



Artificial Intelligence and Global Security

Future Trends, Threats and Considerations

Edited by Yvonne R. Masakowski



Artificial Intelligence and Global Security

This page intentionally left blank

Artificial Intelligence and Global Security: Future Trends, Threats and Considerations

EDITED BY

YVONNE R. MASAKOWSKI

US Naval War College, USA



United Kingdom – North America – Japan – India – Malaysia – China

Emerald Publishing Limited
Howard House, Wagon Lane, Bingley BD16 1WA, UK

First edition 2020

Copyright © 2020 Emerald Publishing Limited

Reprints and permissions service

Contact: permissions@emeraldinsight.com

No part of this book may be reproduced, stored in a retrieval system, transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise without either the prior written permission of the publisher or a license permitting restricted copying issued in the UK by The Copyright Licensing Agency and in the USA by The Copyright Clearance Center. Any opinions expressed in the chapters are those of the authors. Whilst Emerald makes every effort to ensure the quality and accuracy of its content, Emerald makes no representation implied or otherwise, as to the chapters' suitability and application and disclaims any warranties, express or implied, to their use.

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

Disclaimer

The views and material presented in this book are the sole responsibility of the authors/editor and do not reflect the views or the official positions of the US Naval War College, The US Department of the Navy. The US Department of Defense (DoD) or other agencies of the United States Government.

This book is presented solely for educational and informational purposes. Although the authors and publisher have made every effort to ensure that the information in this book was correct at press time, the authors and publisher do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors of omission result from negligence, accident, or any other cause. The authors and publisher are not offering it as legal, accounting, or other professional services advice.

Neither the authors nor the publisher shall be held liable or responsible to any person or entity with respect to any loss or incidental or consequential damages caused, or alleged to have been caused, directly or indirectly, by the information or advice contained herein. Every company and organization is different and the strategies and recommendations contained herein may not be suitable to your organization and/or situation.

ISBN: 978-1-78973-812-4 (Print)

ISBN: 978-1-78973-811-7 (Online)

ISBN: 978-1-78973-813-1 (Epub)



ISOQAR
REGISTERED

Certificate Number 1985
ISO 14001

ISOQAR certified
Management System,
awarded to Emerald
for adherence to
Environmental
standard
ISO 14001:2004.



INVESTOR IN PEOPLE

This book is dedicated to all military personnel who place their lives on the line to preserve our freedoms. I would like to thank my family and US Naval War College friends and colleagues, especially Dr. Timothy J. Demy and Dr. William F. Bundy for their encouragement and support. Special thanks to those military students whom I had the privilege to teach and mentor during my tenure as a Professor at the US Naval War College. Special appreciation to my students from the Ethics and Emerging Military Technologies (EEMT) graduate certificate program for many hours of exciting and inspirational discussion on Artificial Intelligence and future warfare. These Officers are the military's brightest officers selected as students at the Naval War College. These officers are our nation's future military leaders.

If you want one year of prosperity, *grow grain.*

If you want ten years of prosperity, *grow trees.*

If you want one hundred years of prosperity, *grow leaders.*

Chinese Proverb

This page intentionally left blank

Table of Contents

About the Editor	<i>xv</i>
About the Contributors	<i>xvii</i>
List of Contributors	<i>xxi</i>
Preface	<i>xxiii</i>

The book was written by researchers and authors across many disciplines and domains – Artificial Intelligence (AI), autonomous unmanned systems, undersea, space, as well as humanitarian crises, including the ethical, theological, and moral conflicts of war. These areas and topics encompass numerous moral and ethical issues. Among the questions these chapters will explore are: What are the implications of AI for the individual, for personal identity, privacy, and freedom, and for society? What are the consequences of AI advances related to national and global security? These chapters will examine the perspectives and consequences for the integration of AI in our daily lives, as well as its influence on society and war. Authors will present their perspectives on the potential for significant consequences related to the impact of AI on an individual's identity that may place society at risk. What are the moral and ethical boundaries and responsibilities of each person's life as AI blends with humans into the whole of society? Does humanity lose its identity in the process? Where are the lines drawn between AI systems and the human? These are but a few of the questions that will be examined in these chapters. Whatever the course of action, AI will continue to be part of our future world. As such, humans must chart a course of action to navigate the waters of the future that we design for ourselves.

Chapter 1 Artificial Intelligence and the Future Global Security Environment

Yvonne R. Masakowski

1

Advances in Artificial Intelligence (AI) technologies and Autonomous Unmanned Vehicles will shape our daily lives, society, and future warfare. This chapter will explore the evolutionary and revolutionary influence of AI on the individual, society, and warfare in the twenty-first-century security environment. As AI technologies evolve, there will be increased reliance on these systems due to their ability to analyze and manage vast amounts of data. There are numerous benefits in applying AI to system designs that will support smart, digital cities, as well as support the future warfighter. However, advances in AI-enabled systems do not come without some element of risk (Hawking, Musk, & Wozniak, 2015). For the military, AI will serve as a force multiplier and will have a direct impact on future global security. The military seeks to exploit advances in AI and autonomous systems as a means of achieving technological superiority over their adversaries. We will explore the advantages and potential risks associated with the emergence of AI systems in the future battlespace (Armstrong, Bostrom, & Shulman, 2016). This chapter will serve as the foundation for examining issues such as ethical decision-making, moral reasoning, etc., related to the integration of AI systems in our daily lives, as well as in the future battlespace. Consequences for integrating AI into all aspects of society and military operations will be explored, as well as the implications for future global security.

Chapter 2 Artificially Intelligent Techniques for the Diffusion and Adoption of Innovation for Crisis Situations

Thomas C. Choinski

35

The diffusion and adoption of innovation propels today's technological landscape. Crisis situations, real or perceived, motivate communities of people to take action to adopt and diffuse innovation. This chapter will discuss the ability of Artificial Intelligence to resolve the challenges confronting the diffusion and adoption of innovation. Capacity, risk, resources, culture, complexity, ethics, and emerging situations affect the pace of diffusion and adoption. Artificial Intelligence can search the solution space, identify potential solutions, reduce risk, and mitigate unintended consequences while addressing the value proposition in order to chart courses of action through social networks. In doing so, artificial intelligence can accelerate the diffusion and adoption of technological innovation and contribute to the resolution of immediate crisis situations, as well as chart courses of action through emerging landscapes. However, Artificial Intelligence can help humans, but not replace their role this process. Achieving this goal will require a better understanding of human and machine interaction.

