

CHARLES UNIVERSITY
FACULTY OF SOCIAL SCIENCES

Institute of Political Studies
Department of Security Studies

Master's Thesis

2025

Daniela Kůstková

CHARLES UNIVERSITY
FACULTY OF SOCIAL SCIENCES
Institute of Political Studies
Department of Security Studies

**The Automatization of IMINT: the Rules of Camouflage
Redefined**

Master's Thesis

Author of the Thesis: Daniela Kůstková

Study programme: Security Studies

Supervisor: Mgr. Petr Špelda, Ph.D.

Year of the defence: 2025

Declaration

1. I hereby declare that I have compiled this thesis using the listed literature and resources only.
2. I hereby declare that my thesis has not been used to gain any other academic title.
3. I fully agree to my work being used for study and scientific purposes.

In Prague on January 6, 2025

Daniela Kůstková

References

KŮSTKOVÁ, Daniela. *The Automatization of IMINT: the Rules of Camouflage Redefined*. Praha, 2025. 66 s. Master's thesis (Mgr). Charles University, Faculty of Social Sciences, Institute of Political Studies, Department of Security Studies. Supervisor Mgr. Petr Špelda, Ph.D.

Length of the Thesis: 94 055

Abstract

This thesis examines camouflage methods against computer vision algorithms. AI-enabled tools have been deployed to analyze massive volumes of imagery data collected for intelligence purposes. However, as with any other AI model, object detectors are vulnerable to adversarial attacks. In this work, camouflage is studied as a form of visual adversarial attack deployed against AI-enabled analytical tools, represented by object detectors. Through a review of computer science literature, this thesis aims to expand the discussion in security studies by exploring the potential and constraints of computer vision applications, along with the security implications of these emerging technologies. Three types of adversarial attacks on object detectors were identified in the literature: adversarial camouflage attacks, adversarial patches, and imperceptible image perturbations. I conclude the thesis by arguing that militaries are unlikely to adopt the adversarial camouflage attacks proposed in the literature, despite the apparent demand for counterintelligence solutions against automatized detection. Today, sensors collecting data in various spectral bands are commonly used; therefore, camouflage solutions have to manage their signature in those spectral bands accordingly.

Abstrakt

Tato diplomová práce zkoumá maskovací metody proti algoritmům počítačového vidění. K analýze zpravodajských informací byly nasazeny nástroje využívající umělou inteligenci, aby vyřešily problém s masivním objemem sesbíraných dat. Nicméně stejně jako jiné modely umělé inteligence jsou i detektory objektů náchylné vůči adverzariálním útokům. Tato práce se věnuje kamufláži jako formě vizuálního adverzariálního útoku nasazeného proti analytickým nástrojům využívajících umělou inteligenci, zde reprezentovaných objektovými detektory. Prostřednictvím analýzy odborné literatury si tato práce klade za cíl rozšířit diskusi bezpečnostních studií analýzou potenciálu a limitů, které představuje využití počítačového vidění, a také zhodnocením bezpečnostních implikací těchto nově vznikajících technologií. V literatuře technických oborů byly identifikovány tři typy adverzariálních útoků na detektory objektů: adverzariální maskovací vzory, adverzariální záplaty a nepostřehnutelné perturbace. Diplomovou práci uzavírám argumentem, že přijetí vizuálních maskovacích metod předložených v literatuře je ve vojenském prostředí nepravděpodobné, a to i přes zjevný zájem o obranné prostředky proti automatizované detekci. Senzory sbírající

data v různých pásmech elektromagnetického spektra jsou dnes běžným vojenským vybavením, a proto toho musí být i maskovací prostředky schopné modifikovat svou stopu i za hranicí viditelného spektra.

Keywords

intelligence analysis, IMINT, object detection, camouflage, adversarial machine learning, military targets

Klíčová slova

zpravodajská analýza, IMINT, objektová detekce, kamufláž, adverzariální strojové učení, vojenské cíle

Title

The Automatization of IMINT: the Rules of Camouflage Redefined

Název práce

Automatizace IMINT: Pravidla Kamufláže Redefinována

Acknowledgement

I would like to express my sincere gratitude to my supervisor, Mgr. Petr Špelda, Ph.D., for the provided guidance and support throughout the course of this thesis.

Table of Contents

Introduction	8
1. Literature Review.....	11
1.1 Intelligence and the integration of AI-enabled analytical tools	11
1.2 Camouflage methods against computer vision	15
2. Introduction of relevant theoretical concepts	18
2.1 Intelligence.....	18
2.2 Imagery intelligence (IMINT)	21
2.3 Object detection as a tool of IMINT automatization.....	23
2.4 Adversarial attacks on AI models	25
2.5 Camouflage in the physical world.....	27
2.6 Camouflage in the digital space	30
3. Methodology.....	31
4. Empirical Findings	35
4.1 Review of secondary literature	35
4.1.1 Adversarial camouflage patterns	35
4.1.2 Adversarial patches.....	39
4.1.3 Imperceptible Image Perturbations.....	42
4.2 Real-world examples of adversarial techniques.....	45
4.2.1 A Russian warship	45
4.2.2 Russian aircraft covered in tires	45
4.2.3 Painted decoys.....	46
4.2.4 Inflatable decoys.....	48
5. Discussion.....	49
Conclusion.....	54

Summary	56
Shruti.....	57
List of References	59

Introduction

In 2022, a Russian warship with a bow and stern painted in a dark color was captured on satellite imagery. A visual camouflage of ships is an established method of warfare; since ancient times, ships have been painted in dark colors to blend into the sea. However, today, the story is a bit different. The camouflage design of the Russian ship was not meant to mislead a human observer but a detection algorithm deployed to analyze intelligence. The dark color was applied to visually change the shape of the ship and be reported by the algorithm as a ship of a different class, thus providing the adversary with a false picture of reality.

Today, everything on the Earth's surface is under the sight of satellite sensors. This state of extensive and constant observation, besides providing vast benefits for everyday life on the Earth and valuable scientific research opportunities, impacts the way humans organize and ensure their security. As a result, keeping any activity covert seems more challenging. Simultaneously, the technological advances in computation capabilities allowed for processing large quantities of data and their immediate interpretation.

Artificial intelligence was realized as a force that will define the human future. World powers acknowledged the importance of AI-enabled technologies and integrated their development into their national strategies.¹ The power associated with the integration of AI models is also increasingly visible in the current armed conflicts. Therefore, if we are able to assess the strength of the technologies deployed and know the limits of their use, we will be better able to evaluate the international security situation.

An AI model can be a powerful but exploitable capability at the same time. In this thesis, I focus on the vulnerability of computer vision models to deliberate visual modifications of objects appearing in the data that the model receives as input. In other words, a visual modification of an object, here discussed as camouflage, can cause a model to fail in detecting the object or classifying it in the right category. As suggested by the example of the Russian warship, such a camouflage attack can be a solution to the constant monitoring of events on the Earth's surface.

¹ Among them: "A Next Generation Artificial Development Plan" released by the State Council for the People's Republic of China in 2017. The "National Strategy for the Development of Artificial Intelligence" released by The Government of the Russian Federation in 2019. The "American Artificial Intelligence Initiative" released by the White House in 2019.

This thesis explores automatized analysis of imagery data for intelligence purposes and specifically focuses on the techniques capable of preventing the detection of objects in imagery data. Translated into technical language, this thesis addresses the issue of adversarial camouflage attacks on AI-enabled object detectors. Regarding the actors, context, and platforms, my research interest is primarily in the applicability of adversarial camouflage attacks by militaries against the activities conducted by intelligence organizations (military or not). I discuss the applicability of adversarial camouflage attacks on objects such as military equipment or vehicles. In light of the outlined military context, I am particularly interested in imagery data collected by sensors on airborne and spaceborne platforms. While object detection can be performed on images collected by various kinds of sensors (optical, thermal, or radar) the adversarial camouflage attacks presented in this thesis were proposed for images captured within the visual spectral band.

The purpose of this thesis is to bring the technical knowledge about adversarial attacks on object detectors gathered in the field of computer science closer to the researchers in social sciences. I situate the subject in the security studies discussion and thus provide a comprehensible source of information about attacks on computer vision models that is accessible to the broader academic and professional communities. The current discussion about integrating AI models into intelligence analysis takes place in isolation from experts capable of designing and implementing such models, and at the same time, computer scientists do not seem to be occupied with security-related applications of their models. With this thesis, I aim to bridge this gap between social and computer scientists.

Based on the outlined problem, this thesis seeks to answer two research questions: 1) How can object detection models be attacked by camouflage? 2) How have the AI-enabled tools impacted intelligence analysis and the use of camouflage means by militaries? To answer these questions, I review a body of secondary literature devoted to adversarial attacks on object detection models, search for significant research directions, and critically assess the applicability of the proposed adversarial attack methods in security contexts.

The thesis is organized as follows: the introduction is followed by a literature review, in which I present the state of the current discussion on the impact of AI-enabled tools on the work of the intelligence community. Then, I review the literature concerned with the use of camouflage and deception techniques against computer vision algorithms. I proceed with a theoretical chapter introducing concepts relevant to this research, including intelligence & imagery intelligence, object detection as an AI-enabled analytical tool & adversarial attacks

on AI models, and camouflage. The methodological chapter provides information on the secondary literature I gathered for my analysis. Subsequently, in the next chapter, I share my empirical findings from the reviewed secondary literature, defining three major groups of adversarial attacks on object detection models and presenting real-world examples of adversarial attacks on computer vision algorithms. Further, in the discussion, I consider possible applications of these adversarial camouflage attacks in real-world security contexts. I answer my research questions and reflect on the research in the conclusion section.

1. Literature Review

1.1 Intelligence and the integration of AI-enabled analytical tools

Adopting computer vision tools for intelligence work might imply a decrease in the analytical role of humans. How many of the collected images are nowadays analyzed by the human eye, and what portion is evaluated by a computer? What possibilities does AI present for the work of intelligence practitioners, and has it been able to gain their trust?

In this literature review section, I explore what has been written about the attitude of the intelligence community toward adopting AI. As the methodology of my research does not allow me to make sufficiently substantiated conclusions about the impact of object detection on the work of intelligence practitioners, reviewing the works of other authors provides me with at least a theoretical context based on which I can discuss the possible applications of the given technology.

When studying intelligence organizations, it needs to be taken into account that one has the opportunity to gain access only to information that does not conflict with national security interests. The level of secrecy can increase even more if strategically important emerging technologies appear in the picture. As was pointed out by Moran, Burton, and Christou, the literature on the use of AI by intelligence organizations is affected, first, by the organizations' unwillingness to expose their technological capabilities, methods, and resources to adversaries; second, by confidentiality agreements between intelligence organizations and commercial companies about the products they develop; and third, by commercial companies preventing their ideas from being stolen by rivals in the market.²

The most frequently discussed issues in the literature are the role of humans in intelligence analysis following the introduction of computationally powerful AI models, as well as the question of how to properly work with big data and AI models to produce accurate and reliable intelligence.

Puyvelde, Coulthart, and Hossain³ studied the concept of big data and the roles big data plays in the national security context. Looking at the inevitable use of machine learning

² Moran, Christopher R., Joe Burton, and George Christou. 2023. "The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying." *Journal of Global Security Studies* 8 (2). <https://doi.org/10.1093/jogss/ogad005>.

³ Puyvelde, Damien van, Stephen Coulthart, and M. Shahrar Hossain. 2017. "Beyond the Buzzword: Big Data and National Security Decision-Making." *International Affairs* 93 (6): 1397–1416. <https://doi.org/10.1093/ia/iix184>.

for big data processing, at the time of publishing of the article in 2017, the authors concluded that automated analysis did not alter the need for human judgment in national security decision-making, and neither will it fundamentally alter it in the future. This is because it does not substitute for the crucial component of intelligence analysis, which is the human ability of contextualization.

Similarly, Regens⁴ dealt with the issue of the unprecedented increase in data generated and collected in today's world and the capacity of human intelligence to identify and synthesize relevant information. He points out that asking the right questions leads to credible and relevant intelligence and this is not inherently assured by deploying AI systems in intelligence analysis. Regens argues that AI is not a substitute for human judgment. Instead, the computational capacity of AI can serve in the augmentation of human cognition, and as such it should be approached by decision-makers.

The role that remains to be played by human analysts was further analyzed by Brantly.⁵ The author argues, that to create a valuable intelligence product, one needs to use structured analytical techniques to minimize biases and form thoughtfully informed theories and hypotheses because even a strong correlation found in a large dataset is not a substitute for a rigorous scientific method. Brantly concludes that the role of a human analyst would be to correct biases and ensure the model follows rigorous scientific procedures.

Gleeson⁶ discusses the challenges and opportunities of intelligence organizations seeking to implement generative AI in their work. He argues that AI is not a quick fix to the challenge represented by the overabundance of data but rather “a strategic shift in how we think about interacting with massive volumes of data.” The author claims, that as for other information sources, generative AI models need to be sufficiently explainable and transparent to gain the trust of intelligence practitioners. He adds that intelligence analysts need to work in line with the knowledge that has been already produced within the organization before considering the understanding generated by AI.

⁴ Regens, James L. 2019. “Augmenting Human Cognition to Enhance Strategic, Operational, and Tactical Intelligence.” *Intelligence and National Security* 34 (5): 673–87. <https://doi.org/10.1080/02684527.2019.1579410>.

⁵ Brantly, Aaron F. 2018. “When Everything Becomes Intelligence: Machine Learning and the Connected World.” *Intelligence and National Security* 33 (4): 562–73. <https://doi.org/10.1080/02684527.2018.1452555>.

⁶ Gleeson, Dennis J. 2023. “Artificial Intelligence for Analysis: The Road Ahead.” *Studies in Intelligence* 67 (4).

How to correctly deploy AI systems in intelligence missions is discussed by Ish, Ettinger, and Ferris⁷ in their methodologically oriented study. They pose the question of whether replicating human performance is a sufficient reason for deploying AI systems and suggest metrics that would evaluate their impact on intelligence missions.

The opportunities and challenges of integration of AI systems into military intelligence process were analyzed by Ahmed.⁸ According to him, AI systems open new dimensions of information that would not be available for analysis due to insufficient processing capacities and allow for automatized revalidation of information that is dynamic over time. However, the systems need to be assessed whether they analyze the massive flow of data correctly and provide humans with indeed accurate interpretation of reality.

Another group of studies is concerned with the impact the integration of AI had on intelligence organizations as institutions. The authors are interested in the influence of the technology on organizations' internal processes as well as external interactions with the state and the private sector.

The article by Moran, Burton, and Christou⁹ explores how the US intelligence community leverages AI for national security purposes. The authors formulate three arguments: First, the US needs to cooperate with the commercial sector on the development of technologies since it does not possess the expertise to do it on its own. Second, AI was originally deployed mainly in the processing phase of the intelligence cycle but today it has expanded in other phases. And third, although AI will play a crucial role in global security, the US intelligence community will not be able to exploit the full potential of AI, as the collection and use of private data is legally restricted in democratic countries. Also, commercial contractors will not contribute to the weaponization of AI if it does not align with their values.

Internal processes in intelligence organizations influenced by the adoption of AI were

⁷ Ish, Daniel., Jared. Ettinger, and Christopher. Ferris. 2021. *Evaluating the Effectiveness of Artificial Intelligence Systems in Intelligence Analysis*. Santa Monica: RAND Corporation. <https://doi.org/https://doi.org/10.7249/RR-A464-1>.

⁸ Ahmed, Nizam Uddin. 2022. "INTEGRATING MACHINE LEARNING IN MILITARY INTELLIGENCE PROCESS: STUDY OF FUTURISTIC APPROACHES TOWARDS HUMAN-MACHINE." *National Defence College E-Journal 2* (1): 59–89. <https://ndcjournal.ndc.gov.bd/ndcj>.

⁹ Moran, Christopher R., Joe Burton, and George Christou. 2023. "The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying." *Journal of Global Security Studies 8* (2). <https://doi.org/10.1093/jogss/ogad005>.

studied by Vogel et al.¹⁰ Conducting interviews with intelligence practitioners, they described how intelligence practitioners perceive the use of AI technologies in their workplace and how AI affects issues such as collaboration, algorithmic transparency, accountability, and management within the US intelligence community.

