Hastings Science and Technology Law Journal

Volume 11
Number 1 *Winter 2020*

Article 5

Winter 2020

Applied Artificial Intelligence in Modern Warfare and National Security Policy

Brian Seamus Haney

Recommended Citation
Brian Seamus Haney, *Applied Artificial Intelligence in Modern Warfare and National Security Policy*, 11 HASTINGS SCI. & TECH. L.J. 61 (2020).
Available at: https://repository.uchastings.edu/hastings_science_technology_law_journal/vol11/iss1/5

Applied Artificial Intelligence in Modern Warfare and National Security Policy

BRIAN SEAMUS HANEY[1]

Abstract

Artificial Intelligence (AI) applications in modern warfare have revolutionized national security power dynamics between the United States, China, Russia, and the private industry. The United States has fallen behind in military technologies and is now at the mercy of big technology companies to maintain peace. After committing $150 billion toward the goal of becoming the AI technology world leader, China claimed success in 2018. In 2019, Chinese researchers published open-source code for AI missile systems controlled by deep reinforcement learning algorithms. Further, Russia's continued interference in United States' elections has largely been driven by AI applications in cybersecurity. Yet, despite outspending Russia and China combined on defense, the United States is failing to keep pace with foreign adversaries in the AI arms race.

Previous legal scholarship dismisses AI militarization as futuristic science-fiction, accepting without support the United States' prominence as the world leader in military technology. This inter-disciplinary article provides three main contributions to legal scholarship. First, this is the first piece in legal scholarship to take an informatics-based approach toward analyzing the range of AI applications in modern warfare. Second, this is the first piece in legal scholarship to take an informatics-based approach in analyzing national security policy. Third, this is the first piece to explore the complex power and security dynamics between the United States, China, Russia, and private corporations in the AI arms race. Ultimately, a new era of advanced weaponry is developing, and the United States Government is sitting on the sidelines.

1. J.D. Notre Dame Law School 2018, B.A. Washington & Jefferson College 2015. Special thanks to Richard Susskind, Margaret Cuonzo, Max Tegmark, Ethem Alpaydin, Sam Altman, Josh Achiam, Volodymyr Mnih & Angela Elias.

Introduction

Cyberwarfare continues on a daily basis, with the United States under constant attack.[2] Threats of nuclear missile strikes from adversaries appear in daily headlines.[3] Today, Artificial Intelligence (AI) is the United States' most powerful weapon for defense.[4] Yet, in AI development, the United States is falling behind adversaries like China and Russia.[5] In 2017, China committed $150 billion toward becoming the world leader in AI, claiming success the next year.[6] Interference in U.S. elections is largely being driven by substantial Russian investments in AI cybersecurity applications.[7] All the while, the United States Government and Department of Defense remain at the mercy of big technology companies like Google and Microsoft to ensure advancements in AI research and development.[8]

The Law of Accelerating Returns ("LOAR") states that fundamental measures of information technology follow predictable and exponential trajectories.[9] Indeed, information technologies build on themselves in an exponential manner.[10] Applied to AI, the LOAR provides strong support

2. James Kadtke & , John Wharton, *Technology and National Security: The United States at a Critical Crossroads*, DEFENSE HORIZONS 84, National Defense University 1 (March 2018).

3. Hyung-Jin Kim, *North Korea Confirms Second 2nd Test of a Multiple Rocket Launcher*, MILITARY TIMES (Sept. 11, 2019), https://www.militarytimes.com/flashpoints/2019/09/11/north-korea-confirms-2nd-test-of-multiple-rocket-launcher/; *see also* https://time.com/5673813/north-korea-confirms-second-rocket-launcher-test/. *See also* Nasser Karimi &, John Gambrell, *Iran Uuses Advanced Centrifuges, Threatens Higher Enrichment*, ASSOCIATED PRESS (Sept. 7, 2019), https://www.apnews.com/7e896f8a1b0c40769b54ed4f98a0f5e6.

4. Karl ManheimKarl Manheim & Lyric Kaplan, Artificial Intelligence: Risks to Privacy and Democracy, 21 YALE J.L. & TECH. 106, 108 (2019); *see also* User Clip: Elon Musk at the National Governors Association 2017 Summer Meeting, C-SPAN (July 15, 2017) https://www.c-span.org/video/?c4676772/elon-musk-national-governors-association-2017-summer-meeting & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J.L. & TECH. 106, 108 (2019); *see also* User Clip: *Elon Musk at the National Governors Association 2017 Summer Meeting*, C-SPAN (July 15, 2017) https://www.c-span.org/video/?c4676772/elon-musk-national-governors-association-2017-summer-meeting.

5. Kadtke & Wharton, *supra* note 2, at 1.

6. Gregory C. Allen, *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security*, Center for a New American Security 9 (2019).

7. KELLEY M. SAYLER, CONG. RESEARCH SERV., R45178, ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY 24 (2019).

8. Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Challenges, Competencies, and Strategies*, 29 HARV. J.L. & TECH. 353, 354 (2016).

9. RAY KURZWEIL, HOW TO CREATE A MIND 250 (2012).

10. *Id.* at 251-55.

for AI's increasing role in protecting the national defense.[11] Indeed, similar to the way in which aviation and nuclear weapons transformed the military landscape in the twentieth century, AI is reconstructing the fundamental nature of military technologies today.[12]

Yet legal scholars continue to deny and ignore AI's applications as a weapon of mass destruction. For example, in a recent MIT Starr Forum Report, the Honorable James E. Baker, former Chief Judge of the United States Court of Appeals for the Armed Forces, argues "we really won't need to worry about the long-term existential risks."[13] And, University of Washington Law Professor, Ryan Calo argues, regulators should not be distracted by claims of an "AI Apocalypse" and to focus their efforts on "more immediate harms."[14] All the while, private corporations are pouring billions into AI research, development, and deployment.[15] In a 2019 interview, Paul M. Nakasone, The Director of the National Security Agency (NSA) stated, "I suspect that AI will play a future role in helping us discern vulnerabilities quicker and allow us to focus on options that will have a higher likelihood of success."[16] Yet, Elon Musk argues today, "[t]he biggest risk that we face as a civilization is artificial intelligence."[17] The variance in the position of industry leaders relating to AI and defense demonstrates a glaring disconnect and information gap between legal scholars, government leaders, and the private industry.

The purpose of this Article is to aid in closing the information gap by explaining the applications of AI in modern warfare. Further, this article contributes the first informatics-based analysis of the national security policy landscape. This article proceeds in three parts: Part I explains the state-of-the-art in AI technology; Part II explores three national security threats resulting from AI applications in modern warfare; and Part III discusses national security policy relating to AI from international and domestic perspectives.

11. NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES 94 (2017).

12. Honorable James E. Baker, *Artificial Intelligence and National Security Law: A Dangerous Nonchalance*, STARR FORUM REPORT 1 (2018).

13. *Id*. at 5.

14. Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 431 (2017).

15. Andrew Thompson, *The Committee on Foreign Investment in The United States: An Analysis of the Foreign Investment Risk Review Modernization Act of 2018*, 19 J. HIGH TECH. L. 361, 363 (2019).

16. *An Interview with Paul M. Nakasone*, 92 JOINT FORCE Q. 1, 9 (2019).

17. *User Clip: Elon Musk at the National Governors Association 2017 Summer Meeting*, C-SPAN (July 15, 2017) https://www.c-span.org/video/?c4676772/elon-musk-natio nal-governors-association-2017-summer-meeting.

I. Artificial Intelligence

Contemporary scholars have presented several different definitions of AI. For example, MIT Professor Max Tegmark concisely defines intelligence as the ability to achieve goals[18] and AI as "non-biological intelligence."[19] Additionally, according to Stanford Professor Nils Nilsson AI is "concerned with intelligent behavior in artifacts."[20] A recent One Hundred Years Study defines AI as, "a science and a set of computational technologies that are inspired by—but typically operate quite differently from—the ways people use their nervous systems and bodies to sense, learn, reason, and take action."[21] For the purposes of this paper AI is any system replicating the thoughtful processes associated with human thought.[22] Advancements in AI technologies continue at alarming rates.[23] This Part proceeds by discussing three types of AI systems commonly used in the context of national security: deep learning, reinforcement learning, and deep reinforcement learning.

A. Deep Learning

Deep learning is a process by which neural networks learn from large amounts of data.[24] Defined, data is any recorded information about the world.[25] In deep learning, the idea is to learn feature levels of increasing abstraction with minimum human contribution.[26] The models inspiring current deep learning architectures have been around since the 1950s.[27] Indeed, the Perceptron, which serves as the basic tool of neural networks was proposed by Frank Rosenblatt in 1957.[28] However, artificial intelligence research remained relatively unprosperous until the dawn of

18. MAX TEGMARK, LIFE 3.0 BEING HUMAN IN THE AGE OF ARTIFICIAL INTELLIGENCE 50 (2017).

19. *Id.* at 39.

20. NILS J. NILSSON, ARTIFICIAL INTELLIGENCE: A NEW SYNTHESIS 1 (1998).

21. Stan. U., Artificial Intelligence and Life in 2030, One Hundred Year Study on Artificial Intelligence, 1 (2016).

22. Brian S. Haney, *The Perils and Promises of Artificial General Intelligence*, 45 J. LEGIS. 151, 152 (2018).

23. PAUL E. CERUZZI, COMPUTING A CONCISE HISTORY 114 (2012).

24. Haney, *supra* note 22, at 157.

25. ETHEM ALPAYDIN, *MACHINE LEARNING: THE NEW AI* 3 (2016). *See also* MICHAEL BUCKLAND, INFORMATION AND SOCIETY 21-22 (2017) (discussing definitions of information).

26. JOHN D. KELLEHER, BRENDEN TIERNEY, DATA SCIENCE 134 (2018).

27. SEBASTIAN RASCHKA & VAHID MIRJALILI, PYTHON MACHINE LEARNING 18 (2017).

28. *Id*.

the internet.[29] Generally, deep learning systems are developed in four parts: data pre-processing, model design, training, and testing.

Deep learning is all about the data.[30] Every two days humans create more data than the total amount of data created from the dawn of humanity until 2003.[31] Indeed, the internet is the driving force behind modern deep learning strategies because the internet has enabled humanity to organize and aggregate massive amounts of data.[32] According to machine learning scholar, Ethem Alpaydin, it's the data that drives the operation, not human programmers.[33] The majority of the time spent with deep learning system development is during the pre-processing stage.[34] During this initial phase, machine learning researchers gather, organize, and aggregate data to be analyzed by neural networks.[35]

The types of data neural networks process vary.[36] For example, in autonomous warfare systems, images stored as pixel values are associated with object classification for targeting.[37] Another example is gaining political insight with a dataset of publicly available personal data on foreign officials. How the data is organized largely depends on the goal of the deep learning system.[38] If a system is being developed for predictive purposes the data may be labeled with positive and negative instances of an occurrence.[39] Or, if the system is being learned to gain insight, the data may remain unstructured, allowing the model to complete the organization task.[40]

A deep learning system's model is the part of the system which analyzes the information.[41] Most commonly the model is a neural network.[42] Neural networks serve the function of associating information to

29. PETER J. DENNING & MATTI TEDRE, COMPUTATIONAL THINKING 93 (2019).

30. David Lehr & Paul Ohm, *Playing with The Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653, 668 (2017).

31. RICHARD SUSSKIND, TOMORROW'S LAWYERS 11 (2nd ed. 2017).

32. ALPAYDIN, *supra* note 25, at 10-11.

33. *Id.* at 12.

34. KELLEHER & TIERNEY, *supra* note 26, at 97.

35. *Id*.

36. *Id.* at 101.