Chapter 3 “Something Old, Something New” – Reflections on AI and the Just War Tradition

Timothy J. Demy

53

This chapter will focus on the relationship between the centuries-old and prevailing tradition of warfare in the West and the innovations and challenges of AI with respect to the tradition and emerging norms of warfare. It will investigate whether the nature of warfare is changing or the weapons of warfare are changing and how such change affects the normative framework.

Chapter 4 Space War and AI

Keith A. Abney

63

New technologies, including AI, have helped us begin to take our first steps off the Earth and into outer space. But conflicts inevitably will arise and, in the absence of settled governance, may be resolved by force, as is typical for new frontiers. But the terrestrial assumptions behind the ethics of war will need to be rethought when the context radically changes, and both the environment of space and the advent of robotic warfighters with superhuman capabilities will constitute such a radical change. This chapter examines how new autonomous technologies, especially dual-use technologies, and the challenges to human existence in space will force us to rethink the ethics of war, both from space to the Earth, and in space itself.

Chapter 5 Building an Artificial Conscience: Prospects for Morally Autonomous Artificial Intelligence

William D. Casebeer

81

Discussions of ethics and Artificial Intelligence (AI) usually revolve around the ethical implications of the use of AI in multiple domains, ranging from whether machine learning trained algorithms may encode discriminatory standards for face recognition, to discussions of the implications of using artificial intelligence as a substitute for human intelligence in warfare. In this chapter, I will focus on one particular strand of ethics and AI that is often neglected: whether we can use the methods of AI to build or train a system which can reason about moral issues. Here, I discuss (1) what an “artificial conscience” consists of and what it would do, (2) why we collectively should build one soon given the increasing use of AI in multiple areas, (3) how we might build one in both architecture and content, and (4) concerns about building an artificial conscience and my rejoinders. Given the increasing importance of artificially intelligent semi- or fully autonomous systems and platforms for contemporary warfare, I conclude that building an artificial conscience is not only possible but also morally required if our autonomous teammates are to collaborate fully with human soldiers on the battlefield.

**Chapter 6 Artificial Intelligence and Ethical Dilemmas
Involving Privacy**

James Peltz and Anita C. Street

95

This chapter explores how data-driven methods such as Artificial Intelligence pose real concerns for individual privacy. The current paradigm of collecting data from those using online applications and services is reinforced by significant potential profits that the private sector stands to realize by delivering a broad range of services to users faster and more conveniently. Terms of use and privacy agreements are a common source of confusion, and are written in a way that dulls their impact and dopes most into automatically accepting a certain level of risk in exchange for convenience and “free” access. Third parties, including the government, gain access to these data in numerous ways. If the erosion of individual protections of privacy and the potential dangers this poses to our autonomy and democratic ideals were not alarming enough, the digital surrogate product of “you” that is created from this paradigm might one day freely share thoughts, buying habits, and your pattern of life with whoever owns these data. We use an ethical framework to assess key factors in these issues and discuss some of the dilemmas posed by Artificial Intelligence methods, the current norm of sharing one’s data, and what can be done to remind individuals to value privacy. Will our digital surrogate one day need protections too?

**Chapter 7 Artificial Intelligence and Moral Reasoning:
Shifting Moral Responsibility in War?**

Pauline Shanks Kaurin and Casey Thomas Hart

121

How does AI shift the burden of moral responsibility in war? It is no longer merely far-fetched science fiction to think that robots will be the chief combatants, waging wars in place of humans. Or is it? While Artificial Intelligence (AI) has made remarkable strides, tempting us to personify the machines “making decisions” and “choosing targets,” a more careful analysis reveals that even the most sophisticated AI can only be an instrument rather than an agent of war. After establishing the layered existential nature of war, we lay out the prerequisites for being a (moral) agent of war. We then argue that present AI falls short of this bar, and we have strong reason to think this will not change soon. With that in mind, we put forth a second argument against robots as agents: there is a continuum with other clearly nonagential tools of war, like swords and chariots. Lastly, we unpack what this all means: if AI does not add another moral player to the battlefield, how (if at all) should AI change the way we think about war?

Chapter 8 Ethical Constraints and Contexts of Artificial Intelligent Systems in National Security, Intelligence, and Defense/Military Operations

John R. Shook, Tibor Solymosi and James Giordano

137

Artificially intelligent (AI) systems are being considered for their potential utility and value in a variety of warfare, intelligence, and national security (WINS) settings. In light of this, it is becoming increasingly important to recognize the capabilities, limitations, effects, and need for guidance and governance of different types of AI systems and uses in WINS initiatives.

Most generally, AI systems can be regarded as “soft” or “hard,” although, in reality, these are not wholly binary, but rather exist along a continuum of structural and functional complexity of design and operations. “Soft AI” retains and reveals the fingerprint of responsibility incurred by the human builder and operator. It is programmed and controlled, and at best only semi-autonomous. Here attribution can be placed upon human factors in the design and/or articulation-of-action/event(s) chain. “Hard AI” (e.g., autonomous systems), however, can break that chain, if and when the system moves beyond its initial human-programmed input–output features to evidence “developed/inherent” – and not simply directly derived – characteristics and traits.

Law will likely infer that there is a builder’s bias and basis for any man-made system, and thus could argue that burden of responsibility would rest upon the human enterprise that evidenced the most probable custodianship/stewardship of the feature evoking the action in question.

But this could fail to obtain if and when a system becomes autonomous (e.g., via hierarchical generative encoding). In such an instance, the system could develop novel characteristics as adaptive properties, in some cases in response to and as rejective reaction to certain exogenous (i.e., human) attempts at constraint, imposition, and control.

This result would prompt questions of responsibility, attribution, and considerations of developmental trajectories, possible effects, and regulation and possibilities, viability and definable constraints of use.

This chapter will focus upon these possibilities, and address:

1. Peer capability conferred by AI in asymmetrical engagements.
2. Concepts and content of what constitutes *jus contra bellum*, *jus ad bellum*, and *jus in bello* parameters of AI use in political and military engagements.
3. Effect of AI use on relative threshold(s) and tolerances for warfare.
4. Proposed approaches to risk analysis, mitigation, and operational guidance of AI systems in WINS settings.

