The Ethical Midfield in Artificial Intelligence: Practical Reflections for National Security Lawyers

Matthew Ivey*

Abstract

This Article reflects on the ethical lessons learned in national security law during the eighteen years after September 11, 2001, and then applies those lessons to future challenges national security lawyers may face in providing advice in the field of Artificial Intelligence. Further, this Article seeks to move beyond the theoretical or academic and focus instead on the practical aspects of Artificial Intelligence that national security lawyers should consider when advising clients. First, this Article considers how national security lawyers can keep their clients within ethical boundaries by shaping advice and policy. Second, this Article examines how national security lawyers should weigh issues regarding relationships with industry. Third, this Article warns that failing to pay attention to adversaries could lead to drifting off the ethical midfield.

Table Of Contents

* Commander in the United States Navy. The views expressed in this Article are the Author's own. They do not necessarily represent the views of the Department of Defense, the United States Navy, or any of its components. The Author would like to thank the staff of the *Georgetown Journal of Legal Ethics* for their outstanding editorial assistance.

INTRODUCTION

On August 4, 2017, Former Secretary of Defense James Mattis issued a memorandum to all Department of Defense ("DoD") employees, setting forth his expectation that every member of the Department "play the ethical midfield."[1] Secretary Mattis stressed that training and prior reflection will best prepare members of the Department to "remain morally strong especially in the face of adversity."[2] The United States remains in the midst of the post-September 11 "endless war,"[3] during which national security lawyers have learned some hard lessons. And as a society, we are also on the verge of a fourth industrial revolution initiated by exponential advancements in Artificial Intelligence ("AI").[4] The potential for ethical missteps in this emerging space are plentiful, particularly in the area of national security. Inevitably, the legal issues related to AI will capture the attention of all national security lawyers, rather than just a few niche specialists. To paraphrase the old adage, if we do not learn from our mistakes, we are doomed to repeat them.[5] Accordingly, there is no better time than the present to reflect on some ethical lessons learned in national security law during the past eighteen years in the war on terrorism as we prepare for future challenges posed by AI.

---

1. Memorandum for All Department of Defense Employees from James Mattis, Secretary, Department of Defense (Aug. 4, 2017), *available at* https://assets.documentcloud.org/documents/3913969/ETHICAL-STANDARDS-for-ALL-HANDS-OSD009354-17-FOD.pdf [https://perma.cc/59MJ-GMF4].

2. *Id.*

3. *See* Katrina Vanden Heuvel, *The Transpartisan Revolt against America's Endless Wars*, WASH. POST (July 16, 2019), https://www.washingtonpost.com/opinions/2019/07/16/transpartisan-revolt-against-americas-endless-wars/?utm_term=.f8967fe5024c [https://perma.cc/BB2G-GMAZ].

4. *See, e.g.*, Klaus Schwab, *The Fourth Industrial Revolution: What It Means, How to Respond*, WORLD ECON. F. (Jan. 14, 2016), https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond [https://perma.cc/JB4Y-EQ8B].

5. The actual quote is: "Those who cannot remember the past are condemned to repeat it." GEORGE SANTAYANA, THE LIFE OF REASON 12 (1905). The U.S. military experienced this scenario recently in Afghanistan and Iraq. The counterinsurgency efforts in both countries suffered from constant unit turnover, lack of organizational memory, and a tendency to repeat mistakes. Leaving units took hard-earned local knowledge with them, and incoming units had to "reinvent the wheel." *See* JERRY MEYERLE ET AL., ON THE GROUND IN AFGHANISTAN: COUNTERINSURGENCY IN PRACTICE 23 (2012).

In legal circles, new technologies or techniques are often met with skepticism, resistance, fear, or panic.[6] Couple a new technology or technique with critical national security implications, and a lawyer might quickly find himself or herself pressurized to "get to yes" in order to "protect the homeland," "win the fight against terrorism," or otherwise "enable the mission."[7] In such a pressurized environment, a lawyer and his or her client can easily drift beyond the ethical midfield. Since September 11, 2001, the practice of national security law has provided ample examples where new technologies or techniques have given way to "sloppily reasoned, overbroad, and incautious" lawyering.[8] Many lawyers who practiced national security law during this time published their reflections of confronting these challenges in a series of books and articles.[9] But these accounts do no public good unless national security lawyers of today heed their lessons.