37. Symposium, A Framework Using Machine Vision and Deep Reinforcement Learning for Self-Learning Moving Objects in a Virtual Environment, AAAI 2017 Fall Symposium Series (2017), https://aaai.org/ocs/index.php/FSS/FSS17/paper/view/16003/15319.pdf.

38. Michael Simon, et al., *Lola v. Skadden and the Automation of the Legal Profession*, 20 YALE J.L. & TECH 254, 300 (2018).

39. Tariq Rashid, MAKE YOUR OWN NEURAL NETWORK 13 (2018).

40. Alpaydin, *supra* note 25, at 111.

41. Kelleher & Tierney, *supra* note 26, at 121.

42. Tegmark, *supra* note 18, at 76.

derive knowledge.[43] Neural networks models are based on the biological neo-cortex.[44] Indeed, the human brain is composed of processing units called neurons.[45] Each neuron in the brain is connected to other neurons through structures called synapses.[46] A biological neuron consists of dendrites—receivers of various electrical impulses from other neurons—that are gathered in the cell body of a neuron.[47] Once the neuron's cell body has collected enough electrical energy to exceed a threshold amount, the neuron transmits an electrical charge to other neurons in the brain through synapses.[48] This transfer of information in the biological brain provides the foundation on which modern neural networks are modeled and operate.[49]

Every neural network has an input layer and an output layer.[50] However, in between the input and output layer, neural networks contain multiple hidden layers of connected neurons.[51] In a neural network, the neurons are connected by weight coefficients modeling the strength of synapses in the biological brain.[52] The depth of the network is in large part a description of the number of hidden layers.[53] Deep Neural Networks start from raw input and then each hidden layer combines the values in its preceding layer and learns more complicated functions of the input.[54] The mathematics of the network transferring information from input to output varies, but is generally matrix mathematics and vector calculus.[55] During training, the model processes data from input to output, often described as the feedforward portion.[56] The output of the model is typically a prediction.[57] For example, whether an object is the correct target, or the wrong target would be calculated with a convolutional neural network

43. Alpaydin, *supra* note 25, at 106-107.
44. Michael Simon, et al., *supra* note 38, 254.
45. Moheb Costandi, NEUROPLASTICITY 6 (2016).
46. *Id*. at 9.
47. *Id*. at 7.
48. Raschka & Mirjalili, *supra* note 27, at 18.
49. Haney, *supra* note 22 at 158.
50. Kurzweil, *supra* note 9, at 132.
51. Alpaydin, *supra* note 25, at 100.
52. *Id.* at 88.
53. Tegmark, *supra* note 18, at 76.
54. Alpaydin, *supra* note 25, at 104.
55. Manon Legrand, Deep Reinforcement Learning for Autonomous Vehicle Control Among Human Drivers, at 23 (academic year 2016–17) (unpublished C.S. thesis, Université Libre de Bruxelles), https://ai.vub.ac.be/sites/default/files/thesis_legrand.pdf.
56. Eugene Charniak, INTRODUCTION TO DEEP LEARNING 10 (2018).
57. Harry Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87, 90 (2014).

(CNN).[58] The function of the CNN is in essence a classification task, where the CNN classifies objects or areas based upon their similarity.[59] CNNs are the main model used for deep learning in computer vision tasks.[60]

However, the learning occurs during the backpropagation process.[61] Backpropagation describes the way which neural networks are trained to derive meaning from data.[62] Generally, the mathematics of the backpropagation algorithm includes partial derivative calculations and a loss function to be minimized.[63] The algorithm's essential function adjusts the weights of a neural network to reduce error.[64] The algorithm's ultimate goal is the convergence of an optimal network, but probabilistic maximization also provides state-of-the-art performance in real world domains.[65] Dynamic feedback allows derivative calculations supporting error minimization.[66] One popular algorithm for backpropagation is stochastic gradient descent (SGD), iteratively updates the weights of the network according to a loss function.[67]

After the training process the model is then tested on new data, and if successful, deployed for the purpose deriving knowledge from information.[68] The process of deriving knowledge from information is commonly accomplished with feature extraction.[69] Feature extraction is a method of dimensionality reduction allowing raw inputs to convert to an output revealing abstract relationships among data.[70] Neural networks extract these abstract relationships by combining previous input information in higher dimensional space as the network iterates.[71] In other words, deep neural networks learn more complicated functions of their initial input when each hidden layer combines the values of the preceding

58. Daniel Maturana & Sebastian Scherer, 3D Convolutional Neural Networks for Landing Zone Detection from LiDar, 2 (2015), https://ieeexplore.ieee.org/document/7139679.

59. Rashid, *supra* note 39, at 159.

60. Legrand, *supra* note 55, at 23.

61. Kelleher & Tierney, *supra* note 26, at 130.

62. Alpaydin, *supra* note 25, at 100.

63. Paul John Werbos, THE ROOTS OF BACKPROPAGATION FROM ORDERED DERIVATIVES TO NEURAL NETWORKS AND POLITICAL FORECASTING 269 (1994).

64. Alpaydin, *supra* note 25, at 89.

65. Kelleher & Tierney, *supra* note 26, at 131.

66. Werbos, *supra* note 63, at 72.

67. Steven M Bellovin, et al., *Privacy and Synthetic Datasets*, 22 STAN. TECH. L. REV. 1, 29 (2019).

68. Alpaydin, *supra* note 25, at 106-107.

69. *Id.* at 89.

70. *Id.* at 102.

71. Kelleher & Tierney, *supra* note 26, at 135.

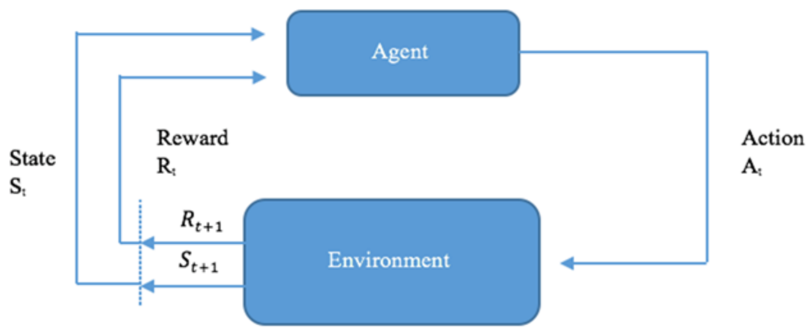
layer.[72] In addition to deep learning, reinforcement learning is also a major cause of concern for purposes of national security policy.

B. Reinforcement Learning

At its core, reinforcement learning is an optimization algorithm.[73] In short, reinforcement learning is a type of machine learning concerned with learning how an agent should behave in an environment to maximize a reward.[74] Agents are the software programs making intelligent decisions.[75] Generally, reinforcement learning algorithms contain three elements:

Model: the description of the agent-environment relationship;
Policy: the way in which the agent makes decisions; and
Reward: the agent's goal.[76]

The fundamental reinforcement learning model is the Markov Decision Process (MDP).[77] The MDP model was developed by the Russian Mathematician Andrey Markov in 1913.[78] Interestingly, Markov's work over a century ago remains the state-of-the-art in AI today.[79] The model below describes the agent-environment interaction in an MDP:[80]



72. ALPAYDIN, *supra* note 25, at 104.

73. Volodymyr Mnih et al., Human-Level Control Through Deep Reinforcement Learning, 518 NATURE INT'L J. SCI. 529, 529 (2015).

74. ALPAYDIN, *supra* note 25, at 127.

75. RICHARD S. SUTTON, ANDREW G. BARTO, REINFORCEMENT LEARNING: AN INTRODUCTION 3 (The MIT Press eds., 2nd ed. 2017).

76. Katerina Fragkiadaki, Deep Q Learning, Carnegie Mellon Computer Science, CMU 10703 (Fall 2018), https://www.cs.cmu.edu/~katef/DeepRLFall2018/lecture_DQL_kate f2018.pdf.

77. Haney, *supra* note 22 at 161.

78. Gely P. Basharin, et al, *The Life and Work of A.A. Markov*, 386 Linear Algebra and its Applications, 4, 15 (2004).

79. GEORGE GILDER, LIFE AFTER GOOGLE 75 (2018).

80. SUTTON & BARTO, *supra* note 75, at 38. (model created by author based on illustration at the preceding citation).

The environment is made up of states for each point in time in which the environment exists.[81] The learning begins when the agent takes an initial action selected from the first state in the environment.[82] Once the agent selects an action, the environment returns a reward and the next state.[83] Generally, the goal for the agent is to interact with its environment according to an optimal policy.[84]

The second element of the reinforcement learning framework is the policy. A policy is the way in which an agent makes decisions or chooses actions within a state.[85] In other words, the agent chooses which action to take when presented with a state based upon the agent's policy.[86] For example, a greedy person has a policy that routinely guides their decision making toward acquiring the most wealth. The goal of the policy is to allow the agent to advance through the environment so as to maximize a reward.[87]

The third element of the reinforcement learning framework is the reward. Ultimately, the purpose of reinforcement learning is to maximize an agent's reward.[88] However, the reward itself may is defined by the designer of the algorithm. For each action the agent takes in the environment, a reward is returned.[89] There are various ways of defining reward, based upon the specific application.[90] But generally, the reward is associated with the final goal of the agent.[91] For example, in a trading algorithm, the reward is money.[92] In sum, the goal of reinforcement learning is to learn good policies for sequential decision problems by optimizing a cumulative future reward.[93] Interestingly, many thinkers throughout history have argued the human mind is itself a reinforcement learning system.[94] Furthermore, reinforcement learning algorithms add

81. ALPAYDIN, *supra* note 25, at 126-127.
82. SUTTON, BARTO, *supra* note 75, at 2.
83. MYKEL J. KOCHENDERFER, DECISION MAKING UNDER UNCERTAINTY 77 (2015).
84. *Id.* at 79.
85. *Id.*
86. SUTTON & BARTO, *supra* note 75, at 39.
87. WERBOS, *supra* note 63, at 311.
88. SUTTON & BARTO, *supra* note 75, at 7.
89. KOCHENDERFER, *supra* note 83, at 77.
90. BOSTROM, *supra* note 11, at 239.
91. MAXIM LAPAN, DEEP REINFORCEMENT LEARNING HANDS-ON 3 (2018).
92. *Id.* at 217.
93. Hado van Hasselt, Arthur Guez, & David Silver, *Deep Reinforcement Learning with Q-Learning*, Google DeepMind, 2094 (2018), https://arxiv.org/abs/1509.06461.
94. WERBOS, *supra* note 63, at 307.

substantial improvements to deep learning models, especially when the two models are combined.[95]

C. Deep Reinforcement Learning

Deep Reinforcement Learning is an intelligence technique combining deep learning and reinforcement learning principles. Max Tegmark suggests that deep reinforcement learning was developed by Google in 2015.[96] However, earlier scholarship explores and explains the integration of neural networks in the reinforcement learning paradigm.[97] Arguably, deep reinforcement learning is a method of general intelligence because of its theoretic capability to solve any continuous control task.[98] For example, deep reinforcement learning algorithms drive state-of-the-art autonomous vehicles.[99] However, it shows poorer performance on other types of tasks like writing, because mastery of human language is—for now—not describable as a continuous control problem.[100] Regardless of its scalable nature toward general intelligence, deep reinforcement learning is a powerful type of artificial intelligence.[101] Generally, there are three different frameworks for deep reinforcement learning: action-value, policy gradient, and actor-critic.[102]

An example of an action-value based framework for a deep reinforcement learning algorithm is the Deep Q-Network (DQN).[103] The DQN algorithm is a type of model-free-learning.[104] In model-free-learning, there isn't a formal description of the agent-environment relationship.[105] Instead, the agent randomly explores the environment, gathering information about the environment's states, actions, and rewards.[106] The algorithm stores the information in memory, called experience.[107]

95. ALPAYDIN, *supra* note 25, at 136.
96. TEGMARK, *supra* note 18, at 85.
97. WERBOS, *supra* note 63, at 307.
98. TEGMARK, *supra* note 18, at 39.
99. Alex Kendall, et al., *Learning to Drive in A Day* (2018), https://arxiv.org/abs/1807.00412.
100. NOAM CHOMSKY, SYNTACTIC STRUCTURES 17 (1957).
101. TEGMARK, *supra* note 18, at 39.
102. Shixun You, et al., *Deep Reinforcement Learning for Target Searching in Cognitive Electronic Warfare*, IEEE Access Vol. 7, 37432, 37438 (2019).
103. Mnih, et al., *supra* note 73, at 529.
104. KOCHENDERFER, *supra* note 83, at 122.
105. *Id.* at 121.
106. LAPAN, *supra* note 91, at 127.
107. CHARNIAK, *supra* note 56, at 133.