The article by Pereira¹¹ proposes two frameworks, designed to evaluate the capabilities of intelligence organizations. The first identifies attack surfaces in governance mechanisms and procedures that are commonly overlooked in cybersecurity and the second is concerned with the impact of dual-use AI capabilities in modern intelligence settings. Such frameworks may help governments to assess national intelligence capabilities and threats related to AI, and create strategies and legislation accordingly.

The last theme I identified in the literature is the impact the deployment of AI-enabled technologies by intelligence has on society.

Ghioni, Taddeo and Floridi¹² reviewed the literature on governance, ethical, legal, and social implications of open source intelligence. Considering the growing reliance of OSINT on AI algorithms, they suggested weak spots in the current literature and future research directions. Most of the suggested issues result from the lack of transparency of AI models stemming from corporates' efforts to safeguard their products, the technical illiteracy of end-users, the covert nature of intelligence applications, and black box structures of algorithms making even the practitioners unable to interpret model's results. Valid results produced by AI models are required, as they might be used for serious decisions, for instance, as evidence in criminal trials. Therefore, data should be carefully filtered from misinformation to reduce biases. The authors also point out the inequality in AI expertise and access to computing power, which may favor private actors and weaken the social control practiced by state actors.

The impact of techno-vision (technologies enhancing human vision providing a near-

¹⁰ Vogel, Kathleen M., Gwendolynne Reid, Christopher Kampe, and Paul Jones. 2021. "The Impact of AI on Intelligence Analysis: Tackling Issues of Collaboration, Algorithmic Transparency, Accountability, and Management." *Intelligence and National Security* 36 (6): 827–48. <https://doi.org/10.1080/02684527.2021.1946952>.

¹¹ Pereira, Antonio L B. 2024. "The IC AI Multiplier: Automating Superiority Seizing Adversarial Artificial Intelligence Use in Intelligence Operations." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4884351.

¹² Ghioni, Riccardo, Mariarosaria Taddeo, and Luciano Floridi. 2024. "Open Source Intelligence and AI: A Systematic Review of the GELSI Literature." *AI and Society* 39 (4). <https://doi.org/10.1007/s00146-023-01628-x>.

real-time interpretation of reality), was analyzed by Saugmann.¹³ He considers techno-vision to be a capability leading to domination in the power competition. Building on the fact that access to such a strategic technology is restricted and surrounded by secrecy, he reconstructs the role of techno-vision by analyzing stories and beliefs left in the public discourse. One of the discussed imprints in the public space is the controversies related to the participation of private companies in military programs integrating AI (such as Google's participation in Project Maven) and developing applications with serious impact such as proposing lethal decisions based on the analysis of data by machine learning models.

To conclude, the discussion about the integration of AI in the intelligence community has developed successfully despite limited access to information. There is a general belief that today's volume of available data cannot be processed without machine learning. However, the research emphasizes the need for human judgment and the human ability of contextualization. The authors agree on the importance of thoughtfully designed and used models that produce unbiased results. It is also evident from the literature that the integration of AI has an impact on relationships between state institutions and the private sector, specifically AI-developing companies.

1.2 Camouflage methods against computer vision

In this literature review section, I present publications related to the use of camouflage and deception methods against computer vision. As will be shown later in this work, computer science literature proposes numerous camouflage solutions that can be deployed against object detection algorithms. Meanwhile, this topic remains underdeveloped in the security studies discussion. Similarly, as for researching intelligence, restrictions regarding access to information may apply. If the development of camouflage means against automatized object detection is a subject of military research, it is justifiable that the know-how is not discussed in public academic literature. The following studies approach the topic from various angles and fields and provide some, but limited, context around camouflage against computer vision.

The possibilities of deception against autonomous weapon systems (AWS) were

¹³ Saugmann, Rune. 2019. "Military Techno-Vision: Technologies between Visual Ambiguity and the Desire for Security Facts." *European Journal of International Security* 4 (3): 300–321. <https://doi.org/10.1017/eis.2019.17>.

analyzed by Sharkey and Sharkey.¹⁴ While AWSs are not analytical tools deployed by intelligence, they are systems autonomously evaluating data collected by their sensors, including visual. Therefore, they can be deceived by similar principles as object detectors.

Monahan¹⁵ and De Vries and Schinkel¹⁶ look into the phenomenon of anti-surveillance tactics, such as face masks and face camouflage. Such face designs are meant to protect one's identity from being recognized by algorithms in street camera footage, images collected by drones, etc. The protection of identity from surveillance systems works on the same principle as hiding military objects in aerial images using camouflage: they both represent adversarial camouflage attacks.

Toroi¹⁷ examines the viability of deception in today's warfare considering the technological advancement in intelligence, surveillance, and reconnaissance. While his focus is particularly on sensor and communication technologies, rather than automatized detection, his work contributes to understanding the complex environment that the future camouflage must withstand. Toroi does not hold the opinion that camouflage is outdated but he emphasizes the need to update military camouflage strategies to keep up with technological development.

Matthews and Matthews¹⁸ analyze the concept of biological and military mimicry on the examples of 21st-century camouflage technologies, such as light-bending invisibility shields, decoy missiles, or invisibility cloaks against thermal cameras. Although their focus is not on the defense against computer vision algorithms, by discussing the possibilities of signature management, they provide context valuable for researching adversarial

¹⁴ Sharkey, Amanda, and Noel Sharkey. 2021. "Sunlight Glinting on Clouds: Deception and Autonomous Weapons Systems." In *Counter-Terrorism, Ethics and Technology. Emerging Challenges at the Frontiers of Counter-Terrorism*, edited by Adam Henschke, Alastair Reed, Scott Robbins, and Seumas Miller, 35–48. Cham: Springer. <https://doi.org/https://doi.org/10.1007/978-3-030-90221-6>.

¹⁵ Monahan, Torin. 2015. "The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance." *Communication and Critical/ Cultural Studies* 12 (2): 159–78. <https://doi.org/10.1080/14791420.2015.1006646>.

¹⁶ Vries, Patricia de, and Willem Schinkel. 2019. "Algorithmic Anxiety: Masks and Camouflage in Artistic Imaginaries of Facial Recognition Algorithms." *Big Data and Society* 6 (1): 1–12. <https://doi.org/10.1177/2053951719851532>.

¹⁷ Toroi, George-Ion. 2024. "MULTI-DOMAIN DECEPTION -CONTEMPORARY OPERATIONAL REQUIREMENT." In *PROCEEDINGS OF THE INTERNATIONAL SCIENTIFIC CONFERENCE STRATEGIES XXI. VOLUME XIX*, 376–88. <https://doi.org/1053477/2971-8813-23-40>.

¹⁸ Matthews, Ron, and Thomas J. Matthews. 2024. "Military Mimicry: The Art of Concealment, Deception, and Imitation." *Defense and Security Analysis*. <https://doi.org/10.1080/14751798.2024.2352271>.

camouflage attacks.

In sum, countermeasures against AI systems using computer vision have not been properly discussed outside of computer science and related disciplines. Therefore, the security implications of these emerging technologies can only be inferred from a thematically broader range of research or technically oriented literature.

2. Introduction of relevant theoretical concepts

2.1 Intelligence

Before taking a closer look at imagery intelligence (IMINT), I will clarify what is understood by intelligence as such, what activities it consists of, describe who the actors conducting intelligence are, what kind of data they use, and introduce possible ways how the discipline of intelligence can be organized.

Broadly, the notion of intelligence can be approached with the meaning of brainpower as a psychological phenomenon, or the meaning of organizational decision support,¹⁹ which will be followed throughout this thesis. With organizational decision support being the mission, intelligence comprises the information of a certain value for the organization, people who handle the process from the collection of information to the production of intelligence reports, as well as the ability to apply knowledge to the acquired data.

Definitions of intelligence often depend on the understanding of who are the actors behind intelligence activities. The phenomenon of intelligence is frequently explained in the context of the protection of national security. Therefore, definitions of governmental intelligence agencies situate their formulations around foreign actors and activities possibly acting against national interests. An oft-cited definition by a former CIA historian Michael Warner links intelligence to the state, presents foreign entities as an opposing force, and adds an element of secrecy: “Intelligence is secret, state activity to understand or influence foreign entities.”²⁰

The element of secrecy is commonly attached to the notion of intelligence. Protection of the intelligence source and maintaining the advantage of surprise can be named as some of the reasons behind it.²¹ At the same time, it can be viewed as a remains of the intelligence culture of the Cold War, when governments tended to be very private about their intelligence

¹⁹ Breakspear, Alan. 2013. “A New Definition of Intelligence.” *Intelligence and National Security* 28 (5): 678–93. <https://doi.org/10.1080/02684527.2012.699285>.

²⁰ Warner, Michael. 2002. “Understanding Our Craft Wanted: A Definition of Intelligence.” *Studies in Intelligence* 46 (3): 15–22, p.21

²¹ Breakspear, Alan. 2013. “A New Definition of Intelligence.” *Intelligence and National Security* 28 (5): 678–93. <https://doi.org/10.1080/02684527.2012.699285>.

structures.²²

However, the conduct of intelligence is not solely a business of governments. Private companies, investigative journalists, NGOs, and open-source enthusiasts are also active users of intelligence. As Breakspear suggests, secrecy should not be a defining characteristic of intelligence, as intelligence from open sources was recognized as a valuable source by the intelligence community.²³ While covert actions are typically linked to the activities of state intelligence agencies, OSINT is the kind of intelligence that can be adopted by a vast range of actors. Therefore, Breakspear defines intelligence as the capability of a group to predict and adapt to changes: “Intelligence is a corporate capability to forecast change in time to do something about it. The capability involves foresight and insight, and is intended to identify impending change, which may be positive, representing opportunity, or negative, representing threat.”²⁴

Similarly, the definition by Gill focuses on foreseeing and preventing a risk: “At the most general level, intelligence can be viewed as a sub-set of surveillance: a ubiquitous social practice, combining processes of knowledge and power and lying at the heart of all risk management. Specifically, intelligence is mainly secret activities – targeting, collection, analysis, dissemination and action – intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities.”²⁵

Considering the focus of this thesis on camouflage in the military context, I will also present the definition of intelligence adopted by NATO: Intelligence is “the product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers.”²⁶ This definition does not specify the institutions involved but highlights its supportive role and exploitation of information on behalf of

²² Gill, Peter. 2010. “Theories of Intelligence.” In *The Oxford Handbook of National Security Intelligence*, 43–58. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780195375886.003.0003>.

²³ Breakspear, Alan. 2013. “A New Definition of Intelligence.” *Intelligence and National Security* 28 (5): 678–93. <https://doi.org/10.1080/02684527.2012.699285>.

²⁴ Breakspear, Alan. 2013. “A New Definition of Intelligence.” *Intelligence and National Security* 28 (5): 678–93. <https://doi.org/10.1080/02684527.2012.699285>, p. 688

²⁵ Gill, Peter. 2010. “Theories of Intelligence.” In *The Oxford Handbook of National Security Intelligence*, 43–58. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780195375886.003.0003>.

²⁶ NATO Standardization Office. 2016. *NATO STANDARD AJP-2 ALLIED JOINT DOCTRINE FOR INTELLIGENCE, COUNTER-INTELLIGENCE AND SECURITY Edition A Version 2*.

security.

I situate my research in the context of intelligence conducted by state intelligence agencies for the needs of state organizations, primarily armed forces. When examining state-organized security organizations, one can expect different motivations and access to resources, such as finances, data, and technology, than in the case of private intelligence agencies, investigative journalists, or OSINT enthusiasts.

Many authors and institutions classify intelligence into disciplines according to data collection. To name a few of the most basic, HUMINT stands for human intelligence, SIGINT refers to signals intelligence, and OSINT to open source intelligence. Imagery intelligence (IMINT) and geospatial intelligence (GEOINT) will be analyzed later in more detail. These “INT” disciplines may become a basis for a structure of state intelligence agencies and define the scope of their responsibilities, such as in the US. This may help to gather specialized expertise in a given data collection method, in practice, however, the boundaries of single-source disciplines may be ignored, as analyzing data from more than one perspective and area of expertise can be beneficial.²⁷

One important intelligence branch stands, however, outside the traditional classification of “INT” disciplines: counterintelligence. It is both an intelligence discipline and a national security mission²⁸ aimed against the intelligence practices of foreign actors. Counterintelligence has a defensive component, which can take the form of hiding objects and events so that data cannot be collected about them, but also an offensive component, which can take the form of deliberately spreading false information so that foreign intelligence receives a distorted picture of reality. To link counterintelligence to the concept of camouflage, camouflage can be understood as a defensive counterintelligence measure against IMINT.

In the military context, based on the intent of use, intelligence can be categorized into strategic, operational, and tactical. Strategic intelligence is used for the creation of policies and military planning on national or international levels. Operational intelligence serves as

²⁷ Clark, Robert M. 2013. “Guide to the Study of Intelligence Perspectives on Intelligence Collection.” *The Intelligencer: Journal of U.S. Intelligence Studies* 20 (2): 47–53. www.afio.com.

²⁸ Cleave, Michelle van. 2013. “What Is Counterintelligence?” *Intelligencer: Journal of US Intelligence Studies* 20 (2): 57–65.

support to “the planning and conduct of campaigns on the operational level,”²⁹ it is concerned with the information on the capabilities and intentions of involved actors. Tactical intelligence supports “the planning and execution of operations at the tactical level”³⁰ and helps the commanders carry out short-term missions and tasks.

2.2 Imagery intelligence (IMINT)

According to the NATO definition, IMINT is “intelligence derived from imagery acquired from sensors that can be ground-based, seaborne or carried by air or space platforms.” In my thesis, I focus on imagery data collected primarily by remote sensing methods, i.e., airborne and spaceborne platforms.

Remote sensing refers to acquiring information about objects on the Earth’s surface, near the surface, and in the atmosphere.³¹ The information is collected from a distance (therefore remote), by sensors (various kinds of cameras creating images), carried by airborne or spaceborne platforms (such as airplanes, UAVs, and satellites). The observation is enabled by the existence of a medium, which is the electromagnetic radiation. Sensors can detect and record the radiation that is emitted, absorbed, and reflected by material objects.³²

In some classifications, IMINT is replaced by GEOINT. GEOINT is a broader discipline that integrates imagery intelligence, as well as geospatial information. Therefore, GEOINT is rather a fusion of intelligence sources, drawing from OSINT, SIGINT, HUMINT and MASINT (measurements and signatures intelligence).³³

Data collected by remote sensing methods require relatively advanced technologies,

²⁹ NATO Standardization Office. 2016. *NATO STANDARD AJP-2 ALLIED JOINT DOCTRINE FOR INTELLIGENCE, COUNTER-INTELLIGENCE AND SECURITY Edition A Version 2*.

³⁰ NATO Standardization Office. 2016. *NATO STANDARD AJP-2 ALLIED JOINT DOCTRINE FOR INTELLIGENCE, COUNTER-INTELLIGENCE AND SECURITY Edition A Version 2*.

³¹ Read, J. M., and M. Torrado. 2009. “Remote Sensing.” In *International Encyclopedia of Human Geography: Volume 1-12*, 335–46. Elsevier. <https://doi.org/10.1016/B978-008044910-4.00508-3>.

³² Tudor, Ciprian Gabriel. 2019. “GEOINT IN MONITORING AND DETECTION OF MILITARY CAMOUFLAGE, CONCEALMENT AND DECEPTION – GEOINT COUNTERDECEPTION.” In *INTERNATIONAL SCIENTIFIC CONFERENCE STRATEGIES XXI. The Complex and Dynamic Nature of the Security Environment - Volume 1*, edited by Florian CÎRCIUMARU and Iulia-Alexandra COJOCARU, 362–70. Bucharest: Carol I National Defence University Publishing House.

³³ Clark, Robert M. 2013. “Guide to the Study of Intelligence Perspectives on Intelligence Collection.” *The Intelligencer: Journal of U.S. Intelligence Studies* 20 (2): 47–53. www.afio.com.

which makes GEOINT a modern discipline.³⁴ Although the idea of collecting imagery from balloons as a form of military operation support occurred already in the American Civil War, specialized surveillance aircraft did not appear earlier than during the Korean War. The development of specialized collection platforms accelerated during the Cold War and expanded into space by placing satellites in orbit in 1957 (USSR), and 1958 respectively (USA).³⁵ In the 1990s, new GEOINT collection opportunities were created by the introduction of digital cameras, UAVs, synthetic aperture radar allowing night vision, and the growth of the market of commercial satellite imagery.³⁶

Imaging sensors play a central role in remote sensing systems. They are devices capable of recording the energy reflected by an object. Sensors can be categorized by their spectral sensitivity, the capability to detect certain wavelengths. Images taken in different spectral bands (i.e., defined ranges of wavelengths, such as radio waves, microwaves, infrared, visible light, ultraviolet, X-ray, and gamma-ray) have different qualities, which can be efficiently combined in multispectral and hyperspectral imaging and provide richer information derived from the imagery data.