This Article serves to reflect on the ethical lessons learned in national security law during the first eighteen years after September 11, 2001, and then applies those lessons to future challenges national security lawyers may face in providing advice in the field of AI. Further, this Article seeks to move beyond the theoretical or academic and focuses instead on the practical aspects of this area that national security lawyers should consider when advising clients. Accordingly, this Article first considers how national security lawyers can keep their clients within ethical boundaries by shaping their legal advice and government policy. Second, this Article examines how national security lawyers should approach relationships with industry. Third, this Article warns that failing to pay attention to adversaries could lead to drifting off the ethical midfield.

I. SHAPING LEGAL ADVICE AND GOVERNMENT POLICY

> "'When I use a word,' Humpty Dumpty said, in rather a scornful tone, 'it means just what I choose it to mean—neither more nor less.' 'The question is,' said Alice, 'whether you can make words mean so many different things.'

6. *See, e.g.*, Mark A. Cohen, *Legal Innovation is the Rage, But There's Plenty of Resistance*, FORBES (Aug. 30, 2018), https://www.forbes.com/sites/markcohen1/2018/08/30/legal-innovation-is-the-rage-but-theres-plenty-of-resistance/#4f2617667cdd [https://perma.cc/632T-ZSVB].

7. "[W]e are not living in times in which lawyers can say no to an operation just to play it safe. We need excellent, aggressive lawyers who give sound, accurate legal advice, not lawyers who say no to an otherwise legal operation just because it is easier to put on the brakes." *On the Nomination of Scott W. Muller to be General Counsel to the Central Intelligence Agency: Hearing Before the S. Select Comm. on Intelligence*, 107th Cong. (2002) (Statement of Sen. Bob Graham, Chair, S. Select Comm. on Intelligence).

8. JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 10 (2007).

9. *See, e.g.*, *id.* at 13; JOHN ASHCROFT, NEVER AGAIN: SECURING AMERICA AND RESTORING JUSTICE 131 (2006); JOHN YOO, WAR BY OTHER MEANS: AN INSIDER'S ACCOUNT OF THE WAR ON TERROR xii (2006); Michael B. Mukasey, *The Role of Lawyers in the Global War on Terrorism*, 32 B.C. INT'L & COMP. L. REV. 179, 181 (2009).

> 'The question is,' said Humpty Dumpty, 'which is to be master—that's all.' Alice was much too puzzled to say anything . . . ."[10]
>
> — Lewis Carroll, Alice's Adventures in Wonderland

A. DEFINE TERMS, CONTEXT, AND STANDARDS

1. WORDS MATTER

The importance of defining terms has been stressed by judges and attorneys in all subjects of the law, including in Supreme Court cases, which serve as the foundation of American jurisprudence.[11] While there are many good justifications for defining terms,[12] two reasons appear to rise above the rest in the field of AI. First, defining terms can help govern behavior.[13] Rules become unenforceable if they do not define what they intend to govern or are so vague that they can easily be circumvented by semantic arguments.[14] Second, defining terms can enhance predictability for decision-makers.[15] Some may counter that flexible or undefined terms are desirable because they allow discretion and create decision-making space.[16] The consequence of allowing such discretion, however, is that it then becomes difficult to control how this discretion is exercised or interpreted.[17]

In the initial years after September 11, 2001, the imprecise definition of "torture" arguably drove the Bush administration away from the ethical midfield. There is wide international consensus that torture is illegal as reflected by the unconditional ban of torture in numerous treaties.[18] Legal analysis of Bush

---

10. LEWIS CARROLL, ALICE'S ADVENTURES IN WONDERLAND AND THROUGH THE LOOKING GLASS 190 (OXFORD UNIVERSITY PRESS 1982).

11. *See, e.g.*, California v. Hodari D., 499 U.S. 621, 622–23 (1991) (defining "seizure"); INS v. Chadha, 462 U.S. 919, 925 n.2 (1983) (defining "veto"); Miller v. California, 413 U.S. 15, 20 n.2 (1973) (defining "obscene" and "pornography"); Roe v. Wade, 410 U.S. 113, 160, n.59 (1973) (defining "fetus"); Samuel A. Thumma & Jeffrey L. Kirchmeier, *The Lexicon Has Become a Fortress: The United States Supreme Court's Use of Dictionaries*, 47 BUFF. L. REV. 227, 228 (1999); Erin Huntington, *Torture and Cruel, Inhuman or Degrading Treatment: A Definitional Approach*, 21 U. CAL. DAVIS J. INT'L L. & POL'Y 279, 289 (2015); George K. Walker & John E. Noyes, *Definitions for the 1982 Law of the Sea Convention*, 32 CAL. W. INT'L L.J. 343, 345 (2003).