The DQN algorithm develops an optimal policy π^* for an agent with a Q-learning algorithm.[108] The optimal policy is the best method of decision making for an agent with the goal of maximizing reward.[109] The Q-learning algorithm maximizes a Q-function: $\mathrm{Q}(s, a)$, where s is the state of an environment and a is an action in the state.[110] In essence, by applying the optimal Q-function Q^* to every state-action pair (s, a) in an environment, the agent is acting according to the optimal policy.[111] However, computing $\mathrm{Q}(s, a)$ for each state-action pair in the environment is computationally expensive.[112]

Instead, the DQN algorithm approximates the value of each state state-action pair:[113]

$$Q(s, a; \phi) \approx (s, a).$$

Here, ϕ represents the function parameters, which are the function's variables.[114] The parameters are determined by a neural network using experience replay.[115] Experience replay refers to the agent's experiences stored in memory, which are used to train the neural network to approximate the value of state-action pairs.[116] The neural network iterates until the convergence of the Q-function as determined by the Bellman Equation:[117]

$$Q^*(s, a) = \mathbb{E}_{s' \sim \varepsilon}\left[r + \gamma \max_{a'} Q^*(s', a') | s, a\right].$$

Here, $\mathbb{E}_{s' \sim \varepsilon}$ refers to the expectation for all states, r is the reward, γ is a discount factor typically defined $0 < \gamma < 1$, allowing present rewards to have higher value.[118] Additionally, the max function describes an action at which the Q-function takes its maximal value for each state-action pair.[119] In other words, the Bellman Equation does two things; it defines the

108. Mnih, et al., *supra* note 73, at 529.
109. KOCHENDERFER, *supra* note 83, at 80-81.
110. Volodymyr Mnih, Koray Kavukcuoglu, Methods and Apparatus for Reinforcement Learning, U.S. Patent Application No. 14/097,862 at 5 (filed Dec. 5, 2013), https://patents.google.com/patent/US20150100530A1/en.
111. LAPAN, *supra* note 91, at 144.
112. Mnih & Kavukcuoglu, *supra* note 110, at 5.
113. *Id*.
114. *Id.*
115. CHARNIAK, *supra* note 56, at 133.
116. *Id.*
117. Haney, *supra* note 22, at 162.
118. KOCHENDERFER, *supra* note 83, at 78.
119. Brian S. Haney, *The Optimal Agent: The Future of Autonomous Vehicles & Liability Theory*, 29 ALB. L.J. SCI. & TECH. (forthcoming 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3261275.

optimal Q-function and allows the agent to consider the reward from its present state as greater relative to similar rewards in future states.[120]
Thus, the DQN algorithm combines Q-learning with a neural network to maximize reward.[121] After the optimal policy is defined according to:

$$\pi^* = Q^*(s', a'),$$

the agent engages in the exploitation of its environment.[122] During the exploitation phase, the agent maximizes its reward by making decisions according to the optimal policy.[123] The DQN is an off-policy algorithm, meaning it uses data to optimize performance.[124] Indeed, DQN is essentially a reinforcement learning algorithm, where the agent uses a neural network to decide which actions to take.

A second variant of deep reinforcement learning is the Proximal Policy Optimization ("PPO") algorithm, a gradient technique.[125] Similar to the DQN algorithm, the PPO algorithm is a method of model-free learning.[126] In contrast to the DQN algorithm, PPO is an on-policy algorithm, meaning it does not learn from old data and instead directly optimize policy performance.[127] One advantage of the PPO model is that it can be used for environments with either discrete or continuous action spaces.[128]

In general, PPO works by computing an estimator of the policy gradient and iterating with a stochastic gradient optimization algorithm.[129] In other words, the algorithm continuously updates the agent's policy based on the old policy's performance.[130] The PPO update algorithm may be defined:[131]

$$\theta_{k+1} = \arg\max_{\theta} \mathbb{E}_{s,a\sim\pi_{\theta_k}} \left[L(s, a, \theta_k, \theta)\right].$$

120. LAPAN, *supra* note 91, at 102-03.

121. WERBOS, *supra* note 63, at 306-07.

122. LAPAN, *supra* note 91, at 127.

123. *Id.*

124. Hado van Hasselt, Arthur Guez, and David Silver, *Deep Reinforcement Learning with Q-Learning*, PROCEEDINGS OF THE THIRTIETH ASS'N FOR THE ADVANCEMENT OF ARTIFICIAL INTELLIGENCE CONF. ON ARTIFICIAL INTELLIGENCE, 2098 (2016), https://www.aaai.org/ocs/index.php/AAAI/AAAI16/paper/download/12389/11847.

125. John Schulman, et al., *High-Dimensional Continuous Control Using Generalized Advantage Estimation*, INT'L CONF. ON LEARNING REPRESENTATIONS (2016), https://arxiv.org/abs/1506.02438.

126. CHARNIAK, *supra* note 56, at 124.

127. OpenAI, Proximal Policy Optimization, OpenAI Spinning UP (2018), https://spinningup.openai.com/en/latest/algorithms/ppo.html.

128. *Id*.

129. John Schulman, et al., *Proximal Policy Optimization Algorithms*, OpenAI at 2 (2017), https://arxiv.org/abs/1707.06347.

130. KOCHENDERFER, *supra* note 83, at 80.

131. Proximal Policy Optimization, *supra* note 127.

Here, $L(s, a, \theta_k, \theta\,)$ is the objective function, θ are the policy parameters, θ_k are the policy parameters for k experiment.[132] Generally, the PPO update is a method of incremental improvement for a policy's expected return.[133] Essentially, the algorithm takes multiple steps via SGD to maximize the objective.[134]

The PPO algorithm's key to the success is obtaining good estimates of an advantage function.[135] The advantage function describes the advantage of a particular policy relative to another policy.[136] For example, if the advantage for the state-action pair is positive, the objective reduces to:[137]

$$L(s, a, \theta_k, \theta) = min\left(\frac{\pi_\theta(a|s)}{\pi_{\theta_k}(a|s)}, (1+\epsilon)\right)A^{\pi_{\theta_k}}(s, a).$$

Here, $A^{\pi_{\theta_k}}$ is the advantage estimate for the policy given parameters $\pi_\theta(a|s)$, and the hyperparameter ϵ corresponds to how far away the new policy can step from the old while still profiting the objective.[138] Where the advantage is positive the objective increases and the min function puts a limit to how much the objective can increase.[139]

The limitation on the objective increase is called clipping.[140] The algorithm's goal is to make the largest possible improvement on a policy, without stepping so far as to cause performance collapse.[141] To achieve this goal, PPO relies on clipping the objective function to remove incentives for the new policy to step far from the old policy.[142] In essence, the clipping serves as a regularizer, minimizing incentives for the policy to change dramatically.[143]

A third variant of Deep Reinforcement Learning and an example of the actor-critic framework is the Deep Deterministic Policy Gradient ("DDPG") algorithm.[144] Like both DQN and PPO, DDPG is a model-free

132. *Id*.
133. Schulman, et al., *supra* note 129, at 2.
134. LAPAN, *supra* note 91, at 427.
135. *See* Schulman, et al., *supra* note 125.
136. *See* Proximal Policy Optimization, *supra* note 127.
137. *Id*.
138. LAPAN, *supra* note 91, at 432.
139. *See* Proximal Policy Optimization, *supra* note 127.
140. Schulman, et al., *supra* note 129, at 3.
141. Proximal Policy Optimization, *supra* note 127.
142. Schulman, et al., *supra* note 129, at 3.
143. Proximal Policy Optimization, *supra* note 127.
144. LAPAN, *supra* note 91, at 410.

learning method.[145] However, unlike PPO, DDPG is only applicable in continuous action spaces.[146] In form DDPG is relatively similar to DQN.[147] DDPG is an off-policy algorithm, meaning it re-uses old data.[148] In short, DDPG is a method of deep reinforcement learning using two function approximators, an actor and a critic.[149]

The critic estimates the optimal action-value function $a^*(s)$.[150] Generally, the action-value function is tailored to continuous action spaces, defined:

$$a^*(s) = arg \max_a Q^*(s, a).$$

Here, the optimal action $a^*(s)$ is defined as a value of $Q^*(s, a)$ at which a takes its optimal value according to the Bellman Equation.[151] The critic's role is to minimize loss, typically using a means squared error function, or target network, which gives consistent target values.[152] The input of the target network is derived from a replay buffer, utilizing experience replay similar to the DQN algorithm.[153] As the process occurs, the actor is iteratively updated accordingly.[154] To learn the optimal policy the DDPG learns a deterministic policy $\pi_\theta(s)$ which gives the action maximizing $Q_\phi(s, a)$:[155]

$$\max_\theta \mathbb{E}_{s \sim \mathcal{D}}\left[Q_\phi\left(s, \pi_\theta(s)\right)\right].$$

Here, the Q-function parameters Q_ϕ are constants and $s \sim \mathcal{D}$ is the state sampled from the replay buffer.[156]

Ultimately, the actor decides which action to take.[157] But, to optimize an agent's reward, after each action, the critic tells the actor and

145. Timothy P. Lillicrap, et al., *Continuous Control with Deep Reinforcement Learning*, 1 (2016), https://arxiv.org/abs/1509.02971.

146. OpenAI, *Deep Deterministic Policy Gradient*, OpenAI Spinning UP (2018), https://spinningup.openai.com/en/latest/algorithms/ddpg.html.

147. Lillicrap et al., *supra* note 145, at 1.

148. Aprit Agarwal, Katharina Muelling, Katerina Fragkiadaki, *Model Learning for Look-ahead Exploration in Continuous Control*, Cornell University (Nov. 20, 2018), https://arxiv.org/abs/1811.08086.

149. Alex Kendall et al., *Learning to Drive in A Day*, Cornell University (Sept. 11, 2018), https://arxiv.org/abs/1807.00412.

150. OpenAI, *supra* note 146.

151. *Id*.

152. Lillicrap et al., *supra* note 145, at 2.

153. Charniak, *supra* note 56, at 133.

154. David Silver et al., *Deterministic Policy Gradient Algorithms*, Deem Mind Technologies (2014), http://proceedings.mlr.press/v32/silver14.pdf.

