “Lethal visions: the eye as function of the weapon,” *Crit. Stud. Secur.*, vol. 5, no. 1, pp. 62–80, Jan. 2017, doi: 10.1080/21624887.2017.1329471.

[107] J. R. Lindsay, “Target practice: Counterterrorism and the amplification of data friction,” *Sci. Technol. Hum. Values*, vol. 42, no. 6, pp. 1061–1099, Nov. 2017, doi: 10.1177/0162243917727353.

[108] J. Weber, “Keep adding. On kill lists, drone warfare and the politics of databases,” *Environ. Plan. Soc. Space*, vol. 34, no. 1, pp. 107–125, Feb. 2016, doi: 10.1177/0263775815623537.

[109] A. Malm, “Operational military violence: A cartography of bureaucratic minds and practices,” PhD Thesis, University of Gothenburg, Gothenburg, Sweden, 2019. Accessed: Jan. 29, 2026. [Online]. Available: https://gupea.ub.gu.se/handle/2077/58611

[110] T. Blackmore, “Dead slow: Unmanned aerial vehicles loitering in battlespace,” *Bull. Sci. Technol. Soc.*, vol. 25, no. 3, pp. 195–214, Jun. 2005, doi: 10.1177/0270467605276097.

[111] E. Schwarz, “Cybernetics at war: Military artificial intelligence, weapon systems and the de-skilled moral agent 1,” in *Routledge Handbook of the Future of Warfare*, Routledge, 2023, pp. 297–307. Accessed: Nov. 02, 2025. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.4324/9781003299011-32/cybernetics-war-elke-schwarz

[112] “Authors | Nmap Network Scanning.” Accessed: Mar. 10, 2026. [Online]. Available: https://nmap.org/book/man-author.html

[113] “The History and Future of Nmap | Nmap Network Scanning.” Accessed: Mar. 10, 2026. [Online]. Available: https://nmap.org/book/history-future.html

[114] “Specifying Target Hosts and Networks | Nmap Network Scanning.” Accessed: May 18, 2026. [Online]. Available: https://nmap.org/book/host-discovery-specify-targets.html

[115] “Finding an Organization’s IP Addresses | Nmap Network Scanning.” Accessed: Mar. 10, 2026. [Online]. Available: https://nmap.org/book/host-discovery-find-ips.html

[116] “Chapter 3. Host Discovery (‘Ping Scanning’) | Nmap Network Scanning.” Accessed: Mar. 10, 2026. [Online]. Available: https://nmap.org/book/host-discovery.html

[117] “Chapter 4. Port Scanning Overview | Nmap Network Scanning.” Accessed: Mar. 10, 2026. [Online]. Available: https://nmap.org/book/port-scanning.html

[118] “Determining Firewall Rules | Nmap Network Scanning.” Accessed: Mar. 18, 2026. [Online]. Available: https://nmap.org/book/determining-firewall-rules.html

[119] M. Curtis Allen, “Compression and noise,” *J. Aesthet. Phenomenol.*, vol. 9, no. 2, pp. 101–117, Jul. 2022, doi: 10.1080/20539320.2022.2143652.

[120] “Command-line Flags | Nmap Network Scanning.” Accessed: Mar. 11, 2026. [Online]. Available: https://nmap.org/book/port-scanning-options.html

[121] A.-L. Barabási and E. Bonabeau, “Scale-free networks,” *Sci. Am.*, vol. 288, no. 5, pp. 60–69, 2003.

[122] D. J. Watts and S. H. Strogatz, “Collective dynamics of ‘small-world’networks,” *nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[123] L. A. N. Amaral, A. Scala, M. Barthélémy, and H. E. Stanley, “Classes of small-world networks,” *Proc. Natl. Acad. Sci.*, vol. 97, no. 21, pp. 11149–11152, Oct. 2000, doi: 10.1073/pnas.200327197.