12. Julian B. McDonnell, *Definition and Dialogue in Commercial Law*, 89 NW. U. L. REV. 623, 626 (1995) (describing six reasons: (1) to systemize the subjects of the law; (2) to conceptualize new terms and ideas; (3) defining terms is part of the larger ritual of legal process; (4) to empower judges to make boundary distinctions; (5) to provide contrast guidance; and (6) to enhance predictability in decision-making).

13. For example, a law is void for vagueness if it "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." United States v. Williams, 553 U.S. 285, 304 (2008).

14. *See id.*

15. *See* McDonnell, *supra* note 12, at 651 (noting definitions can be a means of reducing uncertainty).

16. *Cf.* Greer v. Spock, 424 U.S. 828, 837–38 (1976) (holding that crimes punishable by courts-martial should not be held to the same vagueness standard as would apply to an ordinary criminal statute).

17. *See* KENNETH CULP DAVIS, DISCRETIONARY JUSTICE: A PRELIMINARY INQUIRY 216 (1969).

18. *See* Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, art. 2, Dec. 10, 1984, 1465 U.N.T.S. 85; International Covenant on Civil and Political Rights, arts. 4, 7, Dec. 16, 1966, 999 U.N.T.S. 171 ("No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment."); Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed

administration lawyers, however, focused not on whether certain treatment of prisoners was permissible under the law, but rather on an ambiguous definition of "torture."[19] Specifically, attorneys for the Bush administration argued that a wide range of techniques known as "enhanced interrogation" did not fall within the definition of "torture" and therefore, were lawful and justified in the name of national security.[20]

In the now infamous "Torture Memos," Bush administration attorneys defined torture as an act "equivalent in intensity to the pain accompanying serious physical injury, such as organ failure, impairment of bodily function, or even death."[21] For *mental* anguish to qualify as torture, the harm needed to last "months or years."[22] In order for one to be *criminally* liable for torture, the memos required a demonstration of the actor's "specific intent to cause prolonged mental harm."[23] By establishing these high thresholds, lawyers provided the administration with maximum latitude to develop an interrogation policy and shielded those involved from criminal liability. The memos were roundly criticized in the international legal community for giving legal sanction to practices like waterboarding, extended sleep deprivation, forced nudity, and confinement of prisoners in small, dark boxes.[24] According to Professor Martin Lederman, a former adviser to the Office of Legal Counsel ("OLC") during the Obama Administration, the memos were "seen as one of the most extreme deviations from the rule of law."[25]

If terms are ill-defined—as is currently the case with AI—a national security lawyer can help his or her client by assisting in defining terms and shaping policy rather than allowing ambiguous, overly broad, or otherwise incorrect definitions to open the door to ethical missteps. Remaining in the ethical midfield starts with an appreciation of the existing definitions. National security lawyers must also grasp how the term "artificial intelligence" is commonly understood and why the field of AI matters now. Once terms are better defined, determining what

---

Forces in the Field, art. 3, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention Relative to the Treatment of Prisoners of War, art. 17, Aug. 12, 1949 ("No physical or mental torture, nor any other form of coercion, may be inflicted on prisoners of war to secure from them information of any kind whatever.").

19. *See* Memorandum from Jay S. Bybee, Assistant Attorney Gen., to Alberto R. Gonzales, Counsel to the President, Standards of Conduct for Interrogation Under 18 U.S.C. §§ 2340-2340A 1, 3, 13 (Aug. 1, 2002).

20. *Id*. at 33, 37.

21. *Id*. at 1.

22. Memorandum from Jay S. Bybee, Assistant Att'y Gen., to John Rizzo, Acting Gen. Counsel of the Cent. Intelligence Agency, "Interrogation of Al Qaeda Operative" 15 (Aug. 1, 2002), *available at* https://www.justice.gov/sites/default/files/olc/legacy/2010/08/05/memo-bybee2002.pdf [https://perma.cc/YY2F-HULL].

23. *Id*. at 17.

24. *See* HUMAN RIGHTS WATCH, GETTING AWAY WITH TORTURE: THE BUSH ADMINISTRATION AND MISTREATMENT OF DETAINEES 7 (2011) ("The problem is that the legal advice in question—contained in memoranda drafted by the OLC, which provides authoritative legal advice to the president and all executive branch agencies—itself authorized torture and other ill-treatment.").

25. Johnny Dwyer, *Bush Torture Memo Slapped Down by Court*, TIME (Nov. 3, 2008), http://content.time.com/time/nation/article/0,8599,1855910,00.html [https://perma.cc/ES4L-68N5].

standards will apply when using AI in national security matters will help one's client have a clearer view of all ethical sidelines.