155. OpenAI, *Deep Deterministic Policy Gradient*, *supra* note 146.

156. OpenAI, *Deep Deterministic Policy Gradient*, *supra* note 146.

157. CHARNIAK, *supra* note 56, at 130.

defines necessary adjustment for performance improvement.[158] The DDPG algorithm shows promise in continuous control tasks, for robotics control systems.[159] For example, DDPG has shown state-of-the-art success for driving cars.[160] However, the off-policy nature of the algorithm makes it much slower because it takes more computational power to train compared to the PPO and other on-policy algorithms. As computational hardware develops, quantum computers provide a faster method of computing than classical methods.[161]

In sum, deep learning, reinforcement learning, and deep reinforcement learning provide a framework for analyzing the state-of-the-art in AI technology. While the mathematical models underlying these systems are not new, their capabilities have shown rapid improvement symbiotically with the massive amount of information humans began collecting at the dawn of the digital age.[162] Most importantly, modern AI systems are capable of generalizing information to make predictions and achieve goals.[163] As a result, these systems are transforming the foundations of the defense industry, national security, and global warfare.

II. Security Threats

United States National Defense Strategy prioritizes competition with China and Russia.[164] Currently, among these three countries, there is an on-going arms race toward developing the most powerful AI systems.[165] Some hope this continued escalation can be avoided.[166] However, the incentives associated with becoming the world leader in AI technology are great, while the harms of nations falling behind could surely be fatal.[167] Thus, the AI arms races will certainly continue.

---

158. Aleksandra Faust et al., *PRM-RL: Long-range Robotic Navigation Tasks by Combining Reinforcement Learning and Sampling-based Planning* (2018) https://arxiv.org/abs/1710.03937v2.

159. *Id*.

160. Alex Kendall et al., *Learning to Drive in A Day* (2018), https://arxiv.org/abs/1807.00412.

161. Jacob Biamonte et al., *Quantum Machine Learning* at 2 (2018) https://arxiv.org/abs/1611.09347.

162. GILDER, *supra* note 79, at 75; *see also* SUSSKIND, *supra* note 31, at 11.

163. TEGMARK, *supra* note 18, at 85-86.

164. Mark D. Miles & Charles R. Miller, *Global Risks and Opportunities the Great Power Competition Paradigm*, JFQ 94 3rd Quarter, at 80 (2019).

165. An Interview with Paul M. Nakasone, National Defense University Press, JFQ 92, 1st Quarter, at 5 (2019).

166. Baker, *supra* note 12, at 5.

167. BOSTROM, *supra* note 11, at 96-97.

Northwestern Law Professor, John McGinnis, argues, "[t]he way to think about the effects of AI on war is to think of the consequences of substituting technologically advanced robots for humans on the battlefield."[168] However, this mode of thought completely fails to communicate AI security threats. Indeed, today the battlefield is everywhere, and the United States is bombarded with cyber-attacks every day.[169] McGinnis further argues, "The existential dread of machines that become uncontrollable by humans and the political anxiety about machines' destructive power on a revolutionized battlefield are overblown."[170] Yet, China has developed and made publicly available state-of-the-art AI guided missile technology and computer programs.[171] And, Russia routinely and intentionally manipulates United States voters on social media for the purposes of influencing political elections.[172] In short, AI is the most important weapon in modern warfare, primarily in the defense, and national security sectors. The following sections will discuss AI applications of three types of security threats: missile attack, cyber-attack, and general intelligence.

A. Missiles

Richmond School of Law Professor and Member of the Center for New American Security's Task Force on Artificial Intelligence and National Security, Rebecca Crootof, suggests weapons may be grouped into three categories: inert, semi-autonomous, and autonomous.[173] Inert weapons require human operation to be lethal, such as, stones, knives, or handheld firearms.[174] Semi-autonomous weapon systems have autonomous capabilities in functions relevant to target selection and engagement, but the system cannot both select and engage targets independently.[175] Third, autonomous weapon systems are capable of independently selecting and engaging targets based on conclusions derived from gathered information and preprogramed constraints.[176]

168. John O. McGinnis, *Accelerating AI*, 104 NW. U. L. REV. 1253, 1266 (2010).

169. John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 398 (2016).

170. McGinnis, *supra* note 168, at 1254.

171. Shixun You, et al., *supra* note 102, at 37447.

172. U.S. Department of Justice, Report on The Investigation into Russian Interference in the 2016 Presidential Election, Vol I at 4 (March 2019), https://www.justice.gov/storage/report_volume1.pdf.

173. Rebecca Crootof, Autonomous Weapons Systems and the Limits of Analogy, 9 HARV. NAT'L SEC. J. 51, 59 (2018).

174. *Id.*

175. *Id.*

176. *Id.*

Professor Crootof argues, "autonomous weapon systems in use today act in largely predictable ways."[177] Similarly, The Honorable James E. Baker, argues that autonomous weapon systems are nothing new.[178] Judge Baker claims autonomous weapons have been standard military technology since the 1970s, and the United States reserves the technology for defensive purposes.[179] Further, according to the Department of Defense, "[p]otential adversaries are also developing an increasingly diverse, expansive, and modern range of offensive missile systems that can threaten U.S. forces abroad."[180] However, these perspectives sincerely underestimate the capabilities modern missile systems, particularly in light of AI advancements.[181] Inarguably, AI has changed the role of robotics control systems in warfare.[182]

It is important to understand foreign adversaries have the ability to attack the United States homeland with AI controlled missile systems at such a scale to which the United States would be entirely unable to respond.[183] Indeed, in a recent study funded by the National Natural Science Foundation of China, *Deep Reinforcement Learning for Target Searching in Cognitive Electronic Warfare* (China AI Missile Study), researchers demonstrate Chinese capabilities in deep reinforcement learning control systems for missile control.[184] The United States funded similar research through the Naval Post-Graduate School in a 2017 report, *A Framework Using Machine Vision and Deep Reinforcement Learning for Self-Learning Moving Objects in a Virtual Environment* (Navy AI Study).[185] However, the Chinese research is not only far more advanced, but also open-sourced.[186] Indeed, China's system is adaptable to any environment or target across the globe.[187] And, the code for China's deep reinforcement learning missile control systems is available on GitHub.[188]

177. *Id*. at 60.
178. Baker, *supra* note 12, at 3.
179. *Id*.
180. Department of Defense, Missile Defense Review, Executive Summary III (2009), https://www.defense.gov/Portals/1/Interactive/2018/11-2019-Missile-Defense-Review/The%202019%20MDR_Executive%20Summary.pdf.
181. Shixun You, et al., *supra* note 102, at 37447.
182. JOHN JORDAN, ROBOTS 133 (2016).
183. Shixun You, et al., *supra* note 102, at 37447.
184. *Id*. at 37434.
185. Richard Wu, et al., *supra* note 37.
186. Shixun You, et al., *supra* note 102, at 37435.
187. *Id*. at 37441.
188. youshixun, vCEW New model of cognitive electronic warfare with countermeasures, GitHub https://github.com/youshixun/vCEW (2019).

Further, Google's TensorFlow, is also available open-source and designed specifically for manufacturing and scalability.[189]

AI missile technology is comparatively simple relative to AI controlled vehicles or rocket boosters due to the general lack of obstacles in a missile's environment. Indeed, there are at most three elements needed to control an AI missile. First, a means of perception, which is commonly achieved with Light Detection and Ranging Device (LiDAR) sensors.[190] LiDAR sensors simply work by sending light pulses from a transmitter and measuring return times with a receiver.[191] The time it takes for a pulse to return measures distance according to $\frac{tc}{2} = d$, where t is travel time, c is the speed of light, and d is the distance between the LIDAR sensor and the object.[192] The receiver then generates a point cloud map of the environment for processing.[193]

Second, the processing typically occurs with convolutional neural networks (CNNs), which show state-of-the-art performance in computer vision tasks.[194] CNNs utilize convolutional mathematics to perform computer vision tasks like object detection and classification.[195] Further, CNNs are well suited for three-dimensional point cloud environments and integration with reinforcement learning algorithms.[196] One study, conducted by research firm OpenAI, demonstrated the effectiveness of CNNs in real-time obstacle detection when integrated with reinforcement learning systems.[197]

The third element is a method of optimization for decision making, commonly reinforcement learning.[198] For example, the China AI Missile Study explored the use of DQN, PPO, and DDPG for control in its

189. TensorFlow 2.0 Alpha is Available, TensorFlow, (2019), https://www.tensorflow.org/install.

190. Jeff Hecht, *Lidar for Self-Driving Cars*, OPTICS & PHOTONICS NEWS (Jan. 1, 2018), https://www.osa-opn.org/home/articles/volume_29/january_2018/features/lidar_for_self-driving_cars/.

191. Gaetan Pennecot et al., *Devices and Methods for a Rotating LIDAR Platform with Shared Transmit/Receive Path*, GOOGLE, INC., No: 13/971,606, (Aug. 20, 2013), https://patents.google.com/patent/US9285464B2/en.

192. Matthew J. McGill, *LIDAR Remote Sensing*, NASA Technical Reports Server (NTRS) (2002).

193. Maturana, Scherer, *supra* note 58, at 2.

194. *Id*.

195. Legrand, *supra* note 55, at 23.

196. Mnih et al., *supra* note 73, at 530.

197. Gregory Kahn, *Uncertainty-Aware Reinforcement Learning for Collision Avoidance* (2017).

198. Shixun You et al., *Completing Explorer Games with a Deep Reinforcement Learning Framework Based on Behavior Angle Navigation*, 8 ELECTRONICS 1,17 (2019).

simulated, real-time physics engine.[199] Additionally, the Navy AI Missile Study experimented with the DQN algorithm.[200] In the context of missile control, the reinforcement learning agent is able to visualize its environment with LiDAR and a CNN and generalize to avoid obstacles, including defense missiles.[201] This framework maximizes the probability of success in target searching, detection, and engagement regardless of motion dynamics.[202] As such, AI missile systems guided by LiDAR sensor data and controlled with deep reinforcement learning algorithms have the capability to attack any target on Earth, or in the atmosphere, with pixel precision.[203] Importantly, this information and the tools to build such a system are widely available on the internet.[204]

In short, Professor Crootof and Judge Baker's misunderstandings about the nature of autonomous weapons derive from their grouping of all autonomous weapons as having analogous abilities and posing analogous levels of threat.[205] Indeed, modern AI missile systems, specifically, deep reinforcement learning systems do not act in the same predictable ways as the autonomous missile systems of the 1970s.[206] In fact, they are much different than the autonomous weapons of the 1970s.[207] Critically, deep reinforcement learning missiles today are able to generalize about their environment, adapting, and evolving with the battlefield.[208] Specifically, Chinese AI missile technology "is enhanced by the powerful generalization ability of . . . deep convolutional neural network[s]."[209]

Indeed, according to the 2019 Department of Defense Missile Review, China now has the ability to threaten the United States with about 125 nuclear missiles.[210] The Review explains while the United States relies

199. Shixun You et al., *supra* note 102, at 37438.

200. Richard Wu et al., *supra* note 37, at 233.

201. Gregory Kahn et al., *Uncertainty-Aware Reinforcement Learning for Collision Avoidance* (2017).

202. Serena Yeung et al., *Every Moment Counts: Dense Detailed Labeling of Actions in Complex Videos*, 126 INT'L J. OF COMPUTER VISION 375, 376-378 (2017).

203. Shixun You et al., *supra* note 102, at 37438.

204. *See* Richard Wu et al., *supra* note 37; *see also* youshixun, *New model of cognitive electronic warfare with countermeasures*, GITHUB (2019) https://github.com/youshixun/vCEW; *Install TensorFlow 2*, TENSORFLOW (2019) https://www.tensorflow.org/install; Shixun You et al., *supra* note 102, at 37434-37447.

205. Crootof, *supra* note 173 at 59.

206. *Id*. at 60.

207. Baker, *supra* note 12, at 3; see also Shixun You, *Completing Explorer Games with a Deep Reinforcement Learning Framework Based on Behavior Angle Navigation*, 8 ELECTRONICS 1,17 (2019).