Chapter 9 An AI Enabled NATO Strategic Vision for Twenty-First-Century Complex Challenges

Imre Porkoláb

153

In the twenty-first century, the international defense community has largely struggled with how to organize, strategize, and act effectively in increasingly complex and emergent contexts where the previous distinctions between war and peace have blurred beyond comprehension. Popularly termed “black swan events” continue to shatter any illusion of stability or extension of normalcy in foreign affairs.

Western armed forces as well as intergovernmental military alliances such as NATO appear increasingly unable to deal with these problems using traditional planning and organizing methodologies alone. What had worked well previously no longer appears to possess the same precision and control. The formal operational-level military planning process, initially developed to cope with Cold War Era large-scale military activities in “a conventional, industrialized state vs industrialized state setting” now is seemingly incapable of providing sufficient means of getting the organization unstuck.

Within this new and increasingly complex context, coupled with the increasing tempo of the Fourth Industrial Revolution, NATO has to fulfill all three core tasks at the same time, and in a sense go through a complete digital transformation. It requires new and noble approaches from policymakers, and military personnel alike.

Artificial Intelligence is playing a crucial role during this digital transformation. In this chapter the author will address Artificial Intelligence in future multinational military operations, introduce the most recent political discussions, as well as the research trends and the implications on future warfare for the Alliance.

Specific topics that will be covered include:

- Possibility to use AI in future foresight analysis – better foresight through machine learning.
- Artificial Intelligence and the lessons learned process – how can we transform NATO into a learning organization?
- Capability building – possibilities for using AI and big data analysis to assess capability gaps and improve the defence planning capability system.
- Joint research – cooperation in AI research (Pentagon JAIC, CNAS AI center, and NATO AI research facilities).

Chapter 10 AI Ethics: Four Key Considerations for a Globally Secure Future

Gina Granados Palmer

167

Harnessing the power and potential of AI continues a centuries-old trajectory of the application of science and knowledge for the benefit of humanity. Such an endeavor has great promise, but also the possibility of creating conflict and

disorder. This chapter draws upon the strengths of the previous chapters to provide readers with a purposeful assessment of the current AI security landscape, concluding with four key considerations for a globally secure future.

**Chapter 11 Epilogue: The Future of Artificial Intelligence
and Global Security**

James Canton

177

Dr. James Canton, CEO and Chairman of the Institute for Global Futures (www.GlobalFuturist.com), will provide a Futuristic view of Artificial Intelligence.

Index

185

This page intentionally left blank

About the Editor



Yvonne R. Masakowski, PhD, MPhil, MA, has a distinguished career in Psychology and Human Factors spanning over 25 years. She was recently appointed as a Research Fellow by the US Naval War College following her retirement as an Associate Professor of Strategic Leadership and Leader Development in the College of Leadership and Ethics at the US Naval War College. At the Naval War College, Dr. Masakowski focused on the advancement of leader development for the US Navy and the impact of advanced AI technologies on military affairs. Dr. Masakowski currently serves as the US Chair of a NATO panel on *Leader Development for NATO Multinational Military Operations* (NATO HFM RTG 286). She also serves as a dissertation thesis mentor on Artificial Intelligence in the Ethics and Emerging Military Technology (EEMT) graduate certificate program at the US Naval War College. Prior appointments included serving as an Associate Director for Human Factors, Office of Naval Research Global office in London, UK, and as the CNO Science Advisor to the Strategic Studies Group (CNO SSG).

Dr. Masakowski earned her Doctorate of Philosophy in Psychology and Master's Degree in Philosophy at The City University of New York. She received a Master's Degree in Psychology (Psycholinguistics) from the University of Connecticut and her Bachelor of Arts in Experimental Psychology from Rutgers University. She earned a diploma from the MIT Seminar XXI program in Foreign Policy and National Security. She has also attended Yale University

where she studied biomedical ethics. She has taught leadership, ethics, cross-cultural competence, and the humanities to graduate students. She has also provided executive leader development to US Navy Admirals and US Navy Attorneys. Her research interests include Artificial Intelligence, decision-making, autonomous systems, leader development, cross-cultural competence, and the Humanities. Dr. Masakowski is the author of numerous publications, articles, as well as book chapters. She has edited a book on Decision Making in Complex Environments, and has written the following book chapters: The Impact of Synthetic Virtual Environments on Combat System Design and Operator Performance in Computing with Instinct; Cultural Competence and Leadership in Multinational Military Operations in Military Psychology from an International Perspective; The Dynamics of NATO Multinational Military Operations Inclusive Leadership Practice in Global and Culturally Diverse Leaders and Leadership; and Leaders and Ethical Leadership in Military and Leadership Development.

Dr. Masakowski's leadership and results-oriented philosophy have been recognized nationally and internationally. She has recently been awarded the US Department of Defense *Superior Civilian Service Award* (2019) and the *Lifetime Achievement Award* by the Albert Nelson Marquis Lifetime Achievement Award from the Marquis Who's Who Publications Board. Dr. Masakowski has also been recognized by the Czech Republic and awarded their nation's highest military Medal of Honor, *The Cross of Merit*. She has also been the recipient of awards from France and Poland for her efforts in advancing Science and Technology for military applications.

About the Contributors

Keith A. Abney, MA, is senior lecturer in the Philosophy Department and Research Fellow of the Ethics & Emerging Sciences Group at California Polytechnic State University, San Luis Obispo. His areas of expertise include many aspects of emerging technology ethics and bioethics, especially issues in space ethics and bioethics, robotics, AI and cyberethics, autonomous vehicles, human enhancements, and military technologies. He is a co-editor of *Robot Ethics* (MIT Press) and *Robot Ethics 2.0* (OUP) as well as author/contributor to numerous other books, journal articles, and funded reports.

James Canton, PhD, is a global futurist, social scientist, serial entrepreneur, and advisor to corporations and governments. For over 30 years he has been forecasting global trends, risks, and game changing innovations.

He is the CEO of the **Institute for Global Futures**, the Institute for Global Futures, a leading think tank that he founded in 1990. He has advised three White House Administrations and over 100 companies including the US Department of Defence (DoD), National Science Foundation and MIT's Media Lab, Europe on future trends.

Previously, he worked at Apple, and was a US policy advisor, investment banker, and founder of five tech companies. He is the author of *Future Smart*, *The Extreme Future*, and *Technofutures*.