Based on the source of recorded energy, sensors can be divided into two groups. Passive sensors do not have their own source of illumination and rely on an external source. In the context of remote sensing the Earth's surface, the illumination is provided by the Sun. Photographic cameras, electro-optical, and thermal infrared sensors are all examples of passive devices. Except for thermal infrared sensors, which can detect energy emitted by an object itself, they are dependent on the presence of sunlight when the images are being created. Active sensors have their own source of energy. The energy is radiated towards the objects to be observed, and the sensors record the energy reflected back. Active sensors typically used for remote sensing are radar (emitting radio waves) and lidar (targeting objects with a laser). For both methods, it applies that the recognition of objects by sensors is ensured

³⁴ Tudor, Ciprian Gabriel. 2019. "GEOINT IN MONITORING AND DETECTION OF MILITARY CAMOUFLAGE, CONCEALMENT AND DECEPTION – GEOINT COUNTERDECEPTION." In *INTERNATIONAL SCIENTIFIC CONFERENCE STRATEGIES XXI. The Complex and Dynamic Nature of the Security Environment - Volume 1*, edited by Florian CÎRCIUMARU and Iulia-Alexandra COJOCARU, 362–70. Bucharest: Carol I National Defence University Publishing House.

³⁵ Muszyński-Sulima, Wawrzyniec. 2023. "Cold War in Space: Reconnaissance Satellites and US-Soviet Security Competition." *European Journal of American Studies* 18 (2). <https://doi.org/10.4000/ejas.20427>.

³⁶ Dupré, Robert E. 2011. "Guide to Imagery Intelligence." *The Intelligence Journal of U.S. Intelligence Studies* 18 (2): 61–64.

by their unique interaction with the illuminated energy.

Using imagery data for collecting intelligence is associated with many advantages. The use of remote platforms allows for capturing large areas and is relatively safe, as it does not require one's physical presence in the area to collect data. Also, imagery data provide accurate and objective information, as the information is fact-based and observed objects can be geographically referenced. Lastly, imagery data can be available almost in real-time and they can be collected periodically, allowing observation of changes over time.³⁷

2.3 Object detection as a tool of IMINT automatization

This thesis deals with the automatization of IMINT realized by the method of object detection. Among other applications, object detection can be used as an interpretation method for remote sensing images.

Object detection is one of the most fundamental tasks in computer vision that seeks to detect visual objects of a certain class in digital images.³⁸ The task of object detection consists of two steps: object localization (finding an object in a given image) and object recognition (assigning the object to a certain class).³⁹

As a tool for intelligence analysts, it can independently process and analyze collected data. Considering the data overwhelm problem suggested earlier, if working correctly, it can conveniently separate data with a certain intelligence value from those invaluable for the given task. For example, if an analyst wants to review the movement of vehicles in a certain area, from the whole set of collected images, the object detector can extract only those containing vehicles, even of a certain predefined class. The human analyst can get a report about the occurrence of vehicles without going through the whole amount of collected data.

The technique of object detection was invented in the 1990s. Zou et al. suggested two evolutionary periods of object detection development: the traditional object detectors period before 2014, and the convolutional neural network-based detectors after the expansion of

³⁷ Wysocki, Krzysztof, and Martyna Niewińska. 2022. "Counteracting Imagery (IMINT), Optoelectronic (EOIMINT) and Radar (SAR) Intelligence." *Scientific Journal of the Military University of Land Forces* 204 (2): 222–44. <https://doi.org/10.5604/01.3001.0015.8975>.

³⁸ Zou, Zhengxia, Keyan Chen, Zhenwei Shi, Yuhong Guo, and Jieping Ye. 2023. "Object Detection in 20 Years: A Survey." *Proceedings of the IEEE* 111 (3): 257–76. <https://doi.org/10.1109/JPROC.2023.3238524>.

³⁹ Zhao, Zhong Qiu, Peng Zheng, Shou Tao Xu, and Xindong Wu. 2019. "Object Detection with Deep Learning: A Review." *IEEE Transactions on Neural Networks and Learning Systems* 30 (11): 3212–32. <https://doi.org/10.1109/TNNLS.2018.2876865>.

deep learning methods around 2014.⁴⁰ Traditional object detectors required humans to manually design image features⁴¹ (i.e. descriptive parameters used to interpret the visual content of an image,⁴² such as information about color, pattern, and shape) that would lead the algorithm to detect an object in the image. Following the boom of deep learning technologies, convolutional neural networks (one type of deep learning network) became part of the new object detectors. Deep learning-based models have deeper architectures than traditional detectors and are capable of learning more complex features.⁴³ Thus, deep learning methods significantly improved the robustness of object detectors, i.e. the ability of a model to perform on the testing sample of data with a similar error as on the training sample of data, in case the data samples are similar.⁴⁴

Learning of a model and any performance of a task presumes the existence of a dataset; in the case of object detectors, a dataset consisting of images. The set of images becomes a reality in which the model learns to localize and recognize instances of objects. Many datasets are publicly available to use; however, they might not contain data suitable for a given task (for example, data covering classes of military targets). Also, publicly available datasets and codes are more vulnerable to adversarial attacks, which is an important consideration in intelligence and military applications. Therefore, creating a new dataset might be required to meet the demands of a given assignment.

A dataset for a machine learning model consists of annotated data. Image annotations provide the model with information on what objects it sees in the image. The established style of annotation for object detection is a bounding box (i.e., a frame placed around the object of interest). The process of assigning classes to the objects in the image is called labeling. It can be done manually by a human annotator or with the assistance of another AI-

⁴⁰ Zou, Zhengxia, Keyan Chen, Zhenwei Shi, Yuhong Guo, and Jieping Ye. 2023. "Object Detection in 20 Years: A Survey." *Proceedings of the IEEE* 111 (3): 257–76. <https://doi.org/10.1109/JPROC.2023.3238524>.

⁴¹ Sun, Yibo, Zhe Sun, and Weitong Chen. 2024. "The Evolution of Object Detection Methods." *Engineering Applications of Artificial Intelligence* 133 (July). <https://doi.org/10.1016/j.engappai.2024.108458>.

⁴² Smith, Michael A., and Tsuhan Chen. 2005. "Image and Video Indexing and Retrieval." *Handbook of Image and Video Processing, Second Edition*, January, 993–XXXI. <https://doi.org/10.1016/B978-012119792-6/50121-2>.

⁴³ Zhao, Zhong Qiu, Peng Zheng, Shou Tao Xu, and Xindong Wu. 2019. "Object Detection with Deep Learning: A Review." *IEEE Transactions on Neural Networks and Learning Systems* 30 (11): 3212–32. <https://doi.org/10.1109/TNNLS.2018.2876865>.

⁴⁴ Xu, Huan, and Shie Mannor. 2012. "Robustness and Generalization." *Machine Learning* 86 (3): 391–423. <https://doi.org/10.1007/s10994-011-5268-1>.

enabled tool, as manual annotations can get time-consuming and expensive. The high costs of data collection can be alternatively solved by using synthetic image data, created by the manipulation of real data or by capturing images in virtual environments.⁴⁵ The costs related to annotations can be alternatively overcome by applying unsupervised learning on unlabeled data.⁴⁶

A subset of data from the dataset is dedicated to the training of a model—a phase in which the model updates its parameters based on the reviewed training data. Another subset of the data is designated for testing what the model learned—more specifically, its ability to generalize its knowledge from the instances in the training data and apply it to the previously unseen testing data. The testing phase allows evaluation of the performance of a given model, with accuracy (the precision of detection) and speed being the most crucial evaluation metrics.

When detecting and recognizing objects, a computer vision system may face challenges dissimilar to what the human eye experiences. An algorithm may become confused by seeing the object under a different angle or light than during the learning process, objects that vary across the class in their visual aspect or size, dense occurrence of objects in the image, etc.⁴⁷ Therefore, the adoption of AI-enabled tools proposes new rules of camouflage design.

2.4 Adversarial attacks on AI models

Deep learning-based models allowed for outstanding performances in computer vision tasks. However, they also proved to be vulnerable to adversarial attacks, i.e. manipulations of input data, which are designed to make the system produce incorrect predictions on the output, and potentially cause harm in real-world applications.⁴⁸

Adversarial attacks can be categorized in many different ways. By the space where

⁴⁵ Man, Keith, and Javaan Chahl. 2022. “A Review of Synthetic Image Data and Its Use in Computer Vision.” *Journal of Imaging* 8 (11). <https://doi.org/10.3390/jimaging8110310>.

⁴⁶ Man, Keith, and Javaan Chahl. 2022. “A Review of Synthetic Image Data and Its Use in Computer Vision.” *Journal of Imaging* 8 (11). <https://doi.org/10.3390/jimaging8110310>.

⁴⁷ Zou, Zhengxia, Keyan Chen, Zhenwei Shi, Yuhong Guo, and Jieping Ye. 2023. “Object Detection in 20 Years: A Survey.” *Proceedings of the IEEE* 111 (3): 257–76. <https://doi.org/10.1109/JPROC.2023.3238524>.

⁴⁸ Huang, Lifeng, Chengying Gao, Yuyin Zhou, Cihang Xie, Alan Yuille, Changqing Zou, and Ning Liu. 2019. “Universal Physical Camouflage Attacks on Object Detectors.” In . <http://arxiv.org/abs/1909.04326>.

the attack is implemented, adversarial attacks can be divided into digital and physical attacks. The digital attacks modify the input data in the digital space, while the physical attacks aim at changing the visual appearance in the physical world as a way to mislead an algorithm.⁴⁹ According to the adversarial goal, the attack can be targeted if the model is supposed to produce a particular class on the output, or untargeted if the goal is solely misleading the model to predict any incorrect class.⁵⁰ According to adversarial knowledge of the model, the attack is called the “white box” if the attacker knows the inner architecture of the model and its parameters, and the “black box” if he does not know.⁵¹ Importantly, adversarial attacks can be designed by humans or generated by machine learning models, which have significantly more powerful computational capacities than humans.

Several attack methods on AI models were described in the literature, varying in the data they seek to exploit and the part of the model they target to achieve it. Data poisoning attack aims at the training data and exploits the incapacity to verify them. Evasion is a method of attack aiming at a system in operation, seeking to foist on the model such data that would mislead it based on what it learned in the training phase. The goal of reverse engineering is to reconstruct a model while having control over inputs and the ability to observe the outputs. Similarly, an inference attack seeks to reconstruct a model by having control over inputs and outputs but its ultimate goal is to extract the training data, which is valuable if the data is sensitive or classified.⁵²

In my research, I focus on adversarial attacks that seek to produce flawed output (object misclassification or failure to notice the object) by intentionally manipulating the data on the model’s input (by adjusting their visual appearance). This corresponds with the

⁴⁹ Huang, Lifeng, Chengying Gao, Yuyin Zhou, Cihang Xie, Alan Yuille, Changqing Zou, and Ning Liu. 2019. “Universal Physical Camouflage Attacks on Object Detectors.” In . <http://arxiv.org/abs/1909.04326>.

⁵⁰ Rathore, Pradeep, Arghya Basak, Sri Harsha Nistala, and Venkataramana Runkana. 2020. “Untargeted, Targeted and Universal Adversarial Attacks and Defenses on Time Series.” In *Proceedings of the International Joint Conference on Neural Networks*. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/IJCNN48605.2020.9207272>.

⁵¹ Rathore, Pradeep, Arghya Basak, Sri Harsha Nistala, and Venkataramana Runkana. 2020. “Untargeted, Targeted and Universal Adversarial Attacks and Defenses on Time Series.” In *Proceedings of the International Joint Conference on Neural Networks*. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/IJCNN48605.2020.9207272>.

⁵² Starck, Nick, David Bierbrauer, and Paul Maxwell. 2022. “Artificial Intelligence, Real Risks: Understanding—and Mitigating—Vulnerabilities in the Military Use of AI.” Modern War Institute. January 18, 2022. <https://mwi.westpoint.edu/artificial-intelligence-real-risks-understanding-and-mitigating-vulnerabilities-in-the-military-use-of-ai/>.

evasion strategy described above. In the real world, these adversarial attacks may take the form of camouflage and deception, i.e. blending into the surroundings or visually misleading the observing entity in what it sees. I also consider those types of attacks, that are created in the digital space and can have a form of invisible added noise to an image. These attacks were defined as adversarial examples by Szegedy et al. who described them as imperceptible non-random perturbations applied to a test image with the capability of optimizing the input in a way that maximizes the prediction error.⁵³ Although this type of adversarial example recedes from the traditional understanding of camouflage, it still represents an intentional visual manipulation.

As a countermeasure to adversarial attacks, various methods of defense were introduced. Some of the methods seek to establish control over the input data, others seek to make the models more robust and be able to deal with malicious data. Input sanitization refers to the preprocessing of input data with the aim of removing data intentionally modified by an attacker. Adversarial training improves the robustness of a dataset by adding adversarial examples to the training data. Federated learning uses more independent sources of training data to decrease the risk of attack and improve privacy. The security of AI systems might be also improved by making a model more transparent and explainable or by training multiple models with different architectures to strengthen the system overall.⁵⁴

2.5 Camouflage in the physical world

In this work, camouflage will be discussed in two forms, physical and digital. As I suggested earlier, both forms of camouflage can become adversarial attacks on deep learning models, such as object detectors.

The concept of camouflage has its roots in the basic natural principle of self-preservation: the predator seeks to locate and capture prey, using the advantage of being unseen and thus creating a moment of surprise, while the prey seeks to avoid being spotted and captured.⁵⁵ Camouflage as a strategy and counterstrategy was adopted and employed by

⁵³ Szegedy, Christian, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. 2013. "Intriguing Properties of Neural Networks." <http://arxiv.org/abs/1312.6199>.

⁵⁴ Rahman, Md Mostafizur, Aiasha Siddika Arshi, Md Mehedi Hasan, Sumayia Farzana Mishu, Hossain Shahriar, and Fan Wu. 2023. "Security Risk and Attacks in AI: A Survey of Security and Privacy." In *Proceedings - International Computer Software and Applications Conference, 2023-June*:1834–39. IEEE Computer Society. <https://doi.org/10.1109/COMPSAC57700.2023.00284>.

⁵⁵ Tudor, Ciprian Gabriel. 2019. "GEOINT IN MONITORING AND DETECTION OF MILITARY CAMOUFLAGE, CONCEALMENT AND DECEPTION – GEOINT COUNTERDECEPTION." In

humans already in ancient times.

Camouflage is sometimes characterized as an art, although the growing role of science in the discipline is being emphasized. The technological demands on camouflage have been going hand in hand with the technological development of warfare. Before World War I, soldiers typically fought in colorful uniforms side by side, and camouflage of forces was not too much of a concern, as aerial observation did not exist. Since WWI, the militaries have sought to take advantage of the environmental features in a new way and used camouflage to mask their guns and vehicles.⁵⁶ As it was outlined in the previous section about imagery intelligence, nowadays, a broad range of sensors is used for data collection, expanding the capability of the human eye beyond seeing just the visible wavelengths. Therefore, high demands are applied to camouflage technologies. Masking patterns are designed using computational methods and the materials of fabrics are manipulated on a molecular level.⁵⁷ The most sophisticated methods of camouflage and electronic countermeasures are combined in the discipline of stealth technology, which is in various forms applied to military equipment, vehicles, and personnel.

Carrying the original sense of the French word *camoufler* (to conceal, to mask), camouflage can be broadly defined as the intention of hiding a certain object or activity. For example, Baumbach defines camouflage as “an art of going (as long as possible) undetected by an observer.”⁵⁸ However, sometimes the understanding also includes the intention of purposely misleading the observer, which becomes relevant if the goal is not only self-preservation but also defeating the rival.

The principle of camouflage can be applied to several contexts and disciplines (for instance, psychology and sociology), in my research, I will deal solely with camouflage in the military domain and stick to the military understanding of the concept of camouflage.