[124] “Subverting Intrusion Detection Systems | Nmap Network Scanning.” Accessed: Mar. 12, 2026. [Online]. Available: https://nmap.org/book/subvert-ids.html

[125] M. Kac, “Can one hear the shape of a drum?,” *Am. Math. Mon.*, vol. 73, no. 4P2, pp. 1–23, Apr. 1966, doi: 10.1080/00029890.1966.11970915.

[126] “Chapter 10. Detecting and Subverting Firewalls and Intrusion Detection Systems | Nmap Network Scanning.” Accessed: Mar. 18, 2026. [Online]. Available: https://nmap.org/book/firewalls.html

[127] L. P. Muller, “Cybersecurity in practice: The vigilant logic of kill chains and threat construction,” *Eur. J. Int. Secur.*, vol. 10, no. 2, pp. 231–251, May 2025, doi: 10.1017/eis.2024.27.

[128] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains,” *Lead. Issues Inf. Warf. Secur. Res.*, vol. 1, no. 1, p. 80, 2011.

[129] “Running your first scan with Burp Suite Professional - PortSwigger.” Accessed: Mar. 19, 2026. [Online]. Available: https://portswigger.net

[130] “Proxy intercept - PortSwigger.” Accessed: Mar. 26, 2026. [Online]. Available: https://portswigger.net

[131] “Burp Intruder - PortSwigger.” Accessed: Mar. 26, 2026. [Online]. Available: https://portswigger.net

[132] “Burp - Web Application Security, Testing, & Scanning - PortSwigger.” Accessed: Mar. 26, 2026. [Online]. Available: https://portswigger.net/burp

[133] D. Stuttard and M. Pinto, *The Web Application Hacker’s Handbook: Discovering and Exploiting Security Flaws*, 1st ed. Indianapolis, Indiana, USA: Wiley Publishing, Inc., 2008.

[134] “About us - PortSwigger.” Accessed: Mar. 26, 2026. [Online]. Available: https://portswigger.net

[135] “PORTSWIGGER LTD persons with significant control - Find and update company information - GOV.UK.” Accessed: Mar. 26, 2026. [Online]. Available: https://find-and-update.company-information.service.gov.uk/company/06719143/persons-with-significant-control

[136] “The Web Application Hacker’s Handbook | Web Security Academy.” Accessed: Mar. 26, 2026. [Online]. Available: https://portswigger.net

[137] C. Leuprecht, J. Szeman, and D. B. Skillicorn, “The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity,” *Contemp. Secur. Policy*, vol. 40, no. 3, pp. 382–407, Jul. 2019, doi: 10.1080/13523260.2019.1590960.

[138] V. Kelley, “Keeping it on the surface: design, surfaces and taste,” in *The Routledge Companion to Design Studies*, Routledge, 2016, pp. 123–134. Accessed: Mar. 27, 2026. [Online]. Available: https://api.taylorfrancis.com/content/chapters/edit/download?identifierName=doi&identifierValue=10.4324/9781315562087-13&type=chapterpdf

[139] “Burp Intruder payload positions - PortSwigger.” Accessed: Mar. 27, 2026. [Online]. Available: https://portswigger.net

[140] “Getting started with Burp Intruder - PortSwigger.” Accessed: Mar. 27, 2026. [Online]. Available: https://portswigger.net

[141] C. L. Jurkiewicz, “Big data, big concerns: Ethics in the digital age,” *Public Integr.*, vol. 20, no. sup1, pp. S46–S59, Jan. 2018, doi: 10.1080/10999922.2018.1448218.

[142] R. Herschel and V. M. Miori, “Ethics & big data,” *Technol. Soc.*, vol. 49, pp. 31–36, 2017.

[143] N. M. Richards and J. H. King, “Big data ethics,” *Wake For. Rev*, vol. 49, p. 393, 2014.

[144] K. P. Schneider, “Methods and ethics of data collection,” *Methods Pragmat.*, vol. 37, 2018, Accessed: Mar. 31, 2026. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=6zF1DwAAQBAJ&oi=fnd&pg=P

A37&dq=ethics+AND+mass+data+collection&ots=QrnjifoL0k&sig=C4ZHG5QEGbngAQSF5YGcr8eoq-A

[145] D. Wainwright and S. Sambrook, “The ethics of data collection: unintended consequences?,” *J. Health Organ. Manag.*, vol. 24, no. 3, pp. 277–287, 2010.