208. Richard Wu et al., *supra* note 37, at 231.

209. Shixun You et al., *supra* note 102, at 37438.

210. Office of the Secretary of Defense, *supra* note 180, at III.

on deterrence to protect against sophisticated actors like China, active U.S. missile defense efforts must outpace rogue offensive missile strikes.[211] But, despite massive over-spending, the United States Military is falling behind.[212] Further, due to the availability of AI missile system construction and control information across the internet, AI missile attacks are an immediate national security threat.[213] This is especially true considering hostile relationships with Iran, North Korea, and Middle Eastern militant organizations.[214] Intimately related to the applications of AI missiles in national security, the role of AI in cybersecurity attacks is also a cause for immediate concern.

B. Cybersecurity

Top U.S. national security officials believe that AI and machine learning will have transformative implications for cybersecurity and cyber war.[215] For example, according to National Security Agency (NSA) Director Paul M. Naksone, "As we look at near-peer competitors, China and Russia clearly are at the top of the list because they have the capacity to operate across the full spectrum of cyberspace operations."[216] However, Naksone seems to be behind the times in terms of AI military applications in cyberspace. Indeed, in a 2019 interview with National Defense University, Naksone stated, "I think that the early instantiation of AI will be on the defensive side."[217] Further, recent cybersecurity data and research provide strong evidence AI is already fueling offensive state sponsored cyber-attacks.

The Center for Strategic & International Studies (CSIS), a policy research organization, records reported significant cyber-attacks on governments, defense and high technology companies, or economic crimes

211. *Id*.

212. Craig Whitlock & Bob Woodward, *Pentagon buries evidence of $125 billion in bureaucratic waste*, WASH. POST (Dec. 5, 2016), https://www.washingtonpost.com/investigations/pentagon-buries-evidence-of-125-billion-in-bureaucratic-waste/2016/12/05/e0668c76-9af6-11e6-a0ed-ab0774c1eaa5_story.html; *see also* NATO, Defence Expenditure of NATO Countries (2012-2019), NATO (June 25, 2019), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/20190625_PR2019-069-EN.pdf.

213. *See* youshixun, *New model of cognitive electronic warfare with countermeasures*, GITHUB (2019), https://github.com/youshixun/vCEW; *see also Install TensorFlow 2*, TENSORFLOW (2019), https://www.tensorflow.org/install.

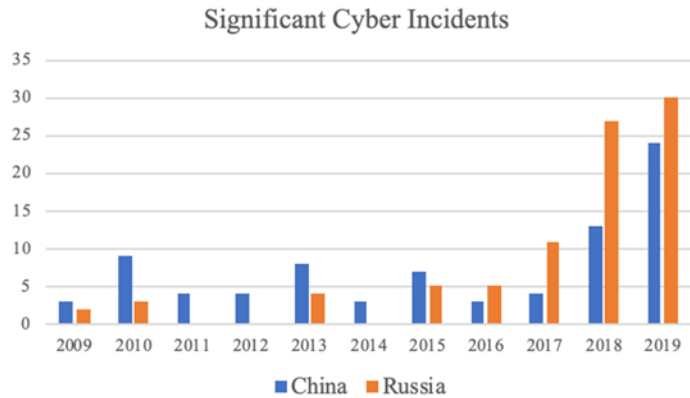
214. Office of the Secretary of Defense, *supra* note 180, at III-IV.

215. Greg Allen &Taniel Chan, *Artificial Intelligence and National Security*, HARV. KENNEDY SCH. BELFER CTR. FOR SCI. AND INT'L AFF. 1, 18 (2017).

216. An Interview with Paul M. Nakasone, National Defense University Press, JFQ 92, 1st Quarter, at 5 (2019).

217. *Id*. at 8.

in excess of a million dollars.[218] The table below illustrates the number of Chinese and Russian cyber-attacks per year.[219]



While the accelerating trend in cyber-attacks could be due to a number of factors, AI is unquestionably playing a contributing rule. Indeed, AI provides more powerful attack mechanisms which are widely available, making this trend likely to continue.[220]

Military defense and political hacking are now commonplace.[221] Some of the most significant defense and political related attacks reported by the CSIS include:[222]

1. *May 2019.* Hackers affiliated with the Chinese intelligence service reportedly had been using NSA hacking tools since 2016, more than a year before those tools were publicly leaked.
2. *March 2019.* U.S. officials reported that at least 27 universities in the U.S. had been targeted by Chinese hackers as part of a campaign to steal research on naval technologies.

218. Center for Strategic and International Studies, Significant Cyber Incidents (August 2019), https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

219. *See* Appendix B. Significant Cyber Incidents for chart data (Chart prepared by author with information from, Center for Strategic and International Studies, Significant Cyber Incidents (August 2019), https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

220. *See* Hyrum S. Anderson et al., *Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning*, Cornell University Library (2018), https://arxiv.org/abs/1801.08917; *see also* endgameinc, Malware Env for OpenAI Gym (2018), https://github.com/endgameinc/gym-malware.

221. Significant Cyber Incidents, CTR. FOR STRATEGIC AND INT'L STUD. (Aug. 2019), https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

222. *Id.*

3. *October 2018.* Media reports state than U.S. agencies warned President Trump that that China and Russia eavesdropped on call made from an unsecured phone.
4. *August 2018.* Microsoft announces that Russian hackers had targeted U.S. Senators and Center conservative think tanks critical of Russia.
5. *February 2016.* Hackers breached the U.S. Department of Justice's database, stealing and releasing the names, phone numbers, and email addresses or 30,000 DHS and FBI employees.
6. *October 2016.* The U.S. Director of National Intelligence and Department of Homeland Security jointly identified Russia as responsible for hacking the Democratic National Committee and using WikiLeaks to dump emails obtained in the hack.
7. *April 2015.* U.S. officials report that hackers gained access to White House networks and sensitive information, such as "real-time non-public details of the president's schedule," through the State Department's network, which has had continued trouble in ousting attackers.
8. *February 2012.* Media reports say that Chinese hackers stole classified information about the technologies onboard F-35 Joint Strike Fighters.[223]

The pervasive use of cyberspace for a variety of covert international operations provides support for the argument that an AI arms race is in full swing.[224] Indeed, AI provides a decisive advantage in the penetration and security of networks.[225] While it is difficult to know the specific architectures used, the wide-spread availability of AI cyber-attack research and code strongly suggests malicious AI software is already common-place.[226]

As the data reflects, cyber-dependent nations are vulnerable to political manipulation.[227] Indeed, politically motivated cyber-attacks are far

223. Significant Cyber Incidents, CTR. FOR STRATEGIC AND INT'L STUD. (Aug. 2019), https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents. (List derived from preceding source).

224. Ido Kilovaty, *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information*, 9 HARV. NAT'L SEC. J. 146, 150 (2018).

225. Alberto Perez Veiga, *Applications of Artificial Intelligence to Network Security*, 14 (2018), https://arxiv.org/abs/1803.09992.

226. Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, 34 (Cornell University Library 2018) https://arxiv.org/pdf/1802.07228.pdf; *see also* Anderson et al., *supra* note 220.

227. Kilovaty, *supra* note 224, at 150.

from a new phenomenon.[228] And, Russia has significantly expanded its budget in these areas over the last few years to sway public opinion around the world.[229] One direct example, includes the Internet Research Agency (IRA), a Russian intelligence company, and The Main Intelligence Directorate of the Russian Army's (GRU) hacking operations during the 2016 Presidential Election.[230] According to the Mueller Report, the IRA and GRU both engaged in hacking Democratic National Committee networks for the purpose of influencing the election's outcome.[231] Further, the *Mueller Report* details the IRA's social media tactics with the intent of swaying voters.[232] Another example refers to the Cambridge Analytica Scandal, where 87 million Facebook users had their personal data exposed without their consent and used by Cambridge Analytica to support political campaigns.[233] As a result, data driven AI cyber-tools for manipulating voters via social media are critical to the integrity of United States elections and thus, National Security.[234]

Unsurprisingly, AI research in cybersecurity is rapidly expanding. For example, one piece of scholarship specifically details guidelines for the development of malicious AI software.[235] The scholarship demonstrates the practical possibilities of developing malicious machine learning algorithms capable of harming humans.[236] Another paper, *Adversarial Reinforcement Learning in a Cyber Security Simulation*, introduces a game played between adversarial reinforcement learning systems: an attacker and a defender.[237] The paper illustrates a cyber security simulation with two Markov agents playing against each other as attacker and defender of a cyber network.[238] Drawing on this work, a third paper was introduced in 2019, *Deep Reinforcement Learning for Cyber Security*, which developed a similar simulation exploring the effectiveness of action-value, policy, and

228. WERBOS, *supra* note 63, at 184.

229. Kilovaty, *supra* note 224, at 158.

230. U.S. Department of Justice, *supra* note 172, at 4.

231. U.S. Department of Justice, *supra* note 172, at 4.

232. *Id*. at 14.

233. Felipe González et al., *Global Reactions to the Cambridge Analytica Scandal: An Inter-Language Social Media Study* (2019), https://faculty.washington.edu/aragon/pubs/LA_WEB_Paper.pdf.

234. Jon M. Garon, *Cyber-World War III: Origins*, 7 J.L. & CYBER WARFARE 1, 9 (2018).

235. Federico Pistono & Roman Yampolskiy, *Unethical Research: How to Create Malevolent Artificial Intelligence* (2016), https://arxiv.org/pdf/1605.02817.pdf.

236. *Id*.

237. Richard Elderman et al., *Adversarial Reinforcement Learning in a Cyber Security Simulation*, SCITEPRESS (2017), https://pdfs.semanticscholar.org/b495/7266c43f1c76ed8dbb275b8510f6fb1e063c.pdf.

238. *Id*. at 566.

actor-critic deep reinforcement learning models for network attack and defense.[239]

Interestingly, one paper, *Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning*, gives specific details regarding reinforcement learning malware models and provided an open-source code on GitHub.[240] The reinforcement learning model in the paper is an evasive malware variant, which can be effective on samples not used during training.[241] Samples are prime examples of malware detection software for processing and classifying data.[242] The purpose of training is to allow the reinforcement learning agent to generalize new experiences; in other words, bypass new malware detection software.[243] The algorithm uses Q-learning and an MDP framework to train a reinforcement learning agent, where the reward function is associated with an anti-malware detection system (or an anti-malware engine).[244] If the anti-malware system detects the agent, its reward is zero, otherwise its reward is ten.[245] The researchers used OpenAI Gym, a software tool for building reinforcement learning environments, to conduct their experiments.[246] Consequently, the key takeaway of the paper is that the attacker requires no prior knowledge about the target to successfully penetrate a system under attack.[247]

Cyberspace allows humanity to communicate, trade, research, and share information on a global scale.[248] Yet, cyber-attacks are surging and increasing in volume each year.[249] As a result, data breaches have escalated increasing criticisms from regulators, private plaintiffs, and public opinion.[250] On the global scale, data and information are only as secure as the algorithms and network structures by which they are protected. Arguably, nothing that happens on a computer is secure, let

239. Thanh Thi Nguyen & Vijay Janapa Reddi, *Deep Reinforcement Learning for Cyber Security* (2019), https://arxiv.org/pdf/1906.05799.pdf.

240. Anderson et al., *supra* note 220; *see also* endgameinc, *Malware Env for OpenAI Gym* (2018), https://github.com/endgameinc/gym-malware.

241. Anderson et al., *supra* note 220.

242. Anderson et al., *supra* note 220.

243. *Id*.

244. *Id*.

245. *Id*.