INTERNATIONAL SCIENTIFIC CONFERENCE STRATEGIES XXI. The Complex and Dynamic Nature of the Security Environment - Volume 1, edited by Florian CÎRCIUMARU and Iulia-Alexandra COJOCARU, 362–70. Bucharest: Carol I National Defence University Publishing House.

⁵⁶ Tudor, Ciprian Gabriel. 2019. “CAMOUFLAGE, CONCEALMENT AND DECEPTION IN MILITARY OPERATIONS.” In *SCIENTIFIC CONFERENCE STRATEGIES XXI. The Complex and Dynamic Nature of the Security Environment*. Vol. 1. Bucharest.

⁵⁷ Baumbach, Johannes. 2012. “Colour and Camouflage: Design Issues in Military Clothing.” In *Advances in Military Textiles and Personal Equipment.*, 79–102. Woodhead Publishing.

⁵⁸ Baumbach, Johannes. 2012. “Colour and Camouflage: Design Issues in Military Clothing.” In *Advances in Military Textiles and Personal Equipment.*, 79–102. Woodhead Publishing.

NATO Terminology database defines camouflage as “the use of natural or artificial material on personnel, objects or tactical positions with the aim of confusing, misleading or evading the enemy,”⁵⁹ reflecting the element of rivalry, unlike the first definition introduced above.

In the military domain, the concept of camouflage often occurs together with the terms concealment, deception, and decoy. In the NATO terminology and the US Department of Defence terminology, the abbreviation CCD, usually stands for camouflage, concealment, and deception. However, in some older documents, CCD refers to camouflage, concealment, and decoy.⁶⁰ In the NATO terminology, concealment is defined as „the protection from observation or surveillance,” deception is defined as “deliberate measures to mislead targeted decision-makers into behaving in a manner advantageous to the commander’s intent,” and decoy is defined as “an imitation of a person, object or phenomenon, which is intended to deceive hostile surveillance or detection systems or mislead the adversary.” These military terms (camouflage, concealment, deception, decoy) represent some form of manipulation with the visual perception and therefore a challenge for an observer. In my thesis, I will simply include all these forms of visual manipulation under the term camouflage, taking into account that military terminology further divides and specifies the ways of visual manipulation.

The concept of CCD includes several techniques aimed at misleading the perception of an adversary. They are hiding (creating a shield over the object using some added material), blending (reducing the object’s contrast with the surroundings), disguising (making the object look like a target of lower importance), disrupting (changing the expected patterns of a target), and decoying (planting dummy targets instead of real ones).⁶¹ If applied correctly, deception can cause the enemy force to lose time, resources, combat power, reveal its intentions, strengths and weaknesses, lead the enemy into mislocating personnel and

⁵⁹ NATO. 2024. “NATOTerm. The Official NATO Terminology Database.” NATOTerm. 2024. <https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en>.

⁶⁰ Department of the Army. 1999. *FM 20-3 CAMOUFLAGE, CONCEALMENT, AND DECOYS*. Washington DC. [https://www.bits.de/NRANEU/others/amd-us-archive/FM20-3\(99\).pdf](https://www.bits.de/NRANEU/others/amd-us-archive/FM20-3(99).pdf).

Department of the Army. 2010. *ATTP 3-34.39 CAMOUFLAGE, CONCEALMENT, AND DECOYS*. Washington DC. <https://apps.dtic.mil/sti/pdfs/ADA535471.pdf>.

⁶¹ Tudor, Ciprian Gabriel. 2019. “CAMOUFLAGE, CONCEALMENT AND DECEPTION IN MILITARY OPERATIONS.” In *SCIENTIFIC CONFERENCE STRATEGIES XXI. The Complex and Dynamic Nature of the Security Environment*. Vol. 1. Bucharest.

resources, and win a moment of surprise.⁶²

In my research, I am mainly interested in the camouflage of military equipment and vehicles such as aircraft, ships, armored vehicles, etc. With aerial imagery as the source of intelligence data, individual persons might be unsuitably small for observation. I equally omit the issue of hiding large static objects, such as buildings, as hiding them does not seem to be a trend in the world of constant surveillance by satellites.

2.6 Camouflage in the digital space

As an opposite category to camouflage in the physical world, I present camouflage in digital images, i.e., the effort of manipulating digital images with the goal of misleading a human observer or a computer vision algorithm. This form of camouflage does not take place in the physical world, and it is only implemented into the imagery data.

A successful camouflage attack through image manipulation demands gaining access to the observer, either a human or an automatized system, and the ability to remain undetected by the observer. If the goal of camouflage is to mislead in what is seen, a manipulated image needs to be presented to the observer. This requires the ability to find a vulnerability in a network, enter it undetected, and foist the manipulated data on the observer. If the data are visibly manipulated, camouflage can be recognized as an attack by the automatized system or a supervising human observer.

⁶² Tudor, Ciprian Gabriel. 2019. "CAMOUFLAGE, CONCEALMENT AND DECEPTION IN MILITARY OPERATIONS." In *SCIENTIFIC CONFERENCE STRATEGIES XXI. The Complex and Dynamic Nature of the Security Environment*. Vol. 1. Bucharest.

3. Methodology

The aim of this thesis is to identify the research trends in the field of computer science and related disciplines and transfer the knowledge to the field of security studies. In the following chapter, I survey the research of a prominent computer vision task, object detection, to explore the opportunities AI-enabled tools offer to the intelligence community on one end and to covert operations on the other.

For the review of secondary literature, I gathered over fifty studies by using search engines (primarily Google Scholar). I studied each document individually to evaluate the relevance of the content to the topic of adversarial attacks on object detectors. After analyzing the documents, I synthesized the knowledge and identified three major clusters of studies. Documents in each group followed similar procedures to achieve concealment or misclassification of a target object in the image.

The vast majority of the included studies proposed original solutions for adversarial attacks against object detectors. The selection of documents included both published papers and preprints to reflect the dynamic development of this young research direction. The studies were collected in journals and conference proceedings dedicated to machine learning, computer vision, image processing, intelligent computing, neural networks, neurocomputing, remote sensing, and others. No criteria regarding the quality of the publication (such as journal rating) or citation frequency were applied.

Considering my first research question (How can object detection models be attacked by camouflage?), I worked with the following keywords in several combinations:

The keywords “adversarial attack”, were selected since it is an established technical term for an attack on an AI model, consisting of a (visual) manipulation of (image) data at the input of a model with the aim of influencing the model’s output. I alternatively used the keywords “adversarial example attack,” as this is also an established term. Although originally referring only to pixel-level perturbations of images (as it was introduced by Szegedy et al.⁶³), today the term adversarial example attack tends to be applied universally to various types of malicious data manipulations. I also applied the keywords “adversarial camouflage attack,” which is a term used for adversarial attacks designed specifically against computer vision models, indicating the goal of concealing an object in the data.

⁶³ Szegedy, Christian, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. 2013. “Intriguing Properties of Neural Networks.” <http://arxiv.org/abs/1312.6199>.

Next, I used the keywords “object detection” and “object detector” to specify the type of model and computer vision task the adversarial attacks are designed to target.

Then, I applied the keywords “camouflage” and “military camouflage”, to indicate the purpose of hiding behind the adversarial attack. I added the adjective “military” to indicate the environment in which the concept originates and because I was interested in the proposals suitable for the military context.

Finally, I used the keywords “intelligence,” “IMINT,” and “military intelligence” to capture the context, in which object detectors can be deployed. Object detection is frequently used in the context of autonomous driving; therefore, this way I sought to gather surveillance-related studies.

I decided to include adversarial camouflage attacks conducted both in the physical world and the digital space. Although the scenarios of their use are distinct (one requiring access to the objects in the physical world, the other requiring access to the network and the ability to feed the model with manipulated images), I considered all adversarial camouflage attacks meeting the condition that the visual modification of the image’s content causes either a complete failure in detecting the target object or its misclassification.

Despite my efforts to review various directions of research and include the most relevant studies, the topic of adversarial attacks is nowadays frequently researched, and I do not consider the collected studies to be an exhaustive review. I primarily focused on including those articles that suggested some form of security or military application and worked with remotely sensed imagery.

It could be questioned why I selected documents focusing on relatively simple camouflage methods based on altering colors and patterns at a time when far more advanced camouflage technologies were introduced. The authors of the discussed proposals do not consider materials to which camouflage patterns would be applied or the collection of images by sensors in multiple spectral bands. Yet, I argue that even camouflage measures this simple should be discussed, as the real examples presented in section 4.2 suggest that sometimes there is a need for a simple improvised solution. Also, technologies with advanced signature management are not available to everyone, and simple but ingenious visual camouflage might be the best capability at one’s disposal.

The choice of a research area that I could explore was, of course, affected by the fact that research and development of technologies with military applications is commonly classified, and studies published in academic journals represent only a specific portion of the

current knowledge. This, however, does not preclude the possibility of critically discussing the security implications and military uses of technologies that have already been introduced in a civilian context.

To address one more possible bias of the selection of documents, I highlight the fact that a significant part of the documents selected by the mentioned criteria was published by Chinese authors. This can be explained by the strategic goal to become the world leader in AI technologies set by the Chinese government, resulting in high interest in AI research. Alternatively, the number of publications can be explained by the publishing culture and policies in China.

Overview of the studies referenced in the following chapter

Year	Author(s)	Title	Attack method
2020	Duan et al.	Adversarial Camouflage: Hiding Physical-World Attacks with Natural Styles	Camouflage pattern
2021	Duan et al.	Learning Coated Adversarial Camouflages for Object Detectors	Camouflage pattern
2020	Huang et al.	Universal Physical Camouflage Attacks on Object Detectors	Camouflage pattern
2023	Li et al.	Fooling Object Detectors in the Physical World with Natural Adversarial Camouflage	Camouflage pattern
2023	Li, Peng, and Lian	Multi-texture Fusion Attack: A Robust Adversarial Camouflage in Physical World	Camouflage pattern
2023	Sun et al.	Differential Evolution Based Dual Adversarial Camouflage: Fooling Human Eyes and Object Detectors	Camouflage pattern
2022	Suryanto et al.	DTA: Physical Camouflage Attacks using Differentiable Transformation Network	Camouflage pattern
2019	Zhang et al.	CAMOU: Learning a Vehicle Camouflage for Physical Adversarial Attack on Object Detectors in the Wild	Camouflage pattern
2020	Hu et al.	CCA: Exploring the Possibility of Contextual Camouflage Attack on Object Detection	Camouflage pattern
2024	Zhou et al.	RAUCA: A Novel Physical Adversarial Attack on Vehicle Detectors via Robust and Accurate Camouflage Generation	Camouflage pattern
2020	Adhikari et al.	Adversarial Patch Camouflage Against Aerial Detection	Adversarial patch
2023	Deng et al.	Rust-Style Patch: A Physical and Naturalistic Camouflage Attacks on Object Detector for Remote Sensing Images	Adversarial patch
2022	Du et al.	Physical Adversarial Attacks on an Aerial Imagery Object Detector	Adversarial patch
2024	Guesmi et al.	AdvART: Adversarial Art for Camouflaged Object	Adversarial patch

Detection Attacks			
2021	Kim et al.	Camouflaged Adversarial Attack on Object Detector	Adversarial patch
2023	Lapid and Sipper	Patch of Invisibility: Naturalistic Physical Black-Box Adversarial Attacks on Object Detectors	Adversarial patch
2023	Tang et al.	Adversarial Patch Attacks against Aerial Imagery Object Detectors	Adversarial patch
2022	Van Etten	The Weaknesses of Adversarial Camouflage in Overhead Imagery	Adversarial patch
2021	Wang et al.	Dual Attention Suppression Attack: Generate Adversarial Camouflage in Physical World	Adversarial patch
2020	Wu et al.	Making an Invisibility Cloak: Real World Adversarial Attacks on Object Detectors	Adversarial patch
2022	Zhang and Ma	Misleading Attention and Classification: An Adversarial Attack to Fool Object Detection Models in the Real World	Adversarial patch
2019	Chen et al.	Adversarial Example in Remote Sensing Image Recognition	Imperceptible perturbations
2021	Deng et al.	Adversarial Examples with Transferred Camouflage Style for Object Detection	Imperceptible perturbations
2020	Li, Zhang, and Huang	Universal Adversarial Perturbations Against Object Detection	Imperceptible perturbations
2021	Ren, Huang, and Yan	Adversarial Examples: Attacks and Defenses in the Physical World	Imperceptible perturbations
2013	Szegedy et al.	Intriguing Properties of Neural Networks	Imperceptible perturbations
2022	Tian et al.	Adversarial Attacks and Defenses for Deep-Learning-Based Unmanned Aerial Vehicles	Imperceptible perturbations
2023	Zhou et al.	CamoNet: A Target Camouflage Network for Remote Sensing Images Based on Adversarial Attack	Imperceptible perturbations

4. Empirical Findings

4.1 Review of secondary literature

In this chapter, I define three types of attacks on object detectors that take the form of visual misleading of this computer vision task. The first two types of attacks, patterns and patches, can be applied in the physical world, unlike the third one, imperceptible image perturbations, which assumes conducting the adversarial attack in the digital space.

The suggested categories of methods differ in the extent of the image area they attack. Adversarial patterns are typically applied as a coat over the object, while adversarial patches tend to be applied only over a part of the object. Imperceptible perturbations can attack pixels in the target object and in the image's background.

Designing adversarial patterns, patches, and imperceptible perturbations is not a task that a human could effectively carry out. The adversarial attacks discussed in this chapter were produced by AI models called generative adversarial networks.

4.1.1 Adversarial camouflage patterns

The first group of studies proposes camouflage patterns designed to mislead object detector models. The ambition and effect of the patterns may vary from complete concealment from the eyes of the object detector, through partial hiding, to misclassification as a different object. These patterns are meant to be applied to the surfaces of objects in the real world; therefore, they fall into the category of physical attacks.

Just as traditional military camouflage patterns, the patterns proposed against computer vision are designed to make objects disappear. Unlike the traditional military patterns, though, patterns designed against computer vision models do not tend to blend in by adopting colors natural to the surroundings but they are often unnaturally colorful. Some studies⁶⁴ proposed simple mosaic-style patterns, some opted for complicated patterns with

⁶⁴ Zhang, Yang, Hassan Foroosh, Philip David, and Boqing Gong. 2019. "CAMOU: LEARNING A VEHICLE CAMOUFLAGE FOR PHYSICAL ADVERSARIAL ATTACK ON OBJECT DETECTORS IN THE WILD." In *ICLR 2019*.

Hu, Shengnan, Yang Zhang, Sumit Laha, Ankit Sharma, and Hassan Foroosh. 2020. "CCA: Exploring the Possibility of Contextual Camouflage Attack on Object Detection." In *Proceedings - International Conference on Pattern Recognition*, 7647–54. Institute of Electrical and Electronics Engineers Inc.

Suryanto, Naufal, Yongsu Kim, Hyeon Kang, Harashta Tatimma Larasati, Youngyeo Yun, Thi-Thu-Huong Le, Hunmin Yang, Se-Yoon Oh, and Howon Kim. 2022. "DTA: Physical Camouflage Attacks Using Differentiable Transformation Network." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 15305–14.

ostensibly semantically meaningful scenes,⁶⁵ and others used edited photos (typically of animals) as a base for their camouflage patterns.⁶⁶

Importantly, most of the studies do not deal with the human eye's visual perception of their camouflage patterns. Therefore, their methods are designed to mislead an object detector but would be likely noticed if a human analyst reviewed the data.

Among the studies reviewed, most of them were situated in the context of autonomous driving, which attracts fairly more attention in the scholarly literature than intelligence applications. Adversarial patterns (similar to adversarial patches) are often designed to be applied to vehicles⁶⁷ or traffic signs,⁶⁸ testing the opportunities and limits of object detectors in traffic, rather than in the context of intelligence and surveillance.

The high costs associated with conducting experiments in the real world (such as printing adversarial patterns on vehicles) have been solved by conducting experiments in

⁶⁵ Duan, Yexin, Jialin Chen, Xingyu Zhou, Junhua Zou, Zhengyun He, Jin Zhang, Wu Zhang, and Zhisong Pan. 2021. "Learning Coated Adversarial Camouflages for Object Detectors." ArXiv Preprint ArXiv:2109.00124.