[146] T. L. Rittenburg and M. B. Lunde, “Ethical issues in target marketing: inclusion, exclusion, and consumer vulnerability,” in *Handbook of Research on Ethnic and Intra-Cultural Marketing*, Cheltenham, UK: Edward Elgar Publishing, 2022, pp. 14–28.

[147] G. A. Callanan, D. F. Perri, and S. M. Tomkowicz, “Targeting vulnerable populations: The ethical implications of data mining, automated prediction, and focused marketing,” *Bus. Soc. Rev.*, vol. 126, no. 2, pp. 155–167, Jun. 2021, doi: 10.1111/basr.12233.

[148] J. Guelke, “The ethics of mass surveillance,” in *The Routledge Handbook to Rethinking Ethics in International Relations*, Routledge, 2020, pp. 283–296. Accessed: Mar. 31, 2026. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.4324/9781315613529-25/ethics-mass-surveillance-john-guelke

[149] N. C. Smith and E. Cooper-Martin, “Ethics and Target Marketing: The Role of Product Harm and Consumer Vulnerability,” *J. Mark.*, vol. 61, no. 3, pp. 1–20, Jul. 1997, doi: 10.1177/002224299706100301.

[150] E. Reichborn-Kjennerud, *The World According to Military Targeting*. Cambridge, MA, USA: MIT Press, 2025. Accessed: Oct. 27, 2025. [Online]. Available: https://books.google.com/books?hl=sv&lr=&id=nSIdEQAAQBAJ&oi=fnd&pg=PR5

[151] S. Caltagirone, A. Pendergast, and C. Betz, “The diamond model of intrusion analysis.” US Department of Defense, Fort Meade, USA, 2013. Accessed: Mar. 29, 2026. [Online]. Available: https://apps.dtic.mil/sti/html/tr/ADA586960/

[152] L. Suchman, K. Follis, and J. Weber, “Tracking and targeting: Sociotechnologies of (in)security,” *Sci. Technol. Hum. Values*, vol. 42, no. 6, pp. 983–1002, Nov. 2017, doi: 10.1177/0162243917731524.

[153] J. Packer and J. Reeves, “Romancing the drone: Military desire and anthropophobia from SAGE to swarm,” *Can. J. Commun.*, vol. 38, no. 3, pp. 309–332, Sep. 2013, doi: 10.22230/cjc.2013v38n3a2681.

[154] A. Bousquet, “Cyberneticizing the American war machine: science and computers in the Cold War,” *Cold War Hist.*, vol. 8, no. 1, pp. 77–102, Feb. 2008, doi: 10.1080/14682740701791359.

[155] S. D. Shaw and G. Nave, “Thinking—fast, slow, and artificial: How AI is reshaping human reasoning and the rise of cognitive surrender,” Jan. 11, 2026, *Social Science Research Network, Rochester, NY*: 6097646. doi: 10.2139/ssrn.6097646.

[156] M. C. Ghanem and T. M. Chen, “Reinforcement learning for efficient network penetration testing,” *Information*, vol. 11, no. 1, p. 6, Jan. 2020, doi: 10.3390/info11010006.

[157] R. H. Pherson, R. J. Heuer, *Structured Analytic Techniques for Intelligence Analysis,* Washington, D.C, USA: CQ Press, 2019.

[158] R. J. Heuer, *Psychology of Intelligence Analysis*. CIA Center for the Study of Intelligence, 1999. Accessed: May 06, 2026. [Online]. Available: https://books.google.com/books?hl=sv&lr=&id=rRXFhKAiG8gC&oi=fnd&pg=PR7

[159] Central Intelligence Agency, “A Primer: Structured Analytic Techniques for Improving Intelligence Analysis.” CIA Center for the Study of Intelligence, 2009. Accessed: May 06, 2026. [Online]. Available: https://www.osint.org/wp-content/uploads/2018/05/structured-analytic-techniques.pdf

[160] S. Artner, R. Girven, and J. Bruce, *Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community*. RAND Corporation, 2016. doi: 10.7249/RR1408.