William D. Casebeer, PhD, MA, is Senior Director of Human-Machine Systems at Scientific Systems Company, Inc. Bill was the Director of the **Innovation Lab at Beyond Conflict**, and was the Senior Research Area Manager in Human Systems and Autonomy for Lockheed Martin's Advanced Technology Laboratories, where he led technology development programs to boost the ability of humans and autonomous systems to work together. Bill served as a Program Manager at the Defense Advanced Research Projects Agency from 2010–2014 in the Defense Sciences Office and in the Biological Technologies Office. He retired from active Air Force duty as a Lieutenant Colonel and intelligence analyst in August 2011 and is a 1991 graduate of the USAF Academy.

Thomas C. Choinski, PhD, **Naval Undersea Warfare Center**, has over 40 years of experience encompassing innovation, management, and engineering that has led to an interdisciplinary approach for technological innovation. Tom has published or presented more than 70 papers in journals or through symposia on

topics including innovation, autonomy, unmanned systems, wargaming, digital signal processing, and microwave design. He holds graduate degrees in business and engineering. Dr. Choinski completed a PhD in humanities (concentration in technology, science, and society), as well as a fellowship through the MIT Seminar XXI Program in National Security Studies.

Timothy J. Demy, PhD, ThD, ThM, MSt, MA, is Professor of Military Ethics at the **US Naval War College**, Newport, RI. Previously, he served for 27 years as an officer in the US Navy. He earned the ThM and ThD from Dallas Theological Seminary, and the PhD from Salve Regina University. Additionally, among other degrees, he earned the MA from the Naval War College and the MSt from the University of Cambridge. He is the author and editor of numerous articles, books, and encyclopedias on a variety of historical, ethical, and theological subjects.

James Giordano, PhD, is Professor in the Departments of Neurology and Biochemistry, Chief of the Neuroethics Studies Program, Chair of the Subprogram in Military Medical Ethics, and Co-director of the O'Neill-Pellegrino Program in Brain Sciences and Global Law and Policy at Georgetown University Medical Center, Washington, DC.

He currently chairs the Neuroethics Subprogram of the IEEE Brain Initiative; is Research Fellow in Biosecurity, Technology, and Ethics at the US Naval War College; Advisory Fellow of the Defense Operations Cognitive Science section, SMA Branch, Joint Staff, Pentagon; Bioethicist for the Defense Medical Ethics Committee; and is senior appointed member of the Neuroethics, Legal and Social Issues Advisory Panel of the Defense Advanced Research Projects Agency (DARPA). The author of over 300 papers, 7 books, 21 book chapters, and 20 government white papers on brain science, national defense and ethics, in recognition of his achievements he was elected to the European Academy of Science and Arts, and named an Overseas Fellow of the Royal Society of Medicine (UK).

Casey Thomas Hart, PhD, is an Ontologist at Cycorp, where he teaches AI what it needs to know to reason about the world. He earned his doctorate in philosophy from the University of Wisconsin-Madison, where he specialized in formal epistemology and the philosophy of science. He lives in Austin, TX. He is inspired by his family: his tireless and wonderful wife Nicole and their two adorable daughters, Juliette and Elizabeth.

Pauline Shanks Kaurin, PhD, is a Professor of Military Ethics at the **US Naval War College**, Newport, RI. She earned her doctorate in Philosophy at Temple University and is a specialist in military ethics and Just War theory, the philosophy of law and applied ethics. Recent publications include: *When Less is not-More: Expanding the Combatant/Non-Combatant Distinction*; *With Fear and Trembling: A Qualified Defense of Non-Lethal Weapons* and *Achilles Goes Asymmetrical: The Warrior, Military Ethics and Contemporary Warfare* (Routledge 2014). She served as a Featured Contributor for *The Strategy Bridge*. Her new book on Obedience will be published by US Naval Institute Press in Spring

2020. She has also published with *Clear Defense*, *The Wavell Room*, *Newsweek* and *Just Security*.

Gina Granados Palmer, MLA, is a faculty member at the **US Naval War College**, Newport, RI. Ms. Palmer received a Master of Liberal Arts degree in International Relations from Harvard University's Division of Continuing Education and a BS in Mechanical Engineering from California Polytechnic State University, CA. She is currently completing her doctoral dissertation on literary and visual representations of war termination in the Pacific Theater at the end of World War II. She is focusing her doctoral research on leadership, ethics, technology, war and the balance between diplomacy and defense at Salve Regina University, Newport, RI.

James Peltz, PhD, is a program manager with the US Government. He is also a graduate of the **US Naval War College**. He has a decade of experience managing government research portfolios in the field of nuclear science, nuclear energy, and nuclear non-proliferation. He has specific experience and scientific expertise in predictive best estimate analysis of engineering systems to include model verification, validation, and uncertainty quantification. James has published several refereed articles and has given several invited presentations on these topics to domestic and international audiences.

Imre Porkoláb, PhD, earned his post-graduate degrees at military and civil universities in Hungary and the United States, including Harvard and Stanford. He is a highly decorated military professional with operational tours in Iraq and Afghanistan. He has also played a crucial role in the development of the Hungarian Special Operational Forces (SOF) capabilities. From 2011 he served in the US, at the NATO Allied Command Transformation, as Supreme Allied Commander Transformation (SACT) Representative to the Pentagon. Since 2018, he has been directing the transformation work on the area of the HDF's innovation, and building the national defence industrial base.

He is an expert in guerrilla and counterterrorism warfare, and his research areas include unconventional leadership, change management in a VUCA environment, innovative methods of organizational transformation, and the applicability thereof in the business world. He is an accomplished international speaker, and writer. His first book titled *Szolgálj, hogy vezethess!* was published in 2016; his second book, *A stratégia művészete*, came out in 2019.

John R. Shook, PhD, teaches philosophy at Bowie State University in Maryland, and Georgetown University in Washington DC. He also teaches research ethics and science education for the University at Buffalo's online Science and the Public EdM program. He has been a visiting fellow at the Institute for Philosophy and Public Policy at George Mason University in Virginia, and the Center for Neurotechnology Studies of the Potomac Institute for Public Policy in Virginia. At Georgetown University, he works with James Giordano of the Pellegrino Center for Clinical Bioethics. Shook's research encompasses philosophy of science, pragmatism, philosophical psychology, neurophilosophy, social neuroscience,

moral psychology, neuroethics, and science-religion dialogue. He co-edited *Neuroscience, Neurophilosophy, and Pragmatism* (2014), and *American Philosophy and the Brain: Pragmatist Neurophilosophy, Old and New* (2014). His articles have appeared in *Cortex*, *Neuroethics*, *AJOB-Neuroscience*, *Cambridge Quarterly of Health Care Ethics*, *Philosophy*, *Ethics*, and *Humanities in Medicine*, and *Journal of Cognition and Neuroethics*.