⁶⁶ Huang, Lifeng, Chengying Gao, Yuyin Zhou, Cihang Xie, Alan Yuille, Changqing Zou, and Ning Liu. 2020. "Universal Physical Camouflage Attacks on Object Detectors." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 720–729.

⁶⁷ Huang et al., 2020; Zhang et al., 2019; Hu et al., 2020; Duan et al., 2021; Suryanto et al., 2022;

Li, Yisheng, Xuekang Peng, and Zhichao Lian. 2024. "Multi-Texture Fusion Attack: A Robust Adversarial Camouflage in Physical World." In *International Conference on Intelligent Computing. Lecture Notes in Computer Science, Vol 14870.*, edited by DS Huang, W Chen, and J Guo, 14870 LNCS:186–98. Springer, Singapore.

Zhou, Jiawei, Linye Lyu, Daojing He, and Yu Li. 2024. "RAUCA: A Novel Physical Adversarial Attack on Vehicle Detectors via Robust and Accurate Camouflage Generation." In *Proceedings of the 41st International Conference on Machine Learning*. <http://arxiv.org/abs/2402.15853>.

⁶⁸ Duan, Ranjie, Xingjun Ma, Yisen Wang, James Bailey, A K Qin, and Yun Yang. 2020. "Adversarial Camouflage: Hiding Physical-World Attacks with Natural Styles." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition.*, 1000–1008.

Li, Dandan, Yufeng Li, Guiqi Zhang, Ke Sun, and Jiangtao Li. 2023. "Fooling Object Detectors in the Physical World with Natural Adversarial Camouflage." In *Proceedings - 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom/BigDataSE/CSE/EUC/ISCI 2023*, 141–48. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/TrustCom60117.2023.00040>.

virtual environments,⁶⁹ alternatively by models of vehicles placed in the real world.⁷⁰

Due to the popularity of the traffic context of experiments, the adversarial patterns tend to be tested on images taken from a relatively short distance, with the camera being placed on a ground-based platform or relatively low above the ground, which could substitute for testing the patterns in the images taken by a UAV. These patterns might not be effective when images are taken from a longer distance; due to camera resolution and atmospheric conditions, the pattern might seem blurry and colors blended.

Aerial images were also used in experiments, in which the adversarial patterns were designed as a background surface and applied under aircraft standing on the ground.⁷¹ These experiments offer an interesting solution against aerial surveillance and they represent an alternative to the challenge of applying a camouflage pattern on an object of a complicated shape.

As mentioned, the experiments often take place in virtual environments, and although some authors were able to simulate various weather and lighting conditions in the environments they used,⁷² the patterns might not be effective under real-world atmospheric conditions.

Universality is another challenge to the effectiveness of adversarial patterns. Some authors sought to develop patterns that would be effective not only when applied to one specific object.⁷³

Further, in real-world scenarios, the adversarial pattern would prove its value if it

⁶⁹ Huang et al., 2020; Zhang et al., 2019; Hu et al., 2020; Duan et al., 2021; Suryanto et al., 2022; Li, Peng and Lian, 2024; Zhou et al., 2024;

Sun, Jialiang, Wen Yao, Tingsong Jiang, Donghua Wang, and Xiaoqian Chen. 2023. "Differential Evolution Based Dual Adversarial Camouflage: Fooling Human Eyes and Object Detectors." *Neural Networks* 163 (June): 256–71.

⁷⁰ Duan et al., 2022; Suryanto et al., 2022; Li, Peng and Lian, 2024

⁷¹ Zhang, Yu, Jianqi Chen, Zhenbang Peng, Yi Dang, Zhenwei Shi, and Zhengxia Zou. 2024. "Physical Adversarial Attacks Against Aerial Object Detection With Feature-Aligned Expandable Textures." *IEEE Transactions on Geoscience and Remote Sensing* 62.

Wang, Xiaofei, Shaohui Mei, Jiawei Lian, and Yingjie Lu. 2024. "Fooling Aerial Detectors by Background Attack via Dual-Adversarial-Induced Error Identification." *IEEE Transactions on Geoscience and Remote Sensing* 62.

⁷² Li, Peng and Lian, 2024; Zhou et al., 2024

⁷³ Huang et al., 2020; Zhang et al., 2019; Sun et al., 2023; Duan et al., 2020; Suryanto et al., 2022;

successfully attacks any unknown object detector, that is, it successfully conducts a “black-box” attack on a model with unknown internal architecture. There are several publicly accessible object detectors and datasets that are frequently used for research experiments. However, it would be naïve to expect such models would be employed in real-world security contexts because using publicly available codes and datasets would increase the system’s vulnerability to adversarial attacks. Some of the proposed patterns were tailored to attack a specific detector,⁷⁴ others tested their performance on multiple models.⁷⁵

⁷⁴ Duan et al., 2020

⁷⁵ Huang et al., 2020; Zhang et al.,2019; Sun et al., 2023; Hu et al., 2020; Duan et al.,2021; Suryanto et al., 2022; Li et al., 2023; Li, Peng and Lian, 2024; Zhou et al., 2024

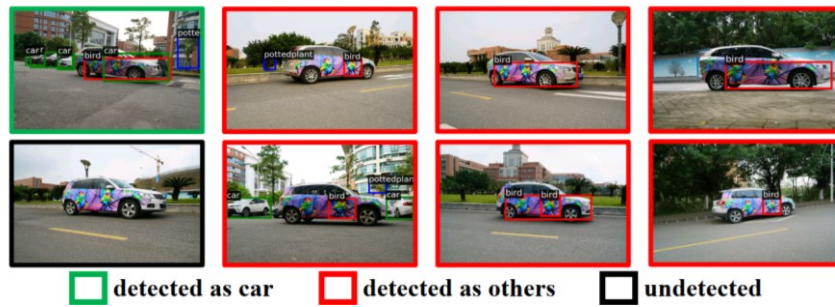


Figure 1. An adversarial camouflage pattern applied on a vehicle proposed by Huang et al. in “Universal Physical Camouflage Attacks on Object Detectors.” *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. © 2020 IEEE

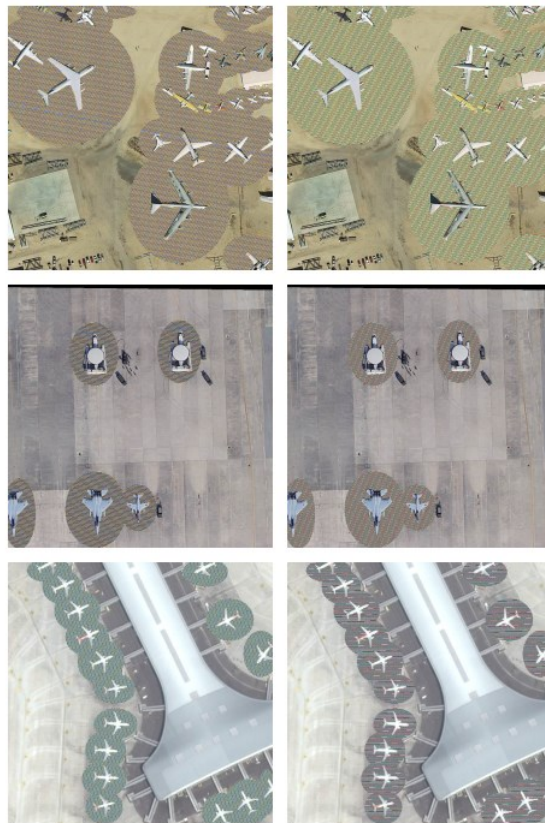


Figure 2. An adversarial camouflage pattern applied under aircraft proposed by Zhang et al. in “Physical Adversarial Attacks Against Aerial Object Detection With Feature-Aligned Expandable Textures.” *IEEE Transactions on Geoscience and Remote Sensing*. © 2024 IEEE

4.1.2 Adversarial patches

Adversarial patches are a popular adversarial method that shares several features and challenges with adversarial camouflage patterns. The principal difference between adversarial patterns and patches is that adversarial patches attack a smaller part of the target

object, which poses new challenges and opportunities for real-world applications.

The majority of proposed patches tend to be of colorful design and thus well-perceptible to the human eye, although patches imitating a rust stain⁷⁶ or traditional military camouflage patterns⁷⁷ were introduced as well.

Also, patches with pictures of animals were proposed,⁷⁸ seeking to create semantically meaningful content that does not attract human attention. Such a patch printed on clothes might mislead a street surveillance camera, as a t-shirt with a picture of a dog is inconspicuous, however, patches with animals probably could not succeed in military contexts. Other applications in the reviewed experiments included patches on car roofs⁷⁹ and patches placed over aircraft at parking stands.⁸⁰

As in the case of adversarial patterns, due to the high cost of experiments in the

⁷⁶ Deng, Binyue, Denghui Zhang, Fashan Dong, Junjian Zhang, Muhammad Shafiq, and Zhaoquan Gu. 2023. “Rust-Style Patch: A Physical and Naturalistic Camouflage Attacks on Object Detector for Remote Sensing Images.” *Remote Sensing* 15 (4).

⁷⁷ Kim, Jeonghun, Kyungmin Lee, Hyeongkeun Lee, Hunmin Yang, and Se Yoon Oh. 2021. “Camouflaged Adversarial Attack on Object Detector.” In *International Conference on Control, Automation and Systems*, 2021-October:613–17. IEEE Computer Society.

⁷⁸ Guesmi, Amira, Ioan Marius Bilasco, Muhammad Shafique, and Ihsen Alouani. 2024. “AdvART: Adversarial Art for Camouflaged Object Detection Attacks.” In *2024 IEEE International Conference on Image Processing (ICIP)*, 666–72. IEEE.

Wang, Jiakai, Aishan Liu, Zixin Yin, Shunchang Liu, Shiyu Tang, and Xianglong Liu. 2021. “Dual Attention Suppression Attack: Generate Adversarial Camouflage in Physical World.” In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*.

Lapid, Raz, and Moshe Sipper. 2023. “Patch of Invisibility: Naturalistic Physical Black-Box Adversarial Attacks on Object Detectors.”

Zhang, Haotian, and Xu Ma. 2022. “Misleading Attention and Classification: An Adversarial Attack to Fool Object Detection Models in the Real World.” *Computers and Security* 122 (November).

⁷⁹ Wang et al., 2021;

Etten, Adam van. 2022. “The Weaknesses of Adversarial Camouflage in Overhead Imagery.” In *Proceedings - Applied Imagery Pattern Recognition Workshop*. Vol. 2022-October. Institute of Electrical and Electronics Engineers Inc.

Du, Andrew, Bo Chen, Tat-Jun Chin, Yee Wei Law, Michele Sasdelli, Ramesh Rajasegaran, and Dillon Campbell. 2022. “Physical Adversarial Attacks on an Aerial Imagery Object Detector.” In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, 1796–1806.

⁸⁰ Tang, Guijian, Tingsong Jiang, Weien Zhou, Chao Li, Wen Yao, and Yong Zhao. 2023. “Adversarial Patch Attacks against Aerial Imagery Object Detectors.” *Neurocomputing* 537 (June): 128–40.

Adhikari, Ajaya, Richard den Hollander, Ioannis Tolios, Michael van Bekkum, Anneloes Bal, Stijn Hendriks, Maarten Kruithof, et al. 2020. “Adversarial Patch Camouflage against Aerial Detection,” August.

physical world, authors often conduct experiments in virtual environments, which raises questions about the real-life applicability and effectiveness of this form of attack. While printing and applying an adversarial patch on a car roof is quite simple, applying a patch on an aircraft seems more complicated considering the object’s shape. To my knowledge, an experiment with aircraft in the real world has not been publicly reported.

One of the challenges of adversarial patches is their size. Larger sizes might be more effective because they cover a larger part of the object and have more space to demonstrate a misleading pattern. On the other hand, smaller patches are less noticeable to the human eye but might become less effective if the distance from the sensor increases.

As for the adversarial patterns, the effectiveness of adversarial patches is inherently impacted by atmospheric conditions. Also, patches may be less effective in images of lower resolution. Both circumstances make the patch design less clear and thus decrease the chance of the patch misleading an object detector.

Lastly, as in the case of other attack methods, it is relevant to test adversarial patches applied to various types of objects and test the patches against various object detectors.⁸¹



Figure 3. Adversarial patches digitally added to the image on the right caused invisibility or misclassification of vehicles. Proposed by Van Etten in “The Weaknesses of Adversarial Camouflage in Overhead Imagery.” *Proceedings - Applied Imagery Pattern Recognition Workshop*. © 2022, IEEE

⁸¹ A test against more than a one object detector was conducted by: Tang et al., 2023; Wang et al., 2021; Guesmi et al., 2024; We et al., 202; Lapid and Sipper, 2023; Zhang and Ma, 2022



Figure 4. Legacy adversarial patches applied on the aircraft stand by Van Etten in “The Weaknesses of Adversarial Camouflage in Overhead Imagery.” *Proceedings - Applied Imagery Pattern Recognition Workshop*. © 2022, IEEE

4.1.3 Imperceptible Image Perturbations

While the previous attack methods represent a way to mislead an AI system by actions carried out in the physical world, adversarial imperceptible perturbation is a type of attack requiring the capability of feeding the system with deliberately modified images. Imperceptible perturbations have a form of manipulation on the image’s pixel level. It means that the numerical value of a pixel’s brightness or color is changed. The image manipulations I consider in my analysis seek to make the objects in the images disappear or appear as something else. By the image modification, the objects may become camouflaged to the vision of an object detector. However, in the context of millions of pixels an image might consist of, this modification can go unnoticed by the human eye at the same time.

Tian et al. proposed a scenario suggesting one of the ways manipulated images can enter an AI system unnoticed. In the considered scenario, the attacker exploits vulnerabilities of the Wi-Fi network transmitting the imagery data from a UAV camera to a processing controller. As a result, in this scenario, the manipulated images caused a threat to the navigation and control of the UAV.⁸² Conducting such a cyber-attack is an alternative to a physical camouflage attack and in a real-world scenario, the choice of a method will depend on the offensive capabilities of the attacker and the defensive capabilities of the actor running the AI system.

The imperceptible perturbations as an attack on an image classifier were introduced by Szegedy et al. who proposed that non-random perturbations found by optimizing the input

⁸² Tian, Jiwei, Buhong Wang, Rongxiao Guo, Zhen Wang, Kunrui Cao, and Xiaodong Wang. 2022. “Adversarial Attacks and Defenses for Deep-Learning-Based Unmanned Aerial Vehicles.” *IEEE Internet of Things Journal* 9 (22): 22399–409.

data can maximize the prediction error on the output.⁸³ They called these perturbations adversarial examples. Later, the term adversarial example became understood more broadly and used for all kinds of attacks in the digital as well as physical world, not only in the image domain.⁸⁴

Optimizing the input data in the context of adversarial examples means finding those pixels that would be the most effective in bringing the desired outcome on the output, as an opposite to changing the value of random pixels. However, the number of pixels might need to be limited, as modification of a high number of pixels could be detectable. If incorrectly designed, manipulations of the input data might not only be detected by a human but also by an anomaly detector.⁸⁵ A remarkable attempt to improve the invisibility of perturbation to the human eye was made by Deng et al. who based their adversarial example on the Canadian Disruptive Pattern.⁸⁶

Experiments with imperceptible adversarial perturbations were conducted in a broad variety of contexts, including remotely sensed images.⁸⁷ The adversarial perturbations might be tailored specifically to each image⁸⁸ (white box setting) or be universal, i.e. effective when applied to any image⁸⁹ (black box setting). Also, proposed perturbations might or might not be transferable across different object detectors. As the manipulations of images take place only in the digital space, there is no risk of unfavorable atmospheric conditions and lighting that would decrease the clarity of camouflage, as in the cases of adversarial patterns and

⁸³ Szegedy, Christian, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. 2013. "Intriguing Properties of Neural Networks."

⁸⁴ Ren, Huali, Teng Huang, and Hongyang Yan. 2021. "Adversarial Examples: Attacks and Defenses in the Physical World." *International Journal of Machine Learning and Cybernetics* 12 (11): 3325–36.

⁸⁵ Tian et al., 2022

⁸⁶ Deng, Xiaotong, Zheng Fang, Yunfei Zheng, Yang Wang, Junming Huang, Xiaobing Wang, and Tiejong Cao. 2021. "Adversarial Examples with Transferred Camouflage Style for Object Detection." In *Journal of Physics: Conference Series*. Vol. 1738. IOP Publishing Ltd.