[161] W. Chang, E. Berdini, D. R. Mandel, and P. E. Tetlock, “Restructuring structured analytic techniques in intelligence,” *Intell. Natl. Secur.*, vol. 33, no. 3, pp. 337–356, Apr. 2018, doi: 10.1080/02684527.2017.1400230.

[162] M. Denzler, “Revisiting the psychology of structured analytical techniques,” *Int. J. Intell. CounterIntelligence*, vol. 37, no. 2, pp. 634–648, Apr. 2024, doi: 10.1080/08850607.2023.2243803.

[163] M. K. Dhami, I. K. Belton, and K. E. Careless, “Critical review of analytic techniques,” in *2016 European Intelligence and Security Informatics Conference (EISIC)*, Aug. 2016, pp. 152–155. doi: 10.1109/EISIC.2016.039.

[164] M. J. Ard, “Structured analytic techniques: A pragmatic approach,” *Int. J. Intell. CounterIntelligence*, vol. 37, no. 2, pp. 617–633, Apr. 2024, doi: 10.1080/08850607.2023.2241308.

Appendix 1 – Non-Exclusive Licence for Reproduction and Publication[21]

I, Konor Sajti,

1 grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis , supervised by

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2 I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3 I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

[21] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Search Terms Used to Identify Academic Literature

The following is a near-complete list of all searches conducted as part of this research. Note that no formal selection criteria was applied to this data set, as systematic literature review was not the purpose.

Search Term	Search Engine	Created time
"Ivan Sutherland"	scholar	November 14, 2024 10:46 AM
"Super Cockpit" AND 1986	scholar	November 14, 2024 10:51 AM
"visually coupled systems"	scholar	November 14, 2024 10:52 AM
"virtual control interface" AND "military" -sport	scholar	November 14, 2024 10:53 AM
"modality" AND "military targeting"	scholar	November 14, 2024 10:54 AM
weapon delivery envelope	duckduckgo	November 14, 2024 10:59 AM
"weapon delivery envelopes"	scholar	November 14, 2024 11:00 AM
"threat warning systems"	scholar	November 14, 2024 11:03 AM
"terrain maps"	scholar	November 14, 2024 11:04 AM
"terrain maps" AND "military"	scholar	November

		14, 2024 11:05 AM
"terrain maps" AND "military vision"	scholar	November 14, 2024 11:05 AM
"man-in-the-loop" AND "military"	scholar	November 14, 2024 11:06 AM
"live cartographic interface" AND "military"	scholar	November 14, 2024 11:10 AM
"cartographic interface" AND "military"	scholar	November 14, 2024 11:11 AM
"god's-eye" AND "military"	scholar	November 14, 2024 11:12 AM
"god's-eye" AND "cybersecurity"	scholar	November 14, 2024 11:13 AM
telepresence	scholar	November 14, 2024 11:15 AM
"synthetic vision system"	scholar	November 14, 2024 11:16 AM
"perceptual architecture"	scholar	November 14, 2024 11:20 AM
"martial imagery" "fix" "target"	scholar	November 14, 2024 11:31 AM
"martial gaze" "fix" "target"	scholar	November 14, 2024 11:32 AM
"active recon"	scholar	November 14, 2024 9:25 PM