Tibor Solymosi, PhD, teaches philosophy at Westminster College in New Wilmington, Pennsylvania. He has previously taught at Allegheny College, Bowie State University, Mercyhurst University, and Case Western Reserve University. His research focuses on the consequences of the sciences of life and mind on our self-conception as conscious, free, and morally responsible selves. He is co-editor of *Pragmatist Neurophilosophy* (Bloomsbury), and *Neuroscience, Neurophilosophy and Pragmatism* (Palgrave Macmillan). He is currently working on the intersection of neuroscience and democratic culture, specifically regarding the effects of social media, digital devices, big data, and artificial intelligence.

Anita C. Street, MS, is a Technical Advisor with the US Government. She has 30 years experience working in the area of strategic foresight, environmental science, emerging technologies, and national security. She has edited and co-authored a number of publications on nanotechnology and clean water applications, Life Cycle Analysis of emerging technologies, peak phosphorus, and the influence of science fiction on research and development of converging technologies.

List of Contributors

Keith A. Abney, MA	California Polytechnic State University, USA
James Canton, PhD	Institute for Global Futures, USA
William D. Casebeer, PhD, MA	Scientific Systems Company, Inc., USA
Thomas C. Choinski, PhD	Naval Undersea Warfare Center, USA
Timothy J. Demy, PhD, ThD, ThM, MSt, MA	US Naval War College, USA
James Giordano, PhD, MPhil	Georgetown University Medical Center, USA
Casey Thomas Hart, PhD	Cycorp, USA
Pauline Shanks Kaurin, PhD	US Naval War College, USA
Yvonne R. Masakowski, PhD, MPhil, MA	US Naval War College, USA
Gina Granados Palmer, MLA	US Naval War College, USA
James Peltz, PhD	Department of Energy, USA
Imre Porkoláb, PhD	Hungarian Defence Forces, Hungary
John R. Shook, PhD	University at Buffalo, NY, USA
Tibor Solymosi, PhD	Westminster College, USA
Anita C. Street, MS	US Government, USA

This page intentionally left blank

Preface

All Warfare is Based on Deception

–Sun Tzu.

The arms race is on and Artificial Intelligence (AI) is the fast track for twenty-first century global dominance. Nations view AI technologies as a force enabler and the key to achieving global dominance. During the twenty-first century, AI technologies will control information, people, commerce and future warfare. It is our responsibility to be at the helm and shape our future as AI joins the fight.

(Masakowski, 2019)

This book had its origins in hours of discussion between the author and her students, colleagues, fellow scientists, and engineers on the important role of Artificial Intelligence (AI) in shaping the future of society and warfare. The topic of Artificial Intelligence is one that lends itself to lively debate as the technology itself has advanced exponentially, often times being overpromised and under-delivered. Indeed, there is a wide array of perspectives on this topic as some view AI as the great problem solver, while others as a threat to humanity itself. I contend that there is a bit of truth in both perspectives. We are facing an unknown entity in many ways. Foremost among these issues is whether AI technologies will achieve total self-awareness and become a serious threat to humanity. For the moment, we can rest assured that there will be a human-in-the-loop and human-on-the-loop to ensure that AI systems do not present dangers to the human (Porat, Oran-Gilad, Rottem-Hovev, & Silbiger, 2016). However, there are serious considerations regarding the ethical, theological, and moral challenges these technologies present to us during times of war. War itself is debated within the context of Just War theories. So, for this purpose, how will AI technologies influence the rules of engagement and Just War practices of warfare in the future? Should AI systems be designed with ethical rules and algorithms that will constrain its actions and serve as its conscience in future conflicts?

In the course of researching and writing this book, I've discussed these topics with my colleagues and invited them to contribute their expertise and knowledge, as well as speculative theories for future warfare in light of advances in AI technologies. We also need to consider the impact of advanced AI systems

fighting against AI systems in the future? How will AI technologies reset the rules of engagement for future warfare? What are the potential ethical and moral implications of such a future war?

Futurizing warfare is a risky business as we can wargame future concepts however these are often limited by our unique personal experience and knowledge. We need to step out of our comfort zone and imagine a world without ethical and moral boundaries for that is what our adversaries will do. They will not be contained or constrained by such limitations.

This book will address questions related to the influence and impact of Artificial Intelligence technologies being applied across a wide array of crises and domains as well as address the ethical and moral conflicts of war. Among the questions these chapters will explore are: What are the implications of AI for the individual's personal freedom, identity, and privacy rights? What are the consequences of AI advances related to national and global security? Is there a need to develop an AI conscience? What are the potential impacts of AI to AI system warfare? Each chapter will examine the perspectives and consequences for the integration of AI in our daily lives, as well as its influence on society and war. There are considerable consequences for underestimating the potential impacts of AI in warfare. Sun Tzu would have fully appreciated the potential benefits of AI as a tool of deception, as he stated, "The supreme **Art of War** is to subdue the enemy without fighting."

We anticipate that AI will continue to evolve and expand its reach on a global scale. Whatever its course, advances in AI will present challenges and risks for its implementation in daily life, as well as in times of war. It is left to the human to chart a course that will help mankind navigate unknown territory and shape the future world in which we want to live.

Acknowledgments

My long-standing interest in research and the topics of neuroscience, brain development, and cognitive psychology has afforded me the opportunity to work with a number of outstanding individuals across civilian and military communities. I believe that our thinking is a tapestry woven throughout the course of our lives shaped by our education, experience, knowledge, and insights gained through research and dialogue with others. I am indebted to those friends, colleagues, mentors, and students with whom I have engaged and learned from over the years. Indeed, they are far too numerous to mention here. However, I would like to share the following acknowledgments with you regarding those who contributed to making this book a reality.

Please allow me to acknowledge the contributions of my contributing authors for sharing their knowledge, expertise, and perspectives on Artificial Intelligence. Special thanks to Dr. Timothy Demy for his encouragement in my research, teaching, and writing. Special acknowledgment to my friend and colleague, Dr. William Bundy who recently passed away. Dr. Bundy was a champion for all of us who reached out to the future to anticipate how technology would change our lives and warfare. He was a friend, teacher, and mentor to many students and colleagues as he led the Gravely Group at the US Naval War College.