⁸⁷ Tian et al., 2022;

Zhou, Yue, Wanghan Jiang, Xue Jiang, Lin Chen, and Xingzhao Liu. 2023. "CamoNet: A Target Camouflage Network for Remote Sensing Images Based on Adversarial Attack." *Remote Sensing* 15 (21).

Chen, Li, Guowei Zhu, Qi Li, and Haifeng Li. 2019. "Adversarial Example in Remote Sensing Image Recognition." ArXiv Preprint ArXiv:1910.13222.

⁸⁸ Tian et al., 2022

⁸⁹ Li, Zhang, and Huang, 2020

patches applied in the physical world.

4.2 Real-world examples of adversarial techniques

This section will provide some examples of real-world camouflage and deception applications against AI-enabled tools. The presented examples occurred during the War in Ukraine and suggest a new chapter in the disciplines of CCD, intelligence, and sensing. As will be shown in the examples, colorful adversarial patterns and patches have not yet found their way to military bases and battlefields. However, the presented deception techniques exploit the vulnerabilities of AI models and their capability of object detection.

4.2.1 A Russian warship

The Russian warship⁹⁰ mentioned in the introduction sought to mislead algorithms by pretending to have a different length and shape. The dark color applied to the bow and stern was supposed to visually blend into the water. Changing an object's shape surely is a way to confuse an object detector, however, when applied in the real world it may be effective only under certain conditions. The light is likely to cause the water and the painting to get distinct shades, moreover, it will make the ship cast a shadow. The perceptibility of both will depend on the resolution of the images. Yet, it is not likely that intelligence would rely on images taken in the visual spectrum only, considering that the images were taken in Crimea during the war. Indeed, radar images were released on the internet as well. After reaching the object, radar waves get reflected back toward the sensor, and no color scheme is able to prevent that. Especially metal materials are well-pronounced in radar images. In theory, it would be possible to apply a paint or material mitigating the radar reflection on the ship's surface, nonetheless, the result might not still be sufficient to prevent a correct detection.

4.2.2 Russian aircraft covered in tires

In the summer of 2023, it was reported that Russia covered its bombers in tires with the intention of protecting it from image-matching capabilities.⁹¹ This time, rather than an automatized tool for intelligence analysis, the inventive camouflage aimed at confusing

⁹⁰ Sutton, H I. 2023. "New Technology Sees Through Russian Attempt to Hide Ships from Ukraine." Naval News. July 12, 2023. <https://www.navalnews.com/naval-news/2023/07/new-technology-sees-through-russian-attempt-to-hide-ships-from-ukraine/>.

⁹¹ Trevithick, Joseph. 2024. "Russia Covering Aircraft With Tires Is About Confusing Image-Matching Missile Seekers U.S. Military Confirms." The Warzone. September 13, 2024. <https://www.twz.com/air/russia-covering-its-aircraft-in-tires-is-about-befuddling-image-matching-seekers-u-s-military-confirms>.

kamikaze drones using computer vision.⁹² As the aircraft were staying at an air base of strategic bombers, it can be assumed that their activity was already under close observation. Thus, causing the drones to miss a target is the more probable goal of the tires. A pitfall of camouflage attacks like this one is that once they are used, images of the scene can be taken, labeled, included in training data, and models can become resistant the next time. The attack with tires is relatively simple but it is likely applicable only as a one-time surprise, rather than a long-term strategy.



Figure 5. An aircraft covered in tires at the military air base in Engels, Russia. The deception attempt was reported by Joseph Trevithick. Snímky © 2024 Airbus, Maxar Technologies, Mapová data © 2024

4.2.3 Painted decoys

At the mentioned Russian air base, another method was applied to thwart drone strikes. The bombers were painted on the aircraft stand.⁹³ Although it was a realistic painting, next to the real bombers the painting seemed apparently flat because it lacked shadow. For this reason, it would be easily detected as fake by an advanced model or a human observer, unless were the images taken under favorable lighting conditions. Also, the painting would be completely helpless against a radar.

⁹² Trevithick, Joseph. 2024. "Russia Covering Aircraft With Tires Is About Confusing Image-Matching Missile Seekers U.S. Military Confirms."

⁹³ Ibid.

Similarly, a painting of a submarine was reported at a Russian port in the Black Sea.⁹⁴ This time, the painting was complemented with 3D components. However, regarding detection, similar to equal results as for the painted decoy bombers may be expected.



Figure 6. A painted decoy aircraft at the military air base in Engels, Russia. The deception attempt was reported by Joseph Trevithick. Snímky © 2024 Airbus, Maxar Technologies, Mapová data © 2024

⁹⁴ Trevithick, Joseph. 2024. "Submarine Decoy Appears On Russian Naval Base Pier." The Warzone. March 20, 2024. <https://www.twz.com/news-features/submarine-decoy-appears-on-russian-naval-base-pier>.



Figure 7. A painted decoy submarine at the military naval base in Novorosijsk, Russia. The deception attempt was reported by Joseph Trevithick. Snímky © 2024 Airbus, Maxar Technologies, Mapová data © 2024

4.2.4 Inflatable decoys

One should not omit inflatable dummy decoys when discussing deception in the context of the War in Ukraine. When unrecognized from the real, dummy vehicles, weapons, and other kinds of military assets can create an illusion of greater capabilities and make the enemy waste munition on false targets. Although the inflatable rubber tanks date back to World War II, their use has not been outdated. Today's decoys are much more sophisticated and able to confuse sensors of several spectral bands at once. Besides having a perfect visual appearance, inflatables can imitate real capabilities on radar and thermal images.⁹⁵ How effective these decoys are depends also on the way they are deployed. However, as a capability resistant against sensors of more electromagnetic spectrums, they represent more mature attacks on algorithms than paintings and tires.

⁹⁵ Such capabilities were listed for the inflatable dummies, for instance, by the Czech company Inflatech Decoy.

5. Discussion

Based on my analysis of the secondary literature, I sought to answer the question of how can be computer vision, represented by the task of object detection, misled by visual camouflage. I defined three techniques that can cause the failure of an object detection algorithm. Covering an object in a camouflage pattern, placing a patch on an object, and deliberately manipulating an image's pixels are the three types of adversarial attacks that scholarly literature discusses the most. Starting my thesis by reviewing the discussion in social sciences, I then moved to the proposals of researchers based in computer science to grasp the current technological advancements and analyze the possible implications for the intelligence community and militaries.

There is a wide consensus in the literature about the need for AI-enabled analytical tools among the intelligence community, as this seems to be the only way to process large amounts of available data. The deployment of automatized analysis together with advanced remote sensors allowed for constant monitoring of the whole Earth's surface and made hiding anything significantly more difficult. Yet adversarial camouflage techniques were proposed, and in conducted experiments, they proved capable of hiding various objects from computer vision algorithms.

Nonetheless, so far, adversarial camouflage against algorithms has not become an established method of counterintelligence. Although the computer science studies I reviewed occasionally briefly outlined the context in which the proposed camouflage methods would be applicable, they typically focus on autonomous driving, leaving other potential areas of use largely unexplored. At the same time, the presented empirical examples showed that the Russian military feels the need to hide its assets from automatized detection. Given the consensus about the increasing reliance on the automatized production of intelligence, one would expect counterintelligence applications would be considered in the literature.

The proposed camouflage attacks on object detection models usually aim at misleading an object detection model only and do not consider hiding the object from the eyes of a human observer. Adversarial camouflage patterns and patches tend to be designed strikingly colorful and therefore unsuitable in scenarios in which a human participates in the analysis of imagery data. The reviewed literature on the integration of AI-enabled tools in intelligence analysis gives the impression that there is a strong awareness of the risks related to incorrectly designed and inappropriately used models. With regard to the vulnerability of object detection models to adversarial attacks, it can be expected that human analysts will

remain in control over the conduct of intelligence tasks, and AI-enabled tools will continue playing an important but supportive role in enhancing human cognitive capacities. Considering that, camouflage and deceptive solutions effective against computer vision algorithms would be adopted more likely if they were less conspicuous to the human eye.

In the future, however, warfare may adopt a faster pace than is standard today. If people entrust decision-making to autonomous systems because they value their speed and accuracy more than human judgment, the human eye may leave the chain of evaluation and decision-making. In such a case, it might no longer be necessary to follow the principle of traditional military camouflage, which consists of visually blending in with the surroundings. In a scenario where one machine seeks to deceive the other, colorful patterns might be a reality.

Of course, adversarial camouflage might not only work as a defensive counterintelligence means. Although in my research, I did not delve into possible applications in direct combat, attacks on computer vision models and adversarial camouflage are relevant for combat operations as well. As it was suggested by Trevithick,⁹⁶ the aircraft covered in tires and painted decoys at the Russian air base were likely designed to thwart a strike by self-guided munition with computer vision capability. Electro-optical guided munition collects, processes, and analyzes images to reach and hit the target. Missiles of the type “fire-and-forget” can do this independently after being launched, which means that there is no need for human assistance, and the system can engage the target autonomously. For now, the deployment of fully autonomous weapons is restrained by ethical concerns, nonetheless, one of the defense methods that could be developed against electro-optical guided missiles is visual adversarial camouflage.

The proposals of adversarial attacks against object detectors discussed in this thesis have one major weakness, which is targeting only visible spectrum sensors. Despite the fact that deep learning models can work equally with images captured by sensors within other spectral bands like radio, infrared, or ultraviolet waves, the literature primarily concentrates on the visual spectrum. Camera sensors collecting visible light are undoubtedly the most accessible and convenient for experiments, and for some applications, such as autonomous

⁹⁶ Trevithick, Joseph. 2024. “Russia Covering Aircraft With Tires Is About Confusing Image-Matching Missile Seekers U.S. Military Confirms.” *The Warzone*. September 13, 2024. <https://www.twz.com/air/russia-covering-its-aircraft-in-tires-is-about-befuddling-image-matching-seekers-u-s-military-confirms>.

driving, they might be sufficient. However, the current challenge of military camouflage is multispectral and hyperspectral sensors. These cameras compose images from various spectral bands and are capable of fully exposing objects that were unnoticeable to the human eye.

Do camouflage patterns for the visible spectrum make any sense, then? Multispectral images have become an established equipment of modern militaries, and they can be integrated into various platforms, including UAVs, reconnaissance aircraft, and satellites. Yet, although the introduction of multispectral and hyperspectral sensors made employing camouflage more difficult and gave an advantage to the side conducting surveillance and reconnaissance, the use of advanced sensors also presented certain limits. Not only are high-performance multispectral and especially hyperspectral cameras expensive devices, but the images represent massive volumes of data requiring high computational power for processing. Consequently, the processing of such images may require more time than the processing of images taken in one spectral band. The longer processing time is not desirable in applications that are meant to produce (proposals for) quick decisions. Security and military contexts may demand real-time data processing, a capability that may not be available to everyone.

The advanced technologies of sensing can be compensated by the deployment of active camouflage and decoys, which target the sensors on several spectral bands. For instance, not only do today's inflatable decoys look indistinguishable from real tanks, armored vehicles, radars, weapons, and aircraft to the naked eye up to a close distance, but they are also capable of imitating radar, thermal, infrared, and radio signature of these objects. In the case of deliberate modification of various signatures besides the visual, the term signature management becomes more apt than camouflage. Signature management (or signature reduction) is, besides the mentioned inflatables, one of the principles of stealth technology. With advanced signature management technology, fighter jets may appear as small as an insect to a radar,⁹⁷ and on the contrary, decoy missiles can imitate signatures of larger and more important assets, such as aircraft.

The identification of such advanced decoys is no longer a task solely for IMINT, data falling within SIGINT and MASINT are also required for detection. This may suggest that

⁹⁷ Heinrichs, Rebecca L., Mackenzie Eaglen, Jennifer Bradley, Christopher Bowie, Rebecca Grant, and Kari A. Bingen. 2023. "America's B-21 Raiders: Deterring and Assuring in the New Cold War."

the future of camouflage and decoys will move towards more complex solutions, aiming at misleading sensors in several spectral bands at a time. Still, less sophisticated camouflage means and decoys may be useful at the tactical level, when there is less time to identify decoys and make decisions. As was pointed out by Mills, “[d]ecoys do not need to stand up to rigorous examination; they only need to complicate the adversary’s decision making to be effective.”⁹⁸ Alternatively, against algorithms, adversarial camouflage means might have a chance of success when deployed outside the realm of intensive surveillance, rather than on the battlefield, where sensors are concentrated on various platforms. In brief, the technological demands for future decoys and camouflage means will depend on the context and the level of deployment.

The opportunities and challenges related to the deployment of AI-enabled tools for intelligence analysis and adversarial camouflage methods targeting these tools could be further studied with other research methods. My research identified adversarial camouflage techniques that are frequently proposed as adversarial attacks on object detectors, presented their limitations, and discussed the possibilities of their real-world applications. By explaining the basic principles of adversarial camouflage attacks and putting them in the context of intelligence gathering, this thesis hopefully helped increase understanding of how computational capabilities can shape intelligence and warfare.

The body of literature I reviewed did not allow me to draw strong conclusions about how adversarial camouflage attacks could be deployed in the real world. In general, the scholarly literature on adversarial attacks on object detectors does not seem to overly engage in intelligence and military applications. This can be explained by the fact that I reviewed only publicly available literature, and I did not have access to knowledge from classified military research programs. Furthermore, the authors of the experiments rarely test their camouflage methods in the physical world, necessitating further testing to determine their applicability as counterintelligence solutions.

However, to better assess the impact on organizations and personnel in intelligence agencies and militaries, future research would undoubtedly benefit from accessing the experience of professionals who are familiar with practical challenges. Do they consider

⁹⁸ Mills, Walker. 2020. “A TOOL FOR DECEPTION: THE URGENT NEED FOR EM DECOYS.” War Room. February 27, 2020. <https://warroom.armywarcollege.edu/articles/tactical-decoys/>.

their AI-enabled tools reliable and trustworthy? How has their role as human analysts changed regarding the increasing reliance on automatized tools? Access to the expertise of intelligence agencies and militaries would certainly advance the academic discussion considerably, but given the sensitive nature of the information, it may be difficult to obtain.

The technological edge in AI is likely going to have a fundamental impact on the distribution of power in the future world. For scholars of security, geopolitics, and international relations, it would be beneficial to closely observe the capabilities that militaries and intelligence agencies have in operation, as this will define their success in future defense. Which countries have a chance to compete for leading positions and which have already dropped out of the AI arms race? How will the gaps between states in AI development affect future armed conflicts? We can better answer these questions if we have a better understanding of how these technologies work.

Conclusion

In a world where computer vision algorithms evaluate intelligence data, camouflage and deception have new rules. Assuming the growing reliance on AI-enabled technologies by the intelligence community and militaries, this research aimed to explore how object detection algorithms can be deceived by adversarial camouflage attacks. Based on my analysis of the secondary literature published in the field of computer science, I identified three basic techniques of adversarial attacks: adversarial camouflage patterns, adversarial patches, and imperceptible image perturbations. The introduced adversarial attacks achieved a high level of success in remaining completely undetected by object detectors or being classified as incorrect objects.

In the publicly available computer science literature, researchers do not tend to situate their proposals of adversarial camouflage attacks in security or military contexts. As a result, the camouflage patterns and patches tend to have conspicuous designs, which is not in accordance with the traditional camouflage principle of blending in with the surroundings. However, the researchers frequently experiment with applying the patterns and patches on vehicles and clothes, which are types of objects relevant to those contexts. Taking into account the attempts to deceive computer vision capabilities deployed in the war between Russia and Ukraine, I discussed the possibilities of applying the proposed adversarial attacks by militaries as a means of counterintelligence.

To answer my first research question, I conclude that object detectors can be attacked by modifying the visual appearance of the objects they sense. The first group of attacks is adversarial camouflage patterns, which can be applied on the surface of objects or, alternatively, on the surface they stand on if they are captured from aerial platforms. The second group of attacks, adversarial patches, affects only a part of an object, presenting potentially a less noticeable solution for the physical world. The third prominent group of attacks, imperceptible image perturbations, is distinct from the previous, as the visual modifications of objects take place in the digital space.