246. Greg Brockman et al., *OpenAI Gym* (2016), https://arxiv.org/abs/1606.01540.

247. Anderson et al., *supra* note 220.

248. Kilovaty, *supra* note 224, at 179.

249. Loren F. Selznick, Carolyn LaMacchia, *Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners to Be?*, 13 J. BUS. & TECH. L. 217, 219 (2018).

250. Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for The Boardroom and The C-Suite*, 2015 COLUM. BUS. L. REV. 613, 615 (2015).

alone private.[251] Thus, there is a great deal of uncertainty surrounding security at all levels.[252] Indeed, the weaponization of cyberspace and resulting cyberwarfare, are creating a world in which traditional security defense models are futile.[253] And, the capability of hacking an enemy car, plane, nuclear reactor, communication system, or financial system has the potential to cripple an opposition's economy and defense capability.[254]

From a national security perspective, the United States is no longer the world leader in cybersecurity.[255] Indeed, The United States is under constant attack online.[256] Adversaries have caught up and arguably surpassed domestic cyber capabilities.[257] Many nations continue investing heavily in AI research and its commercial capabilities, exploiting new advances.[258] At the same time, the United States has been ignoring AI over the last decade.[259] As a result, the United States is consistently attacked on its vulnerable cyber-front and is subject to imminent national security threats.[260] While the United States faces imminent cybersecurity threats stemming from AI, the development of Artificial General Intelligence poses threats to both national and global security.

C. Artificial General Intelligence

AI's holy grail, Artificial General Intelligence (AGI), is a system capable of achieving any goal.[261] Current methods of AGI development are commonly referred to as whole-brain emulation, where the idea is to reverse engineer the human brain with computation.[262] Yet, the Wright brothers' first flight was not aboard a mechanical bird with flapping wings.[263] In fact, prominent physicist Michio Kaku argues computers

251. Jack M. Balkin, *The Constitution in The National Surveillance State*, 93 MINN. L. REV. 1, 14 (2008).

252. TIM MATHER ET AL., CLOUD SECURITY AND PRIVACY, Scitech Book News, Dec. 2009.

253. NAYAN B. RUPARELIA, CLOUD COMPUTING 108 (2016).

254. TEGMARK, *supra* note 18, at 118.

255. Kadtke, Wharton, *supra* note 2, at 1.

256. John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 398 (2016).

257. An Interview with Paul M. Nakasone, National Defense University Press, JFQ 92, 1st Quarter, at 5 (2019).

258. Kadtke, Wharton, *supra* note 2, at 2.

259. *Id*.

260. Center for Strategic and International Studies, Significant Cyber Incidents (August 2019), https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

261. TEGMARK, *supra* note 18, at 68.

262. KURZWEIL, *supra* note 9, at 124.

263. TEGMARK, *supra* note 18, at 156.

cannot truly replicate the behavior of human brains.[264] Kaku argues the shortcomings of modern neural networks persuasively, focusing on their inability to account from neurochemical fluctuations in information transfer.[265]

However, the legendary machine learning developer Paul John Werbos argued, from an engineering point of view, the human brain is an information processing system.[266] Therefore, it may be more likely AGI will result from a more simplified neural processing model capable of recursive self-improvement.[267] For example, famed philosopher of mind, Zoltan Torey approaches the mind from a linguistic perspective.[268] Indeed, according to Torey, the mind is made up of perceptions and words corresponding to those perceptions.[269]

Yet, some argue that AGI may never happen.[270] For example, the late Microsoft co-founder Paul Allen argues that scientific progress is irregular and hypothesizes that at the end the twenty-first century humans will have yet to achieve AGI.[271] Indeed, current systems are far from achieving many goals, particularly time-consuming tasks.[272] One example of such a task would be for a system to litigate a complex case in court from the filing of the complaint, through discovery, all the way to trial and verdict.[273]

To date, the closest mankind has come toward developing an AGI was Volodymyr Mnih's seminal paper, *Human-Level Control Through Deep Reinforcement Learning*, where Mnih introduces the DQN algorithm and associated software code for playing Atari Games.[274] Max Tegmark remarked of Minh's paper, "deep reinforcement learning is a completely general technique."[275] In this sense, Mnih's algorithm, the DQN,

264. MICHIO KAKU, THE FUTURE OF THE MIND 342 (2014).

265. *Id*.

266. WERBOS, *supra* note 63, at 305.

267. MURRAY SHANAHAN, THE TECHNOLOGICAL SINGULARITY 151 (2015). *See also* TEGMARK, *supra* note 18, at 156.

268. ZOLTAN TOREY, THE CONSCIOUS MIND 61 (2014).

269. *Id*.

270. Paul G. Allen, *The Singularity Isn't Near*, MIT TECHNOLOGY REVIEW (2011) https://www.technologyreview.com/s/425733/paul-allen-the-singularity-isnt-near/.

271. Paul G. Allen, *The Singularity Isn't Near*, MIT TECHNOLOGY REVIEW (2011) https://www.technologyreview.com/s/425733/paul-allen-the-singularity-isnt-near/. [Id. ?]

272. MURRAY SHANAHAN, THE TECHNOLOGICAL SINGULARITY 5 (2015).

273. This example ignores any legal ethics issues and is simply meant to be illustrative of a complicated task.

274. Mnih et al., *supra* note 73, at 529. *See also* Code for Human-Level Control through Deep Reinforcement Learning (2015), https://sites.google.com/a/deepmind.com/dqn/.

275. TEGMARK, *supra* note 18, at 85.

generalizes about its environment to achieve its goal.[276] But the DQN is limited by its environment, static reward structure, and training. Thus, a challenge exists to improve the generalizable qualities of current state-of-the-art AI systems.

From a national security perspective AGI is the end-all-be-all in advanced weaponry.[277] Any state or corporation capable of controlling AGI would surely be capable of conquering the world.[278] Indeed, with control of a system capable of achieving any goal controlling enemy defense systems, manipulating public opinion, and controlling information networks would be relatively simple.[279] However, there exists a question as to whether a human creator could control an AGI.[280] According to Max Tegmark, "we have no idea what will happen if humanity succeeds in building human-level AGI."[281] Thus, we cannot take for granted that the outcome will be positive if AGI is created.[282]

III. Policy

New generations of advanced technologies are changing the power dynamics of our global society.[283] Yet, legal scholarship on the topic of AI policy has denied and relatively ignored the national security threats associated with AI's weaponization.[284] For example, University of Washington Law Professor, Ryan Calo encourages regulators not to be distracted by claims of an "AI Apocalypse" and to focus their efforts on "more immediate harms."[285] However, it is important to realize, AI's most immediate applications will be in warfare.

Generally, it is accepted that law never keeps up with technology.[286] However, the kinetics of the two systems are relative, and it is more of an apples to oranges comparison. What is more likely to be true is that United States policy makers and military leaders are ill-equipped to put policies in place to maintain military superiority. For example, Judge Baker explains, "I do not feel a sense of urgency to address the legal,

276. Mnih et al., *supra* note 73, at 531. *See also* Code for Human-Level Control through Deep Reinforcement Learning (2015), https://sites.google.com/a/deepmind.com/dqn/.
277. BOSTROM, *supra* note 11, at 106-107.
278. *Id*. at 96-97.
279. TEGMARK, *supra* note 18, at 118.
280. BOSTROM, *supra* note 11, at 155.
281. TEGMARK, *supra* note 18, at 156.
282. PETER THEIL, ZERO TO ONE 195 (2014).
283. Kadtke, Wharton, *supra* note 2, at 2.
284. Calo, *supra* note 14, at 432.
285. *Id*. at 431.
286. Baker, *supra* note 12, at 7.

ethical, and policy challenges ahead."[287] Another example includes South Carolina Senator Lindsay Graham's infamous question to Mark Zuckerberg, "Is Twitter the same as what you do?" during the Senate Judiciary & Commerce Committees Joint Hearing on Facebook Data Use.[288] As Elon Musk persuasively argues, what governments need right now is not oversight, but rather insight, because right now the Government does not even have insight into AI issues.[289] Specifically, Musk contends we need technically capable people in government positions who can monitor AI's progress and steer it if warranted.[290] This Part explores the policies and developments from the three countries leading the way in AI militarization: Russia, China, and the United States. In analyzing the United States, this Part makes specific recommendations to improve current national security efforts.

Professor Crootof argues in any armed conflict, the right of the parties in the conflict to choose methods or means of warfare is not unlimited.[291] Furthermore, both customary international law and various treaties circumscribe which weapons may be lawfully fielded.[292] However, this line of argument does not apply in the context of AI. In fact, international laws and treaties are not laws in the sense that they are not enforceable because the nature of law rests on the assumption certain conduct be binding.[293] As Hart argued, "If the rules of international law are not binding it is surely indefensible to take seriously their classification as law."[294] The Latin maxim *Auctoritas non veritas facit legem*; which stands for the principle, authority, not truth, makes law, provides insight into the fickle nature of international law.[295] Or, in the words the English poet John

287. *Id*.

288. Committee on the Judiciary, Senate Committee on the Judiciary, Senate Committee on Commerce, Science, and Transportation, Facebook, Social Media Privacy, and the Use and Abuse of Data (Apr. 10, 2018), https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data. (Senator Graham Questioning Zuckerberg at 1:53:40-1:53:51).

289. *Elon Musk at the National Governors Association 2017 Summer Meeting*, C-SPAN (July 15, 2017), https://www.c-span.org/video/?431119-6/elon-musk-addresses-nga. (Musk responding to Arizona Governor Doug Ducey at 57:00-60:00).

290. *Elon Musk at the National Governors Association 2017 Summer Meeting*, C-SPAN (July 15, 2017), https://www.c-span.org/video/?431119-6/elon-musk-addresses-nga. *See also* TEGMARK, *supra* note 18, at 108.

291. Rebecca Crootof, Autonomous Weapons Systems and the Limits of Analogy, 9 Harv. Nat'l Sec. J. 51, 59 (2018).

292. *Id*.

293. H.L.A. HART, THE CONCEPT OF LAW 214 (3d. 2012).

294. *Id*.

295. THOMAS HOBBES: A PIONEER OF MODERNITY, 9 (2015) https://www.sunypress.edu/pdf/63242.pdf.

Lyly, "All is fair in love and war."[296] Therefore, any notion of an international AI treaty would be moot. In addition to the United States, China and Russia are making significant investments in AI for military purposes.[297]

A. China

In July 2017 China's State Council released an AI plan and strategy calling for China to pass the United States by 2020 and become the world's leader in AI by 2030, committing $150 billion to the goal.[298] By the end of 2018, Chinese leadership assessed the program's development as surpassing the United States, achieving its objective earlier than expected.[299] A key advantage of China's recent strategy has been in the development of innovative new systems, in direct contrast to the United States, whose commitments remain to updating outdated technologies and political favors toward the military industrial complex.[300]

Indeed, as a direct result of China's recent investments, China's military and intelligence services possess the sophistication and resources to hack network systems, establish footholds behind perimeter defenses, exfiltrate valuable information, and sabotage critical network functions.[301] In fact, Chinese government organizations routinely translate, disseminate, and analyze U.S. government and think tank reports about AI.[302] Further, in 2017, China expressed a desire to utilize AI for flight guidance and target recognition systems in its new generations of cruise missiles.[303] Just two years later, that desire was realized, and China is the world's leader in missile technology with its development of deep reinforcement learning control systems for targeting and guidance.[304] Further, Chinese

296. John Lyly Quotes, Goodreads, (2019) https://www.goodreads.com/author/quotes/139084.John_Lyly.

297. Department of Defense, Summary of the 2018 Department of Defense Artificial Intelligence Strategy 5 (2018), https://www.defense.gov/Newsroom/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/.