"active reconnaissance"	scholar	November 14, 2024 9:25 PM
"active reconnaissance" "military"	scholar	November 14, 2024 9:26 PM
"weapon systems" AND "critical studies"	scholar	November 15, 2024 10:35 AM
"the hacker's dictionary" OR "jargon file"	scholar	November 15, 2024 11:00 PM
"phantasmal war"	scholar	November 16, 2024 9:47 AM
scientific categorization and the state	scholar	November 16, 2024 10:33 AM
	ieeexplore	November 16, 2024 12:39 PM
author:"Shoshana Zuboff" AND "text"	scholar	November 19, 2024 10:00 AM
author:"Shoshana Zuboff" AND "text" -surveillance	scholar	November 19, 2024 10:01 AM
Army Map Service Robert C. Miller AND (geodesy | geography | mapping)	scholar	November 20, 2024 9:44 AM
military imagery	scholar	November 20, 2024 10:28 AM
"cybernetic steering" AND target*	scholar	November 20, 2024 11:02 AM
"contour maps"	scholar	November 20, 2024 11:08 AM

"terrain entropy"	scholar	November 20, 2024 11:23 AM
"Waldo Tobler"	scholar	November 20, 2024 11:26 AM
"design science"	scholar	November 22, 2024 5:41 PM
author"Martin Libicki"	scholar	November 25, 2024 4:21 PM
battlefield surveillance	scholar	November 25, 2024 4:22 PM
"visual warfare"	scholar	November 25, 2024 4:25 PM
"camouflage" AND "perception"	scholar	November 25, 2024 4:27 PM
"camouflage" AND "computer vision"	scholar	November 25, 2024 4:30 PM
visual warfare and cybernetics and technology	scholar	November 25, 2024 4:39 PM
author:"Hanna Rose Shell"	scholar	November 25, 2024 4:58 PM
"Abbott Thayer"	scholar	November 25, 2024 5:14 PM
"Lucien-Victor Guirand de Scévola"	scholar	November 25, 2024 5:16 PM
"visual warfare" AND ("netting" OR "screening")	scholar	November 25, 2024 5:21 PM

"fractal pattern" AND "camouflage"	scholar	November 25, 2024 10:19 PM
"digital camouflage"	scholar	November 25, 2024 10:19 PM
"camouflage" AND "cybersecurity"	scholar	November 25, 2024 10:20 PM
"CrowdStrike" AND ("camouflage" OR "deception")	scholar	November 25, 2024 10:33 PM
"weapons design" -against -moral	scholar	November 26, 2024 7:41 PM
derek gregory drones	scholar	November 26, 2024 10:18 PM
"combat cloud"	scholar	November 27, 2024 5:28 PM
"imaginaries" AND "cyberwar"	scholar	November 28, 2024 10:24 PM
"weapons platform" AND "cyber"	scholar	December 3, 2024 9:03 AM
"ranged" AND "cyber" AND "weapon"	scholar	December 3, 2024 9:04 AM
"cyber" AND "weapons system"	scholar	December 3, 2024 9:06 AM
"information ecology"	scholar	December 26, 2024 11:06 AM

"ecomyopia"	scholar	December 26, 2024 11:12 AM
derivative wars - Google Scholar	scholar	January 7, 2025 10:16 AM
AI AND martial - Google Scholar	scholar	April 15, 2025 7:24 AM
"soldiering" - Google Scholar	scholar	April 30, 2025 7:47 AM
"knowledge engineering" - Google Scholar	scholar	April 30, 2025 8:08 AM
"weapon" AND "assemblage" AND "understand" - Google Scholar	scholar	November 16, 2025 3:01 PM
military maneuver - Google Scholar	scholar	November 16, 2025 3:01 PM
anthropology AND abductive - Google Scholar	scholar	November 16, 2025 3:02 PM
ingold AND perception - Google Scholar	scholar	November 16, 2025 3:03 PM
touch AND digital - Google Scholar	scholar	November 16, 2025 3:04 PM
"MIT" AND hacker|hack|hacking AND history - Google Scholar	scholar	November 16, 2025 3:06 PM
"early hacking" OR "early hacker" - Google Scholar	scholar	November 16, 2025 3:07 PM
military doctrine | Taylor & Francis Online	tandfonline	November 16, 2025 3:11 PM