Regarding the applicability in real-world military contexts, adversarial camouflage patterns and patches of bold designs suffer from easy detectability by the human eye. And although we assume intelligence analysis is supported by AI-enabled systems, humans still play a role in the process, and there is a risk they will notice unnatural occurrences in the data. The suppression of color and design distinctiveness could, however, reduce the ability to mislead object detectors, especially if we take into account the obstacles created by

atmospheric conditions and the sensing of objects from different angles and distances. The imperceptible image perturbations, on the other hand, are almost undetectable by humans. The challenge of deploying this type of attack is the need to gain access to the given network and the ability to feed the system with modified data. Then, even a human analyst can review the data without noticing an attack.

To answer my second question, how have AI-enabled tools impacted intelligence analysis and the use of camouflage means, I argue that the modification of the visual appearance of objects (meaning, in the visual electromagnetic spectrum) is not the crucial struggle of today or the future. From the perspective of modern militaries, camouflage targeting only the visual spectrum becomes of little use. Advanced sensors are capable of collecting images in several spectral bands, which means that the countermeasures must be realized accordingly. While object detectors can still perform on images taken in spectral bands other than the visual, the visual adversarial camouflage patterns and patches discussed in this thesis will not be able to deceive them. Deployment of visual adversarial camouflage could be still effective in some circumstances, for example at the tactical level, where there is little time to make decisions or when no other data than visual are available to the adversary. For the future of deception, decoys capable of imitating various signatures may be of a greater role than means of visual camouflage, as they are capable of misleading both the human eye and sensors for various spectral bands. Of course, they do not fulfill the role of concealing the real assets, but they can lead the adversary into making wrong decisions.

My research sought to explain some inner principles behind adversarial camouflage attacks on object detectors and discuss the opportunities for their deployment by the intelligence community and militaries. The review of secondary literature as a chosen methodology allowed me to identify the major research trends and explore the technological possibilities and limitations of certain computer vision applications. My work contributes to the discussion of the use of AI applications for intelligence and counterintelligence and may help security studies scholars and intelligence practitioners grasp the basic principles behind computer vision technologies. In a world where governments are struggling to predict what the future of AI holds and how it should be regulated to minimize negative impacts on society, my work can also be useful to policymakers, as it explains the limits of the current object detection models and discusses the possibilities of their deployment in practice.

Summary

This thesis responds to the recent attempts to mislead computer vision algorithms deployed to analyze imagery data. The examples of deliberate visual modifications applied to military equipment and the use of special decoys imply that visual counterintelligence measures are going through an evolution. The challenge is no longer to hide objects from the human eye only but also to make them undetectable to AI-enabled capabilities. Today's world, abundant in collected data, requires intelligence organizations to automatize the process of data analysis, which means that not all data is evaluated by human senses and cognition.

In this research, the vulnerability of automatized intelligence analysis of imagery data is studied through a computer vision task known as object detection. If deep learning models are designed correctly and they are trained on suitable data, object detectors are capable of localizing an object within an image and assigning it to a certain class. As with any other AI model, object detectors are vulnerable to adversarial attacks. In this thesis, visual modifications of imagery data are discussed as a form of adversarial attack capable of preventing object detection algorithms from localizing and recognizing objects in the data. The aim of this thesis was to answer the following research questions: 1) How can object detection models be attacked by camouflage? 2) How have the AI-enabled tools impacted intelligence analysis and the use of camouflage means by militaries?

The current security studies literature does not reflect the new challenges brought by the automatization of IMINT. Some studies have addressed the role of AI for intelligence organizations and intelligence analysis as such, but the issues related to IMINT and the need for appropriate countermeasures remain neglected. Therefore, I turned to the literature in computer sciences to review the proposals for countermeasures against object detection. I sought to capture the main research trends and critically assess the possibilities of their application in intelligence and military contexts.

To answer my first research question, I presented methods of visual manipulations capable of hiding objects in imagery data. I identified three types of adversarial attacks in the literature: adversarial camouflage patterns and adversarial patches, both applied to objects in the physical world, and imperceptible image perturbations conducted through the visual manipulation of an image in the digital space. Then, I discussed their applicability in the real world, focusing on challenges such as perceptibility by the human eye or vulnerability to atmospheric conditions. To further assess the applicability of the camouflage

proposals by computer scientists, I compared them to the real-world examples of deception against computer vision that occurred during the War in Ukraine.

To answer my second research question, I put the findings about adversarial camouflage attacks in the context of the current discussion about the use of AI in intelligence and warfare. I considered scenarios in which the adversarial camouflage attacks could be successfully deployed and under what circumstances they are likely to fail. I argue that although the proposed attacks are capable of misleading computer vision algorithms, the major challenge preventing their deployment in the real world is sensors for imaging beyond visible light. Also, the proposed camouflage attacks suffer from the conspicuousness to the human eye, which creates a significant disadvantage as humans still tend to supervise machines and remain responsible for decision-making. I conclude that although adversarial camouflage attacks have not been deployed as a counterintelligence measure against computer vision algorithms, they might be adopted in the hypothetical future, when warfare becomes faster and less dependent on human decision-making.

Shrnutí

Tato diplomová práce reaguje na nedávné pokusy o oklamání algoritmů počítačového vidění určených k analýze obrazových dat. Případy záměrného pozměnění vzhledu vojenských objektů a využití zvláštních návnad naznačují, že maskovací prostředky prodělávají evoluci. Výzvou není již pouze skrýt objekty před lidským zrakem, ale také zabránit jejich detekci systémy využívajícími umělou inteligenci. V dnešním světě oplývajícím množstvím nashromážděných informací jsou zpravodajské organizace nuceny automatizovat proces analýzy dat, což znamená, že ne všechna data jsou vyhodnocována lidskými smysly a poznáním.

Tento výzkum se věnuje zranitelnosti automatizované zpravodajské analýze obrazových dat, která je analyzována skrze detekci objektů, jednu z úloh počítačového vidění. Detektory objektů, jsou-li správně navrženy a trénovány na vhodných datech, jsou schopny najít v rámci digitálního obrazu známé objekty a přiřadit je k naučeným třídám. Stejně jako každý jiný model strojového učení jsou i detektory objektů náchylné k adverzariálním útokům. V této práci jsou metody vizuální úpravy objektů chápány jako forma adverzariálního útoku schopná zabránit jejich detekci v obrazových datech. Cílem této práce bylo zodpovědět dvě výzkumné otázky: 1) Jak mohou být modely objektové detekce napadeny kamufláží? 2) Jak nástroje využívající umělou inteligenci ovlivnily zpravodajskou

analýzu a využití maskovacích prostředků armádami?

Současná diskuze v bezpečnostních studiích prozatím nereflakuje nové výzvy spojené s automatizací IMINT. Některé dosavadní studie adresovaly roli umělé inteligence ve zpravodajských organizacích a její vliv na zpravodajskou analýzu, nicméně otázkám souvisejícím s IMINT a adekvátním obranným prostředkům se dosud pozornosti nedostalo. Proto se obracím k literatuře publikované na poli informatiky, abych vytvořila přehled toho, jaké řešení se nabízí jako obrana proti detekci objektů. Cílila jsem na zachycení hlavních výzkumných trendů a kritické zhodnocení možného využití navržených adverzariálních útoků ve zpravodajském a vojenském kontextu.

Jako odpověď na první výzkumnou otázku prezentuji metody, které umožňují maskování objektů v obrazových datech. V literatuře jsem identifikovala tři typy adverzariálních útoků: adverzariální maskovací vzory a adverzariální záplaty, které lze aplikovat ve fyzickém světě, a nepostřehnutelné perturbace, které vznikají manipulací obrazu v digitálním prostoru. Poté jsem hodnotila jejich využitelnost v praxi, zejména s ohledem na jejich nápadnost lidskému zraku a vliv atmosférických podmínek na jejich efektivitu, a porovnála je s metodami klamání počítačového vidění, které byly využity během války mezi Ukrajinou a Ruskem.

S cílem zodpovědět druhou výzkumnou otázku jsem zasadila poznatky z výzkumu adverzariálních maskovacích útoků do diskuze o využití umělé inteligence pro zpravodajské a vojenské účely. Zvážila jsem scénáře, ve kterých by mohly být adverzariální maskovací útoky úspěšně nasazeny a za jakých podmínek by naopak neobstály. Předkládám argument, že ačkoli jsou adverzariální maskovací útoky schopny oklamat algoritmy počítačového vidění, zásadní problém komplikující jejich využívání jsou senzory snímající elektromagnetického záření za hranicí viditelného spektra. Současně jsou navrhované maskovací vzory příliš nápadné pro lidského oko, což znamená podstatnou nevýhodu, dokud lidé dohlížejí na práci automatizovaných systémů a jsou zodpovědní za rozhodování. Práci uzavírám tvrzením, že byť nebyly adverzariální maskovací útoky nasazeny jako obranný prostředek proti sledování algoritmy počítačového vidění, mohou najít své místo v hypotetické budoucnosti, ve které se válčení odehrává ve vyšším tempu a je méně závislé na lidském rozhodování.

List of References

- Adhikari, Ajaya, Richard den Hollander, Ioannis Tolios, Michael van Bekkum, Anneloes Bal, Stijn Hendriks, Maarten Kruithof, et al. 2020. "Adversarial Patch Camouflage against Aerial Detection," August. <http://arxiv.org/abs/2008.13671>.
- Ahmed, Nizam Uddin. 2022. "INTEGRATING MACHINE LEARNING IN MILITARY INTELLIGENCE PROCESS: STUDY OF FUTURISTIC APPROACHES TOWARDS HUMAN-MACHINE." *National Defence College E-Journal 2* (1): 59–89. <https://ndcjournal.ndc.gov.bd/ndcj>.
- Baumbach, Johannes. 2012. "Colour and Camouflage: Design Issues in Military Clothing." In *Advances in Military Textiles and Personal Equipment.*, 79–102. Woodhead Publishing.
- Biletskyi, Ihor, Hanna Dulfan, Lidiia Piddubna, and Nataliia Shyshko. 2023. "Objects Camouflage Possibilities Analysis in the Modern Military Conflicts Conditions." *Lighting Engineering & Power Engineering 62* (1): 23–27. <https://doi.org/10.33042/2079-424x.2023.62.1.04>.
- Brantly, Aaron F. 2018. "When Everything Becomes Intelligence: Machine Learning and the Connected World." *Intelligence and National Security 33* (4): 562–73. <https://doi.org/10.1080/02684527.2018.1452555>.
- Breakspear, Alan. 2013. "A New Definition of Intelligence." *Intelligence and National Security 28* (5): 678–93. <https://doi.org/10.1080/02684527.2012.699285>.
- Cannaday, Alan B., Curt H. Davis, and Trevor M. Bajkowski. 2023. "Detection of Camouflage-Covered Military Objects Using High-Resolution Multi-Spectral Satellite Imagery." In *International Geoscience and Remote Sensing Symposium (IGARSS)*, 2023-July:5766–69. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/IGARSS52108.2023.10281409>.
- Chen, Li, Guowei Zhu, Qi Li, and Haifeng Li. 2019. "Adversarial Example in Remote Sensing Image Recognition." ArXiv Preprint ArXiv:1910.13222. <http://arxiv.org/abs/1910.13222>.
- Clark, Robert M. 2013. "Guide to the Study of Intelligence Perspectives on Intelligence Collection." *The Intelligencer: Journal of U.S. Intelligence Studies 20* (2): 47–53. www.afio.com.
- Cleave, Michelle van. 2013. "What Is Counterintelligence?" *Intelligencer: Journal of US Intelligence Studies 20* (2): 57–65.
- Deng, Binyue, Denghui Zhang, Fashan Dong, Junjian Zhang, Muhammad Shafiq, and Zhaoquan Gu. 2023. "Rust-Style Patch: A Physical and Naturalistic Camouflage Attacks on Object Detector for Remote Sensing Images." *Remote Sensing 15* (4). <https://doi.org/10.3390/rs15040885>.
- Deng, Xiaotong, Zheng Fang, Yunfei Zheng, Yang Wang, Junming Huang, Xiaobing Wang, and Tiejong Cao. 2021. "Adversarial Examples with Transferred Camouflage Style for Object Detection." In *Journal of Physics: Conference Series*. Vol. 1738. IOP Publishing Ltd. <https://doi.org/10.1088/1742-6596/1738/1/012130>.
- Department of the Army. 1999. *FM 20-3 CAMOUFLAGE, CONCEALMENT, AND DECOYS*. Washington DC. [https://www.bits.de/NRANEU/others/amd-us-archive/FM20-3\(99\).pdf](https://www.bits.de/NRANEU/others/amd-us-archive/FM20-3(99).pdf).
- Department of the Army. 2010. *ATTP 3-34.39 CAMOUFLAGE, CONCEALMENT, AND DECOYS*. Washington DC. <https://apps.dtic.mil/sti/pdfs/ADA535471.pdf>.
- Dhillon, Anamika, and Gyanendra K. Verma. 2020. "Convolutional Neural Network: A Review of Models, Methodologies and Applications to Object Detection." *Progress in Artificial Intelligence 9* (2): 85–112. <https://doi.org/10.1007/s13748-019-00203-0>.
- Du, Andrew, Bo Chen, Tat-Jun Chin, Yee Wei Law, Michele Sasdelli, Ramesh Rajasegaran, and Dillon Campbell. 2022. "Physical Adversarial Attacks on an Aerial Imagery Object Detector." In *Proceedings of the*

IEEE/CVF Winter Conference on Applications of Computer Vision., 1796–1806.
<https://doi.org/doi:10.1109/WACV51458.2022.00385>.

Duan, Ranjie, Xingjun Ma, Yisen Wang, James Bailey, A K Qin, and Yun Yang. 2020. “Adversarial Camouflage: Hiding Physical-World Attacks with Natural Styles.” In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition.*, 1000–1008.

Duan, Yexin, Jialin Chen, Xingyu Zhou, Junhua Zou, Zhengyun He, Jin Zhang, Wu Zhang, and Zhisong Pan. 2021. “Learning Coated Adversarial Camouflages for Object Detectors.” ArXiv Preprint ArXiv:2109.00124 (2021). <http://arxiv.org/abs/2109.00124>.

Dupré, Robert E. 2011. “Guide to Imagery Intelligence.” *The Intelligence Journal of U.S. Intelligence Studies* 18 (2): 61–64.

Etten, Adam van. 2022. “The Weaknesses of Adversarial Camouflage in Overhead Imagery.” In *Proceedings - Applied Imagery Pattern Recognition Workshop*. Vol. 2022-October. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/AIPR57179.2022.10092201>.

Ghioni, Riccardo, Mariarosaria Taddeo, and Luciano Floridi. 2024. “Open Source Intelligence and AI: A Systematic Review of the GELSI Literature.” *AI and Society* 39 (4). <https://doi.org/10.1007/s00146-023-01628-x>.

Gill, Peter. 2010. “Theories of Intelligence.” In *The Oxford Handbook of National Security Intelligence*, 43–58. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780195375886.003.0003>.

Gleeson, Dennis J. 2023. “Artificial Intelligence for Analysis: The Road Ahead.” *Studies in Intelligence* 67 (4).

Guesmi, Amira, Ioan Marius Bilasco, Muhammad Shafique, and Ihsen Alouani. 2024. “AdvART: Adversarial Art for Camouflaged Object Detection Attacks.” In *2024 IEEE International Conference on Image Processing (ICIP)*, 666–72. IEEE. <https://doi.org/10.1109/ICIP51287.2024.10648014>.

Heinrichs, Rebecca L., Mackenzie Eaglen, Jennifer Bradley, Christopher Bowie, Rebecca Grant, and Kari A. Bingen. 2023. “America’s B-21 Raiders: Deterring and Assuring in the New Cold War.”

Hu, Shengnan, Yang Zhang, Sumit Laha, Ankit Sharma, and Hassan Foroosh. 2020. “CCA: Exploring the Possibility of Contextual Camouflage Attack on Object Detection.” In *Proceedings - International Conference on Pattern Recognition*, 7647–54. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ICPR48806.2021.9413194>.

Huang, Lifeng, Chengying Gao, Yuyin Zhou, Cihang Xie, Alan Yuille, Changqing Zou, and Ning Liu. 2020. “Universal Physical Camouflage Attacks on Object Detectors.” In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition.*, 720–29. <http://arxiv.org/abs/1909.04326>.