298. Baker, *supra* note 12, at 1.

299. Allen, *supra* note 6, at 9.

300. Alexander Rogosa, *Shifting Spaces: The Success of The SpaceX Lawsuit and The Danger of Single-Source Contracts in America's Space Program*, 25 Fed. Circuit B.J. 101, 104 (2015). *See also* Chris Anderson, *Elon Musk's Mission to Mars*, WIRED MAGAZINE (Oct. 21, 2012) https://www.wired.com/2012/10/ff-elon-musk-qa/.

301. John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 402-403 (2016).

302. Allen, *supra* note 6, at 3.

303. STEPHAN DE SPIEGELEIRE, ET AL., THE HAGUE CTR. FOR STRATEGIC STUDIES, ARTIFICIAL INTELLIGENCE AND THE FUTURE OF DEFENSE: STRATEGIC IMPLICATIONS FOR SMALL – AND MEDIUM-SIZED FORCE PROVIDERS 79 (2017).

304. YOU, ET AL., *supra* note 102, at 37447.

intercontinental ballistic missile and cruise missile systems reflect the state-of-the-art.[305]

Chinese commercial markets for autonomous drones and AI surveillance technologies have seen significant growth and success.[306] Additionally, Chinese weapons manufacturers are already selling armed AI controlled drones.[307] Chinese AI market success directly increases its military and intelligence abilities because Chinese companies developing AI work in close cooperation with the Chinese Military.[308] Some argue that many Chinese AI achievements are actually achievements of multinational research teams and companies.[309] For example, regarding SpaceX's decision not to patent its rocket technologies, Founder & CEO Elon Musk stated, "our primary long-term competition is in China—if we published patents, it would be farcical, because the Chinese would just use them as a recipe book."[310] Notably, none of the most popular machine learning software frameworks have been developed in China.[311] However, China's behavior of aggressively developing, utilizing, and exporting increasingly autonomous robotic weapons and surveillance AI technology runs counter to China's stated goals of avoiding an AI arms race.[312]

B. Russia

Vladimir Putin announced Russia's commitment to AI technologies stating, "[W]hoever becomes the leader in this field will rule the world."[313] Further, Russia continues to display a steady commitment to developing and deploying a wide range of AI military weapons.[314] In fact, Russia is significantly expanding its budget in AI cybersecurity to sway public and political opinion around the world.[315] For example, the IRA and GRU continue their hacking operations relating to United States

305. Michael S. Chase, PLA Rocket Force Modernization and China's Military Reforms, Testimony Before the U.S.-China Economic and Security Review Commission, RAND Corporation (Feb. 15, 2018), https://www.rand.org/pubs/testimonies/CT489.html.
306. Allen, *supra* note 6, at 6.
307. *Id*.
308. *Id*. at 21.
309. *Id*. at 10.
310. Anderson, *supra* note 300.
311. Allen, *supra* note 6, at 12.
312. Allen, *supra* note 6, at 7.
313. SAYLER, *supra* note 7, at 1.
314. DE SPIEGELEIRE, ET AL., *supra* note 303, at 81.
315. Kilovaty, *supra* note 224, at 158.

elections.[316] These efforts largely reflect effective and extensive use of AI driven cybersecurity technologies.[317]

Indeed, Russia stands out as a renewed threat in cyberspace.[318] Russia has demonstrated consistent and effective capabilities in implementing AI for behavior influencing.[319] Prior to the 2016 presidential election, the IRA utilized Facebook and YouTube, targeting millions of users with advertisements aimed at influencing the election's outcome.[320] Further, in October 2017, news broke of a Russian spy campaign targeted at key United States officials beginning in 2015 and lasting until the intrusion was discovered by the United States in September 2017.[321]

In addition, Russia is establishing a number of organizations devoted to the development of military AI applications.[322] Indeed, the Russian military has been researching and developing AI robotics control systems, with an emphasis on autonomous vehicles and planes with autonomous target identification and engagement capabilities.[323]And, in March 2018, Russia released plans for a National Center for Artificial Intelligence, among other defense related initiatives.[324] Despite Russia's aspirations, some analysts argue that it may be difficult for Russia to make significant progress in AI development due to lack of funding.[325] However, others argue despite trailing behind the United States and China in military funding, Russia has still managed to become a powerful force in cyberspace.[326] For example, in 2013 Russia was confident enough to grant the infamous Edward Snowden political asylum against pressure from the United States.[327]

C. United States

On February 11, 2019, President Trump issued an executive order aimed at establishing America's place as the global leader in artificial

316. ROBERT S. MUELLER, U.S. DEPARTMENT OF JUSTICE, *supra* note 172, at 4.
317. SAYLER, *supra* note 7, at 24.
318. Garon, *supra* note 234, at 4.
319. DE SPIEGELEIRE, ET AL., *supra* note 303, at 67.
320. Garon, *supra* note 234, at 8-9.
321. *Id.* at 6-7.
322. DE SPIEGELEIRE, ET AL., *supra* note 303, at 81-82.
323. Congressional Research Service, *supra* note 7, at 23.
324. *Id.*
325. *Id.* at 24.
326. *Id.*
327. David D. Cole, *Assessing the Leakers: Criminals or Heroes?*, 8 J. NAT'L SECURITY L. & POL'Y 107, 107 (2015). *See also* Jacob Stafford, *Gimme Shelter: International Political Asylum in The Information Age*, 47 VAND. J. TRANSNAT'L L. 1167, 1170 (2014).

intelligence technology.[328] The Executive Order on Maintaining American Leadership in Artificial Intelligence (Executive Order), explains the United States' policy to enhance scientific, technological, and economic leadership in AI research and development guided by five principles:[329]

1. The United States must drive technological breakthroughs in AI across the Federal Government, industry, and academia in order to promote scientific discovery, economic competitiveness, and national security.
2. The United States must drive development of appropriate technical standards and reduce barriers to the safe testing and deployment of AI technologies in order to enable the creation of new AI-related industries and the adoption of AI by today's industries.
3. The United States must train current and future generations of American workers with the skills to develop and apply AI technologies to prepare them for today's economy and jobs of the future.
4. The United States must foster public trust and confidence in AI technologies and protect civil liberties, privacy, and American values in their application in order to fully realize the potential of AI technologies for the American people.
5. The United States must promote an international environment that supports American AI research and innovation and opens markets for American AI industries, while protecting our technological advantage in AI and protecting our critical AI technologies from acquisition by strategic competitors and adversarial nations.[330]

While, the Executive Order is a nice gesture in supporting development in the right direction, a clear course of action is lacking.[331] The United States Government has a limited rule in scientific progress and development. Specifically, the only real role played in the development of technology comes from the power of the purse.[332] And, the Executive Order does not provide for new research funds.[333]

328. Donald J. Trump, Executive Order on Maintaining American Leadership in Artificial Intelligence, Exec. Order No. 13,859, 84 Fed. Reg. 3967 (Feb. 14, 2019).
329. *Id*.
330. *Id*.
331. Winston Luo, President Trump Issues Executive Order to Maintain American Leadership in Artificial Intelligence, HARV. J. J.L. & TECH. REPORTS, (Mar. 6, 2019), https://jolt.law.harvard.edu/digest/president-trump-issues-executive-order-to-maintain-american-leadership-in-artificial-intelligence.
332. Kate Stith, *Congress' Power of The Purse*, 97 YALE L.J. 1343, 1344 (1988).
333. Luo, *supra* note 331.

Some AI & Law scholars argue AI should be regulated by a Government agency.[334] For example, Matthew Scherer argues that the starting point for regulating AI should be a statute that establishes the general principles of AI regulation.[335] Scherer proposes the Artificial Intelligence Development Act ("AIDA"), which would create an agency tasked with certifying the safety of AI systems.[336] The main idea is that AIDA would delegate the substantive task of assessing the safety of AI systems to an independent agency staffed by specialists, thus insulating decisions about the safety of specific AI systems from the pressures exerted by electoral politics.[337] But, it is unlikely that standard command and control models of regulation would be effective to regulate AI.[338]

Further, Government agencies are notorious for over-spending and political corruption, specifically in defense procurement and regulation.[339] Indeed, in the words of the late John McCain, "Our broken defense acquisition system is a clear and present danger to the national security of the United States."[340] Despite calls for change, the military industrial complex is far too politically powerful to allow the system to improve.[341] Indeed, despite outspending Russia and China combined on defense, the United States is still falling behind.[342] The reason is largely attributable to billions in administrative waste and a lack of agency accountability.[343] In fact, one report suggests the Chinese are confident the United States will fail to innovate, continuing to overspend maintaining and upgrading outdated systems.[344] Others argue, no matter the potential for AI, the

334. Scherer, *supra* note 8, at 394.

335. *Id*.

336. *Id*. at 393.

337. *Id*.

338. Michael Guihot, et al., *Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence*, 20 VAND. J. ENT. & TECH. L. 385, 415 (2017).

339. Whitlock, Woodward, *supra* note 212. *See also University Research Company, LLC*, 2004 WL 2496439, at 10 (2004). *See also Femme Comp Inc. v. United States*, 83 Fed. Cl. 704, 767 (2008).

340. United States Committee on Armed Services, Press Release: Senate Armed Services Committee Completes Markup of National Defense Authorization Act for Fiscal Year 2016, https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-completes-markup-of-national-defense-authorization-act-for-fiscal-year- 2016.

341. *See generally* Brian S. Haney, *Automated Source Selection & FAR Compliance*, 48 PUB. CONT. L.J. (2019) (Forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3261360

342. Niall McCarthy, *The Top 15 Countries for Military Expenditure in 2016*, FORBES (Apr. 21, 2017), https://www.forbes.com/sites/niallmccarthy/2017/04/24/the-top-15-countries-for-military-expenditure-in-2016-infographic/#6ef65a0b43f3.

343. Whitlock & Woodward, *supra* note 212.

344. Allen, *supra* note 6, at 8.

Government should handle development carefully.[345] But the United States Government may have a more limited role in AI development than many suspect.

Private companies are driving progress in AI. For example, Google has a massive intelligence portfolio.[346] Some argue, Google's AI technologies are scalable to an AGI model.[347] Commercial AI products are already heavily deployed in marketing. Indeed, to take advantage of the services offered by today's major online corporation such as Google, Facebook, and Twitter, consumers are forced to give away a great deal of personal information.[348] A person's browser history and buying habits, together with their personal information, are enough for machine learning algorithms to predict what they'll buy and how much they'll pay for it.[349]

Interestingly, Judge Baker argues, national security law serves three purposes, providing essential values, process, and the substantive authority to act, as well as the left and right boundaries of action.[350] However, law is characterized by the relationship between a sovereign and subject acting in a habit of obedience.[351] Whether, technology companies like Facebook, Google, Amazon, Microsoft, and Apple have more sovereignty than the United States an interesting debate. Further, most AI research advances are occurring in the private sector, where talent and funding exceeds the United States Government.[352] As a result, militaries and intelligence agencies depend on the private sector for essential goods and services.[353] Thus, some suggest the challenges of regulating fast-

345. Michael Guihot et al., *supra* note 338, at 454.

346. US 2015/0100530, Methods and Apparatus for Reinforcement Learning, to Mnih, et al., Google (2015). WO 2018/083532, World Intellectual Property Organization, Training action selection using neural networks, to Wang Ziyu, et al., DeepMind (2016). WO 2018/083667 World Intellectual Property Organization Reinforcement Learning systems, to Silver, et al. DeepMind (2016). WO 2018071392, World Intellectual Property Organization, Neural networks for selecting actions to be performed by a robotic agent, to Pascanu, Razvan, et al., DeepMind (2016). WO 2018/081089, World Intellectual Property Organization, Processing sequences using neural networks, to Van Den Oord, et al., DeepMind (2016).