I am especially grateful to my US Naval War College, Ethics and Emerging Military Technology (EEMT) graduate students for the hours spent discussing, brainstorming, speculating, and imagining a future with ubiquitous Artificial Intelligence shaping and controlling our future lives and warfare.

Special thanks to my editors at Emerald Publishing for their patience, support, and continuous encouragement. This book is evidence of their commitment to excellence in their work and publishing.

This page intentionally left blank

Chapter 1

Artificial Intelligence and the Future Global Security Environment

Yvonne R. Masakowski

Abstract

Advances in Artificial Intelligence (AI) technologies and Autonomous Unmanned Vehicles are shaping our daily lives, society, and will continue to transform how we will fight future wars. Advances in AI technologies have fueled an explosion of interest in the military and political domain. As AI technologies evolve, there will be increased reliance on these systems to maintain global security. For the individual and society, AI presents challenges related to surveillance, personal freedom, and privacy. For the military, we will need to exploit advances in AI technologies to support the warfighter and ensure global security. The integration of AI technologies in the battlespace presents advantages, costs, and risks in the future battlespace. This chapter will examine the issues related to advances in AI technologies, as we examine the benefits, costs, and risks associated with integrating AI and autonomous systems in society and in the future battlespace.

Keywords: Artificial intelligence; future; autonomous; unmanned; decision-making; modeling; deep learning; military; strategy; tactics

The world is very different now. For man holds in his mortal hands the power to abolish all forms of human poverty and all forms of human life. –John Fitzgerald Kennedy.

Introduction

The next world war will not be focused on who fired the first shot. Rather, future warfare will be focused on the control and dissemination of information across all domains, including information about everything and everyone! AI networks will

serve as the grid and blueprint of the new battlespace of the twenty-first century. Becoming the leader in Artificial Intelligence (AI) is the key to achieving global dominance. Nations will use AI technological superiority to shape the geopolitical, social, and economic environment to their nation's strategic advantage. Nations will integrate AI technologies and networks across a wide spectrum of applications to expand and enhance their economic, geopolitical, and military agendas. Advances in AI will influence every phase of humanity and daily life, thereby impacting the individual, society, and shaping the battlespace of war.

As nations strive to address each of these global challenges, they seek to identify tools and technologies that will support them in their decisions during times of crises across a range of domains. We see AI being used today during the Global Pandemic in the development of models and surveillance systems to monitor people's movements and travel patterns on a local and global level. Nations require information management tools that help to sort through the elements of crisis management, such as logistics, personnel management, supply chains, the distribution of goods, and technologies for maintaining regional security (Hamel & Green, 2007). Each of these topics requires a means of managing vast amounts of data and indeed, AI technologies excel at Big Data management (ICO, 2017). Advances in AI technologies will support both government and nongovernment agencies such as the United Nations and the International Committee of the Red Cross, to prepare and manage crises as they emerge. The United States, NATO, and its allied partners have identified AI technologies as critical for ensuring technological superiority and achieving the military strategic advantage (US Department of Defense, 2019; Masakowski, 2019d).

AI affords the military and nongovernment agencies the means of managing and analyzing large data sets and supporting decision-making at all levels (Tegmark, 2018). Indeed, there is a great deal of enthusiasm for the development of AI-enabled technologies to improve daily life and enhance warfare. AI technologies serve as a force multiplier for the military as it can streamline the information pipeline, analyze data, and accelerate the decision cycle. However, we contend that it is essential to keep the human-in-the-loop as they alone have the ability to understand context and integrate the nuances of contextual information across a wide domain of contributing factors that the AI system has yet to master (e.g., culture, organizational hierarchy, etc.).

AI technologies, to some extent, have been overpromised and underdelivered as people become excited about its capabilities and often misunderstand the complexities and limitations of AI systems. Simply stated, you can't buy a pound of AI and insert it like plaster in a crack in the wall. You have to first understand the problem and related issues within the context of the situation itself. This requires knowledge and understanding of the situation in which you want to deploy AI as part of a network, part of the organization, or merely augment a human decision-maker's thinking. One of the principal advantages for the military is to develop adaptive and agile AI networks that will facilitate information management during times of crises.

Distributed sensors collecting information across all domains including air, land, sea, undersea, and in space will be analyzed and managed by integrated and

distributed AI networks. Satellites will be linked as information nodes within the grid of AI networks emanating across all domains and at all levels to capture data and attempt to make sense of it all. AI is the key to achieving global dominance for all nations seeking to control information across all domains to their strategic advantage! China and Russia have provided evidence for this objective in their national strategic strategies.

China has put its stake in the ground stating that it aims to be the global leader of AI technologies by 2030 and is well on its way to make good with its claim (Allen, 2019; Chan & Lee, 2018; China State Council, 2017; Dai & Shen, 2018). China has invested heavily in AI technologies for numerous applications, from facial recognition for identity management, population control, resource management (i.e., water, minerals, materials, etc.) to manufacturing applications. China has provided further evidence of the potential impact of AI technologies on society and global security.

Likewise, Russia has invested in AI to shape their global political and strategic objectives. Their nation is investing in AI to weaponize information to their political and strategic advantage. Regardless of our personal or political views, the fact is that AI technologies have facilitated new, advanced capabilities. The question is: What type of future do we want to create? How can democratic nations use AI technologies to ensure global security?

Advances in AI technologies will provide a means of safeguarding a stable environment in which the national security strategy, productivity, and economic progress is ensured. Indeed, national strategies are designed to ensure economic and geopolitical stability. In the book, *Future Smart*, we are advised about game-changing trends that will shape the future of business and warfare. (Canton, 2015). Canton highlights the similarities between current advances in AI technologies with those innovations and inventions of the Industrial Revolution. He posits that AI will influence and accelerate the development of AI technologies across a wide range of domains including medicine, manufacturing, and warfighting (Canton, 2015). He further hypothesizes that the impact of AI will be further accelerated by the integration of quantum computing, as well as advances in batteries, and materials. One can extrapolate from this hypothesis that the integration of AI advances with new materials, batteries, and computing power will only expand and enhance its capabilities. Time to decide and act will grow shorter with each advance! Each advance in AI technology and computing power increases the level of risk in global security as advances will present new and unanticipated challenges to maintain global security.