Ish, Daniel., Jared. Ettinger, and Christopher. Ferris. 2021. *Evaluating the Effectiveness of Artificial Intelligence Systems in Intelligence Analysis*. Santa Monica: RAND Corporation. <https://doi.org/https://doi.org/10.7249/RR-A464-1>.

Kim, Jeonghun, Kyungmin Lee, Hyeongkeun Lee, Hunmin Yang, and Se Yoon Oh. 2021. “Camouflaged Adversarial Attack on Object Detector.” In *International Conference on Control, Automation and Systems*, 2021-October:613–17. IEEE Computer Society. <https://doi.org/10.23919/ICCAS52745.2021.9650004>.

Lapid, Raz, and Moshe Sipper. 2023. “Patch of Invisibility: Naturalistic Physical Black-Box Adversarial Attacks on Object Detectors.” <http://arxiv.org/abs/2303.04238>.

Li, Dandan, Yufeng Li, Guiqi Zhang, Ke Sun, and Jiangtao Li. 2023. “Fooling Object Detectors in the Physical World with Natural Adversarial Camouflage.” In *Proceedings - 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications*,

TrustCom/BigDataSE/CSE/EUC/ISCI 2023, 141–48. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/TrustCom60117.2023.00040>.

Li, Debang, Junge Zhang, and Kaiqi Huang. 2020. “Universal Adversarial Perturbations against Object Detection.” *Pattern Recognition* 110 (February). <https://doi.org/10.1016/j.patcog.2020.107584>.

Li, Xin, Jian Chen, Xinpeng Jiang, Junxiang Zeng, Xinye Liao, Yutai Chen, Siyang Xiao, et al. 2023. “Multispectral Camouflage Nanostructure Design Based on a Particle Swarm Optimization Algorithm for Color Camouflage, Infrared Camouflage, Laser Stealth, and Heat Dissipation.” *Optics Express* 31 (26): 44811–22. <https://doi.org/10.1364/oe.510680>.

Li, Yisheng, Xuekang Peng, and Zhichao Lian. 2024. “Multi-Texture Fusion Attack: A Robust Adversarial Camouflage in Physical World.” In *International Conference on Intelligent Computing. Lecture Notes in Computer Science, Vol 14870.*, edited by DS Huang, W Chen, and J Guo, 14870 LNCS:186–98. Springer, Singapore. https://doi.org/10.1007/978-981-97-5606-3_16.

Man, Keith, and Javaan Chahl. 2022. “A Review of Synthetic Image Data and Its Use in Computer Vision.” *Journal of Imaging* 8 (11). <https://doi.org/10.3390/jimaging8110310>.

Matthews, Ron, and Thomas J. Matthews. 2024. “Military Mimicry: The Art of Concealment, Deception, and Imitation.” *Defense and Security Analysis*. <https://doi.org/10.1080/14751798.2024.2352271>.

Mills, Walker. 2020. “A TOOL FOR DECEPTION: THE URGENT NEED FOR EM DECOYS.” War Room. February 27, 2020. <https://warroom.armywarcollege.edu/articles/tactical-decoys/>.

Monahan, Torin. 2015. “The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance.” *Communication and Critical/ Cultural Studies* 12 (2): 159–78. <https://doi.org/10.1080/14791420.2015.1006646>.

Moran, Christopher R., Joe Burton, and George Christou. 2023. “The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying.” *Journal of Global Security Studies* 8 (2). <https://doi.org/10.1093/jogss/ogad005>.

Muszyński-Sulima, Wawrzyniec. 2023. “Cold War in Space: Reconnaissance Satellites and US-Soviet Security Competition.” *European Journal of American Studies* 18 (2). <https://doi.org/10.4000/ejas.20427>.

NATO. 2024. “NATOTerm. The Official NATO Terminology Database.” NATOTerm. 2024. <https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en>.

NATO Standardization Office. 2016. *NATO STANDARD AJP-2 ALLIED JOINT DOCTRINE FOR INTELLIGENCE, COUNTER-INTELLIGENCE AND SECURITY Edition A Version 2*.

Pereira, Antonio L B. 2024. “The IC AI Multiplier: Automating Superiority Seizing Adversarial Artificial Intelligence Use in Intelligence Operations.” https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4884351.

Puyvelde, Damien van, Stephen Coulthart, and M. Shahriar Hossain. 2017. “Beyond the Buzzword: Big Data and National Security Decision-Making.” *International Affairs* 93 (6): 1397–1416. <https://doi.org/10.1093/ia/iix184>.

Rahman, Md Mostafizur, Aisha Siddika Arshi, Md Mehedi Hasan, Sumayia Farzana Mishu, Hossain Shahriar, and Fan Wu. 2023. “Security Risk and Attacks in AI: A Survey of Security and Privacy.” In *Proceedings - International Computer Software and Applications Conference, 2023-June*:1834–39. IEEE Computer Society. <https://doi.org/10.1109/COMPSAC57700.2023.00284>.

Rathore, Pradeep, Arghya Basak, Sri Harsha Nistala, and Venkataramana Runkana. 2020. “Untargeted, Targeted and Universal Adversarial Attacks and Defenses on Time Series.” In *Proceedings of the International Joint Conference on Neural Networks*. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/IJCNN48605.2020.9207272>.

- Read, J. M., and M. Torrado. 2009. "Remote Sensing." In *International Encyclopedia of Human Geography: Volume 1-12*, 335–46. Elsevier. <https://doi.org/10.1016/B978-008044910-4.00508-3>.
- Regens, James L. 2019. "Augmenting Human Cognition to Enhance Strategic, Operational, and Tactical Intelligence." *Intelligence and National Security* 34 (5): 673–87. <https://doi.org/10.1080/02684527.2019.1579410>.
- Ren, Huali, Teng Huang, and Hongyang Yan. 2021. "Adversarial Examples: Attacks and Defenses in the Physical World." *International Journal of Machine Learning and Cybernetics* 12 (11): 3325–36. <https://doi.org/10.1007/s13042-020-01242-z>.
- Saugmann, Rune. 2019. "Military Techno-Vision: Technologies between Visual Ambiguity and the Desire for Security Facts." *European Journal of International Security* 4 (3): 300–321. <https://doi.org/10.1017/eis.2019.17>.
- Scheuerman, Morgan Klaus, Alex Hanna, and Emily Denton. 2021. "Do Datasets Have Politics? Disciplinary Values in Computer Vision Dataset Development." *Proceedings of the ACM on Human-Computer Interaction* 5 (CSCW2). <https://doi.org/10.1145/3476058>.
- Sharkey, Amanda, and Noel Sharkey. 2021. "Sunlight Glinting on Clouds: Deception and Autonomous Weapons Systems." In *Counter-Terrorism, Ethics and Technology. Emerging Challenges at the Frontiers of Counter-Terrorism*, edited by Adam Henschke, Alastair Reed, Scott Robbins, and Seumas Miller, 35–48. Cham: Springer. <https://doi.org/10.1007/978-3-030-90221-6>.
- Smith, Michael A., and Tsuhan Chen. 2005. "Image and Video Indexing and Retrieval." *Handbook of Image and Video Processing, Second Edition*, January, 993–XXXI. <https://doi.org/10.1016/B978-012119792-6/50121-2>.
- Starck, Nick, David Bierbrauer, and Paul Maxwell. 2022. "Artificial Intelligence, Real Risks: Understanding—and Mitigating—Vulnerabilities in the Military Use of AI." Modern War Institute. January 18, 2022. <https://mwi.westpoint.edu/artificial-intelligence-real-risks-understanding-and-mitigating-vulnerabilities-in-the-military-use-of-ai/>.
- Sun, Jialiang, Wen Yao, Tingsong Jiang, Donghua Wang, and Xiaoqian Chen. 2023. "Differential Evolution Based Dual Adversarial Camouflage: Fooling Human Eyes and Object Detectors." *Neural Networks* 163 (June): 256–71. <https://doi.org/10.1016/j.neunet.2023.03.041>.
- Sun, Yibo, Zhe Sun, and Weitong Chen. 2024. "The Evolution of Object Detection Methods." *Engineering Applications of Artificial Intelligence* 133 (July). <https://doi.org/10.1016/j.engappai.2024.108458>.
- Suryanto, Naufal, Yongsu Kim, Hyoeun Kang, Harashta Tatimma Larasati, Youngyeo Yun, Thi-Thu-Huong Le, Hunmin Yang, Se-Yoon Oh, and Howon Kim. 2022. "DTA: Physical Camouflage Attacks Using Differentiable Transformation Network." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 15305–14. https://openaccess.thecvf.com/content/CVPR2022/html/Suryanto_DTA_Physical_Camouflage_Attacks_Using_Differentiable_Transformation_Network_CVPR_2022_paper.html.
- Sutton, H I. 2023. "New Technology Sees Through Russian Attempt to Hide Ships from Ukraine." Naval News. July 12, 2023. <https://www.navalnews.com/naval-news/2023/07/new-technology-sees-through-russian-attempt-to-hide-ships-from-ukraine/>.
- Szegedy, Christian, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. 2013. "Intriguing Properties of Neural Networks." <http://arxiv.org/abs/1312.6199>.
- Talas, Laszlo, Roland J. Baddeley, and Innes C. Cuthill. 2017. "Cultural Evolution of Military Camouflage." *Philosophical Transactions of the Royal Society B: Biological Sciences* 372 (1724). <https://doi.org/10.1098/RSTB.2016.0351>.

- Tang, Guijian, Tingsong Jiang, Weien Zhou, Chao Li, Wen Yao, and Yong Zhao. 2023. "Adversarial Patch Attacks against Aerial Imagery Object Detectors." *Neurocomputing* 537 (June): 128–40. <https://doi.org/10.1016/j.neucom.2023.03.050>.
- Tian, Jiwei, Buhong Wang, Rongxiao Guo, Zhen Wang, Kunrui Cao, and Xiaodong Wang. 2022. "Adversarial Attacks and Defenses for Deep-Learning-Based Unmanned Aerial Vehicles." *IEEE Internet of Things Journal* 9 (22): 22399–409. <https://doi.org/10.1109/JIOT.2021.3111024>.
- Toroi, George-Ion. 2024. "MULTI-DOMAIN DECEPTION -CONTEMPORARY OPERATIONAL REQUIREMENT." In *PROCEEDINGS OF THE INTERNATIONAL SCIENTIFIC CONFERENCE STRATEGIES XXI. VOLUME XIX*, 376–88. <https://doi.org/1053477/2971-8813-23-40>.
- Trevithick, Joseph. 2024a. "Submarine Decoy Appears On Russian Naval Base Pier." The Warzone. March 20, 2024. <https://www.twz.com/news-features/submarine-decoy-appears-on-russian-naval-base-pier>.
- Trevithick, Joseph. 2024b. "Russia Covering Aircraft With Tires Is About Confusing Image-Matching Missile Seekers U.S. Military Confirms." The Warzone. September 13, 2024. <https://www.twz.com/air/russia-covering-its-aircraft-in-tires-is-about-befuddling-image-matching-seekers-u-s-military-confirms>.
- Tudor, Ciprian Gabriel. 2019a. "CAMOUFLAGE, CONCEALMENT AND DECEPTION IN MILITARY OPERATIONS." In *SCIENTIFIC CONFERENCE STRATEGIES XXI. The Complex and Dynamic Nature of the Security Environment*. Vol. 1. Bucharest.
- Tudor, Ciprian Gabriel. 2019b. "GEOINT IN MONITORING AND DETECTION OF MILITARY CAMOUFLAGE, CONCEALMENT AND DECEPTION – GEOINT COUNTERDECEPTION." In *INTERNATIONAL SCIENTIFIC CONFERENCE STRATEGIES XXI. The Complex and Dynamic Nature of the Security Environment - Volume 1*, edited by Florian CÎRCIUMARU and Iulia-Alexandra COJOCARU, 362–70. Bucharest: Carol I National Defence University Publishing House.
- Vogel, Kathleen M., Gwendolynne Reid, Christopher Kampe, and Paul Jones. 2021. "The Impact of AI on Intelligence Analysis: Tackling Issues of Collaboration, Algorithmic Transparency, Accountability, and Management." *Intelligence and National Security* 36 (6): 827–48. <https://doi.org/10.1080/02684527.2021.1946952>.
- Vries, Patricia de, and Willem Schinkel. 2019. "Algorithmic Anxiety: Masks and Camouflage in Artistic Imaginaries of Facial Recognition Algorithms." *Big Data and Society* 6 (1): 1–12. <https://doi.org/10.1177/2053951719851532>.
- Wang, Jiakai, Aishan Liu, Zixin Yin, Shunchang Liu, Shiyu Tang, and Xianglong Liu. 2021. "Dual Attention Suppression Attack: Generate Adversarial Camouflage in Physical World." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*.
- Wang, Xiaofei, Shaohui Mei, Jiawei Lian, and Yingjie Lu. 2024. "Fooling Aerial Detectors by Background Attack via Dual-Adversarial-Induced Error Identification." *IEEE Transactions on Geoscience and Remote Sensing* 62. <https://doi.org/10.1109/TGRS.2024.3386533>.
- Warner, Michael. 2002. "Understanding Our Craft Wanted: A Definition of Intelligence." *Studies in Intelligence* 46 (3): 15–22.
- Wu, Zuxuan, Ser-Nam Lim, Larry S Davis, and Tom Goldstein. 2020. "Making an Invisibility Cloak: Real World Adversarial Attacks on Object Detectors." In *Computer Vision – ECCV 2020. ECCV 2020. Lecture Notes in Computer Science, Vol 12349*, edited by Andrea Vedaldi, Horst Bischof, Thomas Brox, and Jan-Michael Frahm. Vol. 12349. Lecture Notes in Computer Science. Springer, Cham. <https://doi.org/10.1007/978-3-030-58548-8>.
- Wysocki, Krzysztof, and Martyna Niewińska. 2022. "Counteracting Imagery (IMINT), Optoelectronic (EOIMINT) and Radar (SAR) Intelligence." *Scientific Journal of the Military University of Land Forces* 204 (2): 222–44. <https://doi.org/10.5604/01.3001.0015.8975>.

- Xu, Huan, and Shie Mannor. 2012. "Robustness and Generalization." *Machine Learning* 86 (3): 391–423. <https://doi.org/10.1007/s10994-011-5268-1>.
- Zhang, Haotian, and Xu Ma. 2022. "Misleading Attention and Classification: An Adversarial Attack to Fool Object Detection Models in the Real World." *Computers and Security* 122 (November). <https://doi.org/10.1016/j.cose.2022.102876>.
- Zhang, Yang, Hassan Foroosh, Philip David, and Boqing Gong. 2019. "CAMOU: LEARNING A VEHICLE CAMOUFLAGE FOR PHYSICAL ADVERSARIAL ATTACK ON OBJECT DETECTORS IN THE WILD." In *ICLR 2019*.
- Zhang, Yu, Jianqi Chen, Zhenbang Peng, Yi Dang, Zhenwei Shi, and Zhengxia Zou. 2024. "Physical Adversarial Attacks Against Aerial Object Detection With Feature-Aligned Expandable Textures." *IEEE Transactions on Geoscience and Remote Sensing* 62. <https://doi.org/10.1109/TGRS.2024.3426272>.
- Zhao, Zhong Qiu, Peng Zheng, Shou Tao Xu, and Xindong Wu. 2019. "Object Detection with Deep Learning: A Review." *IEEE Transactions on Neural Networks and Learning Systems* 30 (11): 3212–32. <https://doi.org/10.1109/TNNLS.2018.2876865>.
- Zhou, Jiawei, Linye Lyu, Daojing He, and Yu Li. 2024. "RAUCA: A Novel Physical Adversarial Attack on Vehicle Detectors via Robust and Accurate Camouflage Generation." In *Proceedings of the 41st International Conference on Machine Learning*. <http://arxiv.org/abs/2402.15853>.
- Zhou, Yue, Wanghan Jiang, Xue Jiang, Lin Chen, and Xingzhao Liu. 2023. "CamoNet: A Target Camouflage Network for Remote Sensing Images Based on Adversarial Attack." *Remote Sensing* 15 (21). <https://doi.org/10.3390/rs15215131>.
- Zou, Zhengxia, Keyan Chen, Zhenwei Shi, Yuhong Guo, and Jieping Ye. 2023. "Object Detection in 20 Years: A Survey." *Proceedings of the IEEE* 111 (3): 257–76. <https://doi.org/10.1109/JPROC.2023.3238524>.