347. Iuliia Kotseruba, John K. Tsotsos, *A Review of 40 Years in Cognitive Architectures Research Core Cognitive Abilities and Practical Application*, 7 (2018), https://arxiv.org/abs/1610.08602v3.

348. MURRAY SHANAHAN, THE TECHNOLOGICAL SINGULARITY 170 (2015).

349. *Id.*

350. Baker, *supra* note 13, at 6.

351. Hart, *supra* note 293, at 50.

352. Allen, Chan, *supra* note 215, at 1.

353. Johnathan Wakely, Andrew Indorf, *Managing National Security Risk is an Open Economy: Reforming the Committee on Foreign Investment in the United States*, 9 HARV. NAT'L SEC. J. 1, 4 (2018).

moving technology are so great that industry self-regulatory approaches are often presented as the most effective mechanism to manage risk.[354] Therefore, one argument is the United States' national security law is in the hands of private companies, rather than the Government.

Some argue the United States' technological superiority is increasingly being challenged by competitors.[355] In truth, the United States government's technological superiority has already been surpassed, if not by China, certainly by the private sector.[356] Indeed, a serious question exists as to whether the AI arms race is between governments or private firms. Matthew Scherer argues Microsoft Google, Facebook, Amazon, and Baidu are in a private AI arms race.[357] An indication of this arms race is Microsoft's investment, OpenAI, whose stated mission is "to ensure that artificial general intelligence (AGI)—by which we mean highly autonomous systems that outperform humans at most economically valuable work—benefits all of humanity."[358] This mission was only slightly believable until the company received $1 billion in funding from Microsoft.[359] Google's AI principles include a mission to create an AI that is socially beneficial.[360] Yet, despite being a world leader in AI, Google's AI is used mainly for advertising, where Google derives ninety-five percent of its revenue.[361]

There is little social benefit or societal good to come from AI. There are some benefits in fields like law and medicine, but AI innovation fails to solve the access problems foundational to these industries.[362] At a

354. Michael Guihot, et al., *supra* note 338, at 431.

355. Kadtke & Wharton, *supra* note 2, at 1.

356. US 2015/0100530, Methods and Apparatus for Reinforcement Learning, to Mnih, et al., Google (2015). WO 2018/083532, World Intellectual Property Organization, Training action selection using neural networks, to Wang Ziyu, et al., DeepMind (2016). WO 2018/083667 World Intellectual Property Organization Reinforcement Learning systems, to Silver, et al. DeepMind (2016). WO 2018071392, World Intellectual Property Organization, Neural networks for selecting actions to be performed by a robotic agent, to Pascanu, Razvan, et al., DeepMind (2016). WO 2018/081089, World Intellectual Property Organization, Processing sequences using neural networks, to Van Den Oord, et al., DeepMind (2016).

357. Scherer, *supra* note 8, at 354.

358. *OpenAI Charter*, OpenAI (April 9, 2018), https://openai.com/charter/.

359. Stephen Nellis, Microsoft to Invest $1 Billion in OpenAI, Reuters (July 22, 2019), https://www.reuters.com/article/us-microsoft-openai/microsoft-to-invest-1-billion-in-openai-idUSKCN1UH1H9.

360. Sundar Pichai, AI at Google: Our Principles, (June 7, 2018), https://ai.google/principles/.

361. GILDER, *supra* note 79, at 37.

362. HEMANT TANEJA, UNSCALED: HOW AI AND NEW GENERATION OF UPSTARTS ARE CREATING THE ECONOMY OF THE FUTURE, 73 (2018). *See also* KEVIN D. ASHLEY, ARTIFICIAL INTELLIGENCE AND LEGAL ANALYTICS 3 (2018).

deeper level, inequality and injustice are largely supported by societal structures, staying blind to technological developments and AI will only exacerbate these problems. Indeed, AI is developing in corporations whose principle purpose is to maximize shareholder wealth.[363] Further, the AI & Ethics school of thought is largely idealistic and academic.[364] In a perfect world, corporate ethics would support AI development in compliance with certain principles.[365] In reality, the United States Government has little control over profit driven big technology corporations and lacks meaningful insight into AI research.[366] The Russian and Chinese Government also lack control over big technology corporations, relying on their research to develop their own AI systems. [367] In sum, the dynamics of United States AI national security policy largely revolve around decisions made by corporate actors, specifically: Amazon, Google, Facebook, Microsoft, and Apple.[368] There is an improbable exception that a breakthrough in AI will occur by a smaller team or single person producing AGI.[369]

Conclusion

Conventional wisdom teaches technological progress is driven by the Law of Accelerating Returns (LOAR).[370] The LOAR's application to information technology, Moore's Law, projects exponential trends in technological progress converging to an ultimate technological singularity.[371] This notion has developed into a school of thought called Technological Utopianism.[372] Technological Utopianism refers to the idea that digital life is the natural and desirable next step in the cosmic evolution

363. Julian Velasco, *The Fundamental Rights of The Shareholder*, 40 U.C. DAVIS L. REV. 407, 409 (2006).

364. Karl & Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J.L. & TECH. 106, 160 (2019).

365. Veronica Root, *Coordinating Compliance Incentives*, 102 CORNELL L. REV. 1003, 1051 (2017).

366. Veronica Root, *The Compliance Process*, 94 IND. L.J. 203, 231 (2019). *See also Elon Musk at the National Governors Association 2017 Summer Meeting*, C-SPAN (July 15, 2017), https://www.c-span.org/video/?431119-6/elon-musk-addresses-nga. (Musk responding to Arizona Governor Doug Ducey at 57:00-60:00).

367. Allen, *supra* note 6, at 12.

368. Alexander Tsesis, *Marketplace of Ideas, Privacy, and The Digital Audience*, 94 NOTRE DAME L. REV. 1585, 1589 (2019).

369. BOSTROM, *supra* note 11, at 101.

370. Haney, *supra* note 22 at 155.

371. KURZWEIL, *supra* note 9, at 250.

372. TEGMARK, *supra* note 18, at 32.

of humanity, which will be good.[373] As a result of Technological Utopianism, a majority of literature on the subject of technology is inherently optimistic, both in terms of outcomes and rates of progress.[374] Yet, it is critical to resist the temptation to accept the claims of this literature.[375] The future does not happen on its own and AI technologies could certainly have terrible outcomes.[376]

One argument for the future of the United States Government in AI development is to pursue an open government model. Open government is a concept referring to the free flow of information between the Government and the public.[377] The goal of such a model would be to improve transparency, education and access to critical AI information.[378] As a result, AI issues could be discussed, debated, and decided democratically. However, in practice there is little hope such a model would be put into practice. This is particularly true in the United States where agencies fight tooth and nail to hide information to which the public has a right via FOIA litigation.[379]

A second argument is that AI technology's likely dissemination into the wrong hands resolves the Fermi Paradox. A paradox is a set of arguments with apparently true propositions, leading to a false conclusion.[380] Consider, the Milky Way is one of hundreds of billions of galaxies in the Universe, each containing hundreds of billions of stars.[381] Commonly, these stars contain Earth-like planets.[382] As a result, statistically it is almost certain life would have developed somewhere else in the Universe before life on Earth.[383] And yet, mankind finds itself bound to a pale blue dot on the outskirts of the Milky Way, apparently alone in the Universe. Fermi's Paradox asks the question, "Where are they?"[384]

373. MARTINE ROTHBLATT, VIRTUALLY HUMAN 283 (2104).

374. BOSTROM, *supra* note 11, at 34.

375. Peter Thiel, *The Education of a Libertarian*, CATO UNBOUND (May 1, 2009).

376. PETER THIEL, ZERO TO ONE 195 (2014).

377. Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 895 (2006).

378. Joshua Apfelroth, *The Open Government Act: A Proposed Bill to Ensure the Efficient Implementation of The Freedom of Information Act*, 58 ADMIN. L. REV. 219, 220 (2006).

379. John C. Brinkerhoff Jr., FOIA's Common Law, 36 YALE J. ON REG. 575, 576 (2019). (FOIA is an acronym for Freedom of Information Act).

380. MARGARET CUONZO, PARADOX 2 (2014).

381. CARL SAGAN, PALE BLUE DOT A VISION OF THE HUMAN FUTURE IN SPACE 21 (1994).

382. Nick Bostrom, *In the Great Silence there is Great Hope* 2 (2007) https://nickbostrom.com/papers/fermi.pdf.

383. *Id.*

384. *Id.* at 5.

The great British Mathematician Irving J. Good argued AGI would be the "last invention that man need ever make."[385] And the late Stephen Hawking observed, "The development of artificial intelligence could spell the end of the human race."[386] Further, both Nick Bostrom and Max Tegmark have argued persuasively, humans may not be able to control AGI.[387] These observations provide support that AI may lead to a catastrophic event resolving the Fermi Paradox.

In sum, the United States' national security is now dependent, not on its Military or Defense Agencies, but on big technology companies. In part because big technology companies have powerful influence over political decision makers.[388] Further, big technology companies have the most talented people and own the rights to the most powerful weapons. Yet, the answer is not to break up big technology companies, which disadvantages the United States compared to our adversaries.[389] Instead the answer is to accept the changing power dynamics and do the best we can with a broken political system. The only alternative would be revolution.[390]

385. Irvin J. Good, *Speculations Concerning the First Ultraintelligent Machine*, 6 ADVANCES IN COMPUTERS 31 (1965).

386. Rory Cellan-Jones, *Stephen Hawking Warns Artificial Intelligence Could End Mankind*, BBC NEWS (Dec. 2, 2014), http://christusliberat.org/wp-content/uploads/2017/10/Stephen-Hawking-warns-artificial-intelligence-could-end-mankind-BBC-News.pdf.

387. BOSTROM, *supra* note 11, at 155. *See also* TEGMARK, *supra* note 18, at 176.

388. Megan Henney, *Big tech has spent $582M lobbying Congress. Here's where that money went*, FOXBUSINESS (July 26, 2019), https://www.foxbusiness.com/technology/amazon-apple-facebook-google-microsoft-lobbying-congress.

389. Sheelah Kolhatkar, *How Elizabeth Warren Came Up with a Plan to Break Up Big Tech*, THE NEW YORKER (August 20, 2019), https://www.newyorker.com/business/currency/how-elizabeth-warren-came-up-with-a-plan-to-break-up-big-tech.

390. NATIONAL ARCHIVES, THE DECLARATION OF INDEPENDENCE: A TRANSCRIPTION (July 4, 1776), https://www.archives.gov/founding-docs/declaration-transcript.

APPENDIX A. SUMMARY OF NOTATION

Notation	
π^*	
$\mathrm{Q}(s,a)$	
(s,a)	
ϕ	
γ	
$\mathbb{E}[x]$	
$arg \max_a f(a)$	
r	
θ_k	
$L(s,a,\theta_k,\theta\ )$	
$A^{\pi_{\theta_k}}$	
$\pi_\theta(a\|s)$	
ϵ	
$a^*(s)$	
$\mathcal{D}$	

APPENDIX B. SIGNIFICANT CYBER INCIDENTS DATA

Year	China	Russia
2009 (September 2008 - August 2009)	3	2
2010 (September 2009 - August 2010)	9	3
2011 (September 2010 - August 2011)	4	0
2012 (September 2011 - August 2012)	4	0
2013 (September 2012 - August 2013)	8	4
2014 (September 2013 - August 2014)	3	0
2015 (September 2014 - August 2015)	7	5
2016 (September 2015 - August 2016)	3	5
2017 (September 2016 - August 2017)	4	11
2018 (September 2017 - August 2018)	13	27
2019 (September 2018 - August 2019)	24	30

***