China is aware of these benefits and has already integrated AI technologies in the design of what they call, *Intelligentization* of design (Zhou, 2013). Shifting from innovation to intelligentization refers to the fact that new systems and technologies being designed will be integrated with a level of intelligence that will make them safer, more reliable, self-sustaining, and just plain smarter than previously thought. For example, the design of a locomotive that has been integrated with AI intelligence affords it increased capabilities of being self-aware, self-learning, self-maintaining, and ensures network connectivity and communication that makes the locomotive safer, more reliable, and cost-

effective. Like the Industrial Revolution, we anticipate that intelligitized systems will continue to expand and contribute to a network of self-sustaining, automated systems capable of manufacturing a host of products, technologies, systems, and tools of war.

We recognize that AI is having an impact on society, politics, economics, and gains in manufacturing capabilities. Advances in AI are also having significant effects on the battlespace and twenty-first century warfare. AI networks have accelerated the decision cycle for the warfighter and for the adversary. AI networks and intelligent agents can quickly detect, collect and analyze data to inform decisions and make recommendations for the benefit of the decision maker. However, these same capabilities may also prove to be a weapon in the hands of the adversary. The real advantage democratic nations have is its people. From the American Revolution through the Space race, the human spirit has launched mankind into new territories. This time is no different. Humans have a pioneering spirit and adapt quickly to change. This is such a time that calls for adaptation and innovation.

For the twenty-first century is a time rife with opportunity, complexity, and uncertainty. We must acknowledge that global security rests not on an individual nation but requires all nations to consider working together collaboratively to achieve a sense of collective security for all its members. There are challenges and concerns regarding trusting the source of data and determining whether the information received is trustworthy. It is essential that democratic nations work together to ensure that trust and truth are the essential ingredients of AI networks and systems to ensure global security. Indeed, nations must reckon with issues related to national sovereignty that, up until now, prohibited them from sharing historical database and information that is proprietary. However, if we are to ensure global security; then, nations must work collaboratively and cooperatively to achieve unity of effort to ensure the security of our world. There will be a trade space in which nations must contribute to the greater good of maintaining global situation awareness (GSA) if they are to ensure global security. “Those who would give up essential Liberty, to purchase a little temporary Safety deserve neither Liberty nor Safety” (Franklin, 1776).

Advances in AI present a paradigm shift for nations to be assured of controlling their national security agenda. Nations must collectively defend against future adversaries as their collective security to safeguard their individual national security agendas will depend upon it. The responsibility for ensuring and safeguarding national agendas will necessarily be a collective venture between nations across the private and public sectors. This collective investment is due to the tremendous investment it will take to ensure that nations have AI systems in place that can detect behaviors, if not anticipate, adversarial intent before negative events occur! Anticipatory and predictive AI networks and agents must be developed if we are to be agile and adaptive in this new complex and uncertain global security environment.

AI networks facilitate cyberwarfare and the weaponization and manipulation of information presenting cyber threats that raise serious challenges and concerns for ensuring global and national security. The question is: How will AI be used to

shape future governments and future generations? How will we defend our nation in the cyberspace of the future to secure global security? For now, we are at the intersection of innovation, intelligentization, and an evolution and revolution of AI networks and system designs that present opportunities and challenges, each of which may have grave consequences for mankind. It is apparent to some of us that corporate and government defense organizations must work together if we are to be successful in ensuring a secure future for all.

Future AI networks and systems will be used to shape the global security landscape. Indeed, AI dominance will ensure a nation's global geopolitical and economic dominance as they attain control of the information environment and its resources across all domains, air, land, sea, undersea, and most especially, space. China and Russia recognize the military gain in this regard. There is no time to waste for nations including NATO and its Allied partners to invest in AI technologies as a means of ensuring global security.

If nations (NATO, Allied partners, etc.) are to remain adaptive and agile, we must develop AI systems that are anticipative and predictive. Future AI situational awareness (SA) systems will play a pivotal role in providing nations with the decision advantage. We no longer will have the luxury of time. It took approximately 22 minutes to rally a military response to 911 attacks. Today, we have less time to respond and far less time to understand the complexities of the situation. AI technology and networks can reduce the time and accelerate the decision cycle to ensure global security.

Investment in AI technologies will provide the military strategic advantage that is essential for global security. Intuitive AI systems, designed with adaptive neural networks and machine learning algorithms, will detect intent and forecast events in the future. Automated bots, adaptive computer algorithms, and smart systems will transform business and warfare. Disseminated sensors, embedded from sea floor to satellites in space, will facilitate global situational awareness (GSA) with predictive capabilities. AI technological superiority will support nations who collaborate and cooperate with each other to ensure global security. This will take the political will of those leaders who wish to gain the strategic advantage and those who make decisions regarding sharing of national information to achieve a common understanding of a complex and uncertain environment.

Today's operational environment has become more complex as a result of advances in AI, and AI-enabled technologies such as robotics and Autonomous Unmanned Vehicles (AUVs) and systems. Indeed, the character of warfare has been transformed by the emergence and utilization of AI networks and unmanned autonomous systems including AUVs and Unmanned Underwater Vehicle (UUV) systems. These AI-enabled system designs have expanded our SA in the battlespace with extensive networks of sensors from sea floor to space satellites. The information garnered from these distributed sensor networks has been collated and analyzed by AI networks to facilitate more effective mission planning and execution (Finney & Klug, 2016). However, these systems have yet to be challenged strategically by adversaries equipped with similar capabilities. That day will come. Consideration has been given to the potential impact of AI

technologies in urban warfare and one can only hope that it doesn't come to that to experience such a reality.

Advanced AI technologies are considered critical components for gaining the military decision advantage by our global competitors such as China, Russia, and North Korea. Each of these nations has also developed strategic doctrine on AI technologies and how they intend to invest in their future development for maintaining global military dominance.

Advances in AI and computing power will continue to increase system capabilities and contribute to the complexity of the operational environment. It is a propitious time to consider the effects of AI technology within the context of future global security. As nations compete to be the global leader in AI technologies, the security of the world is in play and at risk.

AI networks of the future must be designed to ensure global security for adversarial nations seeking global dominance will exploit every vulnerability to their strategic and economic, geopolitical advantage. Nations must work collaboratively to develop the AI technologies necessary to ensure global security. Global security with AI networks and systems must be a strategic imperative!