"artefact" OR "artifact" AND "cybersecurity" AND... - Google Scholar	scholar	November 16, 2025 3:11 PM
[All: perception] AND [All: drone] | Taylor & Francis Online	tandfonline	November 16, 2025 3:13 PM
All: offensive cyberspace operations | Taylor & Francis Online	tandfonline	November 16, 2025 3:14 PM
"offensive" AND "cyber" AND ("case study" OR "case studies") - Google Scholar	scholar	November 16, 2025 3:17 PM
method of science and technology studies - Google Scholar	scholar	November 16, 2025 3:21 PM
method of critical technology studies - Google Scholar	scholar	November 16, 2025 3:22 PM
method of critical war studies - Google Scholar	scholar	November 16, 2025 3:22 PM
"induction" AND "hard sciences" - Google Scholar	scholar	November 16, 2025 3:22 PM
""Recorded" "Future"" AND site:wikileaks.org - Sök på Google	google	February 11, 2026 3:26 PM
""Recorded" "Future"" AND "Form S-1" AND site:sec.gov - Sök på Google	google	February 11, 2026 3:26 PM
"Ivan Sutherland"	scholar	November 14, 2024 10:46 AM
"Super Cockpit" AND 1986	scholar	November 14, 2024 10:51 AM
"visually coupled systems"	scholar	November

		14, 2024 10:52 AM
"virtual control interface" AND "military" -sport	scholar	November 14, 2024 10:53 AM
"modality" AND "military targeting"	scholar	November 14, 2024 10:54 AM
weapon delivery envelope	scholar	November 14, 2024 10:59 AM
"weapon delivery envelopes"	scholar	November 14, 2024 11:00 AM
"threat warning systems"	scholar	November 14, 2024 11:03 AM
"terrain maps"	scholar	November 14, 2024 11:04 AM
"terrain maps" AND "military"	scholar	November 14, 2024 11:05 AM
"terrain maps" AND "military vision"	scholar	November 14, 2024 11:05 AM
"man-in-the-loop" AND "military"	scholar	November 14, 2024 11:06 AM
"live cartographic interface" AND "military"	scholar	November 14, 2024 11:10 AM
"cartographic interface" AND "military"	scholar	November 14, 2024 11:11 AM
"god's-eye" AND "military"	scholar	November 14, 2024 11:12 AM
"god's-eye" AND "cybersecurity"	scholar	November

		14, 2024 11:13 AM
telepresence	scholar	November 14, 2024 11:15 AM
"synthetic vision system"	scholar	November 14, 2024 11:16 AM
"perceptual architecture"	scholar	November 14, 2024 11:20 AM
"martial imagery" "fix" "target"	scholar	November 14, 2024 11:31 AM
"martial gaze" "fix" "target"	scholar	November 14, 2024 11:32 AM
"active recon"	scholar	November 14, 2024 9:25 PM
"active reconnaissance"	scholar	November 14, 2024 9:25 PM
"active reconnaissance" "military"	scholar	November 14, 2024 9:26 PM
"weapon systems" AND "critical studies"	scholar	November 15, 2024 10:35 AM
"the hacker's dictionary" OR "jargon file"	scholar	November 15, 2024 11:00 PM
"phantasmal war"	scholar	November 16, 2024 9:47 AM
scientific categorization and the state	scholar	November 16, 2024 10:33 AM
	scholar	November

		16, 2024 12:39 PM
author:"Shoshana Zuboff" AND "text"	scholar	November 19, 2024 10:00 AM
author:"Shoshana Zuboff" AND "text" -surveillance	scholar	November 19, 2024 10:01 AM
Army Map Service Robert C. Miller AND (geodesy | geography | mapping)	scholar	November 20, 2024 9:44 AM
military imagery	scholar	November 20, 2024 10:28 AM
"cybernetic steering" AND target*	scholar	November 20, 2024 11:02 AM
"contour maps"	scholar	November 20, 2024 11:08 AM
"terrain entropy"	scholar	November 20, 2024 11:23 AM
"Waldo Tobler"	scholar	November 20, 2024 11:26 AM
"design science"	scholar	November 22, 2024 5:41 PM
author"Martin Libicki"	scholar	November 25, 2024 4:21 PM
battlefield surveillance	scholar	November 25, 2024 4:22 PM
"visual warfare"	scholar	November 25, 2024 4:25 PM
"camouflage" AND "perception"	scholar	November