Innovation and Advances in AI

There have been significant advances in AI technologies as evidenced by the wide array of systems developed by the commercial marketplace. From smart phones to digital cities, we have only begun to see the potential for the integration of AI technologies in our lives (Masakowski, Smythe, & Creely, 2016). We anticipate that advances in AI technologies and tools will expand and infiltrate every aspect of life. Just as the telephone, radio, rail, and the airplane emerged and influenced society during the Industrial Revolution, so too, AI technologies will reshape twenty-first century society and warfare.

Such technological changes will be both evolutionary and revolutionary. Evolutionary in that AI technologies will continue to modify our behaviors and the way that we live and conduct daily life. Whether we are booking a flight, traveling from one city to another, get stuck in traffic, or look for a restaurant in a new city, we check our AI-enabled smart phone to help guide our decision-making. The military uses AI technologies to collect and manage sensor data, gain SA, and conduct Intelligence Preparation of the Battlespace (IPB) which are essential elements for ensuring mission success.

We are sitting at the precipice of great changes in society and in our lives. The arms race is on for global dominance (Masakowski, 2019a, 2019b). AI is the fast track to the future where nations will compete to be the leader in AI as a step toward controlling global commerce and warfare.

As nations and society integrate AI advances to improve the quality of daily life, such changes will also become integrated in the future battlespace. As advances in AI technologies continue to evolve, we anticipate that the revolution in warfare has only just begun (Geissler, 2019). Specifically, advances in AI-enabled technology will shape the roles and responsibilities for individuals,

society, and the military (O'Flanagan, 2018). We must acknowledge that as AI technologies advance and become integrated in society, the military will seek to exploit such advances to their strategic advantage (Masakowski, 2019c). Once turned on, these capabilities will not be turned off.

We anticipate that AI technologies will reshape the battlespace similar to what occurred as a result of the development of the long bow, tank, radar, airplane, and the aircraft carrier. Regardless of its era, each technological advance was a game-changer on the battlefield that revolutionized warfare for its time. However, unlike the long bow, whose use was confined to the battlefield, AI technologies will not be confined nor constrained. Advances in AI technologies will extend beyond the battlespace and reach into our homes and personal lives.

Today, the commercial community is redesigning the environment with digital cities, energy grid management systems, AI networked air traffic control systems, and integrated networks that link individuals, cities, and governments. For the military, this constellation of AI networks presents opportunities for nations and adversaries to manage information and exploit the AI network to their tactical and strategic advantage.

I would argue that the blueprint design of digital cities may be readily converted to the command and control grid for future warfare. The integrated network designed to manage a city's infrastructure may also be seconded and repurposed for warfare by our adversaries. There are grave implications for global security when thinking about the ways in which such AI networks can be used in the future. Foremost among these is the issue of managing crises and conducting warfare in urban regions, a topic that has been and will continue to be explored (Geissler, 2019).

The future operational environment extending from 2020 to 2050 and beyond will continue to be dynamic and challenging with increased complexity and uncertainty. We must take time to consider how these changes will affect future warfighting. Nations must develop doctrine, policies, and warfighting rules of engagement, as well as legal and ethical practices that will integrate AI systems into the network of mission plans as a critical step for ensuring their nation's security. One of the principal questions my students raised in this regard has been: Will I be court martialed if I don't listen to the AI system recommendations and follow them? As well as, Will I be court martialed if I listen to the AI system recommendations and they are wrong? There are serious ethical considerations for military leaders and warfighters that must be addressed by policymakers.

Technology in and of itself is not the principal issue. Rather, there are considerable ethical and moral consequences related to the implementation and integration of advanced AI systems for society and warfare (Geissler, 2019; O'Flanagan, 2018; Peltz, 2017). We must remain vigilant and perspicacious regarding advances in AI technologies as these will provide capabilities to the military as well as to our adversaries. We must anticipate and war game worst-case scenarios and the potential for adversaries to use such technological advances as weapons against society (Ashrafian, 2015a; 2015b; Bostrom, 2014).

Civilian and Military Applications: Shaping Expectations

As a society, we have already become somewhat accustomed to advances in artificial intelligence technology. We have a set of expectations regarding the capabilities of such technologies at our fingertips. We Google our questions, searching for answers and trusting that the information provided to us is accurate. Regardless of our search engines, we anticipate that these tools will help us find the answer to our question. We implicitly trust that the information will be reliable. Our expectations have been shaped by our interactions with these AI networks.

We have adapted to this new world environment where our perceptions are shaped by the news media. This sense of trust that we have acquired based on our interactions with AI systems have set the stage for shaping our societal and political perspectives as well. Recent revelations regarding the Russian intrusion into our last presidential election has shown that AI facilitates our adversaries' ability to shape our nation's politics. We have come to accept cameras and surveillance systems monitoring our decisions and movements. Alexa placed in our homes, provides a means of monitoring our thoughts, social interactions and political perspectives.

We have unwittingly invited personal surveillance into our homes as an accepted part of the twenty-first century norm. We have abdicated our personal privacy rights as part of this process. We anticipate that surveillance systems will continue to monitor and mold every facet of our lives, including national economic and political agendas. As AI systems become more integrated in each city's infrastructure, we anticipate that events will be monitored continuously on a local and global level. Monitoring unwitting civilians has far-reaching ethical consequences for society as it violates individual privacy rights and intellectual freedoms (Geissler, 2019; Masakowski et al., 2016; Peltz, 2017). Therefore, attention must be paid to the level of intrusiveness and control that AI technologies will be allowed to exert on the civilian population. We must align our system designs with the values and ethics of the society in which they will function.

From an individual perspective, members of society will be presented with privacy challenges that will affect every aspect of their personal lives, their jobs, housing, education, associations, friendships, and political views. From a national perspective, nations will shape and control their citizens' perceptions. Private citizens will be monitored in their home and workplace. Friendships and associations will be scrutinized by AI systems that collect data to ensure that individuals are aligned with government policies as a means of ensuring stability within a region. It really is all about control of information, people, and warfare. However, there are consequences for this approach. According to Geissler (2019):

This *Orwellian* capability creates a one-sided *Panopticon*, leaving the targeted population paralyzed and without privacy. Being left with little choice to fight back, distrust and fear will disrupt the informal life and damage the social fabric.