		25, 2024 4:27 PM
"camouflage" AND "computer vision"	scholar	November 25, 2024 4:30 PM
visual warfare and cybernetics and technology	scholar	November 25, 2024 4:39 PM
author:"Hanna Rose Shell"	scholar	November 25, 2024 4:58 PM
"Abbott Thayer"	scholar	November 25, 2024 5:14 PM
"Lucien-Victor Guirand de Scévola"	scholar	November 25, 2024 5:16 PM
"visual warfare" AND ("netting" OR "screening")	scholar	November 25, 2024 5:21 PM
"fractal pattern" AND "camouflage"	scholar	November 25, 2024 10:19 PM
"digital camouflage"	scholar	November 25, 2024 10:19 PM
"camouflage" AND "cybersecurity"	scholar	November 25, 2024 10:20 PM
"CrowdStrike" AND ("camouflage" OR "deception")	scholar	November 25, 2024 10:33 PM
"weapons design" -against -moral	scholar	November 26, 2024 7:41 PM
derek gregory drones	scholar	November 26, 2024 10:18 PM
"combat cloud"	scholar	November

		27, 2024 5:28 PM
"imaginaries" AND "cyberwar"	scholar	November 28, 2024 10:24 PM
"weapons platform" AND "cyber"	scholar	December 3, 2024 9:03 AM
"ranged" AND "cyber" AND "weapon"	scholar	December 3, 2024 9:04 AM
"cyber" AND "weapons system"	scholar	December 3, 2024 9:06 AM
"information ecology"	scholar	December 26, 2024 11:06 AM
"ecomyopia"	scholar	December 26, 2024 11:12 AM
derivative wars - Google Scholar	scholar	January 7, 2025 10:16 AM
AI AND martial - Google Scholar	scholar	April 15, 2025 7:24 AM
"soldiering" - Google Scholar	scholar	April 30, 2025 7:47 AM
"knowledge engineering" - Google Scholar	scholar	April 30, 2025 8:08 AM
"weapon" AND "assemblage" AND "understand" - Google Scholar	scholar	November 16, 2025 3:01 PM
military maneuver - Google Scholar	scholar	November

		16, 2025 3:01 PM
anthropology AND abductive - Google Scholar	scholar	November 16, 2025 3:02 PM
ingold AND perception - Google Scholar	scholar	November 16, 2025 3:03 PM
touch AND digital - Google Scholar	scholar	November 16, 2025 3:04 PM
"MIT" AND hacker|hack|hacking AND history - Google Scholar	scholar	November 16, 2025 3:06 PM
"early hacking" OR "early hacker" - Google Scholar	scholar	November 16, 2025 3:07 PM
military doctrine | Taylor & Francis Online	scholar	November 16, 2025 3:11 PM
"artefact" OR "artifact" AND "cybersecurity" AND... - Google Scholar	scholar	November 16, 2025 3:11 PM
[All: perception] AND [All: drone] | Taylor & Francis Online	scholar	November 16, 2025 3:13 PM
All: offensive cyberspace operations | Taylor & Francis Online	scholar	November 16, 2025 3:14 PM
"offensive" AND "cyber" AND ("case study" OR "case studies") - Google Scholar	scholar	November 16, 2025 3:17 PM
method of science and technology studies - Google Scholar	scholar	November 16, 2025 3:21 PM
method of critical technology studies - Google Scholar	scholar	November 16, 2025 3:22 PM
method of critical war studies - Google Scholar	scholar	November

		16, 2025 3:22 PM
"induction" AND "hard sciences" - Google Scholar	scholar	November 16, 2025 3:22 PM
""Recorded" "Future"" AND site:wikileaks.org - Sök på Google	scholar	February 11, 2026 3:26 PM
""Recorded" "Future"" AND "Form S-1" AND site:sec.gov - Sök på Google	Google	February 11, 2026 3:26 PM