2. WHAT IS "ARTIFICIAL INTELLIGENCE" AND WHY DOES IT MATTER NOW?

Although the term "artificial intelligence" has existed for at least seventy years, there is no single widely accepted definition.[26] Indeed, "artificial intelligence" has been defined varyingly by scientists and salesman as a "rational agent," a field of study, a technique, a demonstrated capability, and in myriad other ways.[27] For the purposes of this Article, however, AI can be understood as any technique aimed at approximating some aspect of human cognition using machines.[28]

"Artificial intelligence" is "an umbrella term, comprised by many different techniques" rather than just a single method.[29] Two of the most commonly referenced subsets of AI are (1) machine learning and (2) deep learning, which are often used by practitioners incorrectly or interchangeably.[30] *Machine learning* is a technique that drives a computer (i.e. a *machine*) to accomplish a task without being explicitly programmed to do so (i.e. *learn on its own*).[31] In essence, machine learning uses algorithms that "parse past data, learn from that data," and then *apply* what is learned from the data to make informed recommendations or decisions.[32] A basic machine learning model progressively improves at whatever

---

26. Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 404 (2017).

27. *See* John McCarthy, What Is Artificial Intelligence? 2 (Nov. 12, 2007) (unpublished manuscript) (on file with Stanford University). Dartmouth Professor John McCarthy, who first used the term in 1956, defined artificial intelligence as "the science and engineering of making intelligent machines, especially intelligent computer programs." *Id.*; *see also* STUART J. RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 4 (3d ed. 2010). Stuart Russell and Peter Norvig, the writers of the quintessential textbook on artificial intelligence, defined artificial intelligence as a "rational agent" in which machines "operate autonomously, perceive their environment, persist over a prolonged time period, adapt to change, and create and pursue" the best expected outcome. *Id.*; Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 HARV. J.L. & TECH. 353, 364 (2016). Matthew Scherer defined artificial intelligence as "machines that are capable of performing tasks that, if performed by a human, would be said to require intelligence." *Id.*; A.M. Turing, *Computing Machinery and Intelligence*, 59 MIND 433, 434 (1950). In computing pioneer Alan Turing's imitation game, a computer attempted to convince a human interrogator that it is a human instead of a machine thereby displaying "artificial intelligence." *Id.*

28. *See* RUSSELL & NORVIG, *supra* note 27; Scherer, *supra* note 27; Turing, *supra* note 27; McCarthy, *supra* note 27.

29. Calo, *supra* note 26, at 405.

30. *See* Eric Yates, *What is the Difference Between AI, Machine Learning, and Deep Learning?*, TOWARDS DATA SCIENCE (Mar. 14, 2019), https://towardsdatascience.com/clarity-around-ai-language-2dc16fdb6e82 [https://perma.cc/45T2-MJJ7].

31. *See* A.L. Samuel, *Some Studies in Machine Learning Using the Game of Checkers. II – Recent Progress*, 11 IBM J. 601, 601 (1967); *see also* Andrew Ng, CS229 Lecture Notes, Introduction to Machine Learning: Lecture 1, Stanford Univ. (2011), (transcript available through Stanford University).

32. Michael Copeland, *What's the Difference Between Artificial Intelligence, Machine Learning, and Deep Learning?*, NVIDIA (Jun. 29, 2016), https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/ [https://perma.cc/4RPW-QCGJ]; *see* Kevin Parrish, *Deep Learning vs. Machine Learning: What's the Difference Between the Two?*, DIGITAL TRENDS (Jan. 27, 2018), https://www.digitaltrends.com/cool-tech/deep-learning-vs-machine-learning-explained/2/ [https://perma.cc/SAM3-ZZ7M].

task it is designed to complete, but still requires guidance or input from a human programmer to ensure recommendations and decisions are correct.[33]

Deep learning is an advanced form of machine learning, inspired by the interconnected neurons of the human brain.[34] Billions of neurons in the human brain work together to perform any coordinated activity in everyday life.[35] For example, to answer a phone, different neurons work to recognize the ring sound, pick up the phone, greet the caller, and perform all other life-sustaining functions, such as breathing and blinking. Mimicking this biological system, deep learning structures algorithms in multiple internal layers to create an *artificial* neural network that can learn and make intelligent decisions.[36] Each layer performs a different function to facilitate a larger task. Unlike machine learning, deep learning can determine if predictions are accurate without the intervention of a human programmer.[37]

Hollywood movies, like *The Terminator*, prognosticate a future where machines can think and fight wars like humans but without any human involvement.[38] While most mainstream scientists believe it is unlikely that machines will achieve true cognition or sentience in the near future,[39] one can nevertheless look at the significant progress made in games involving AI to gain a better understanding of key terms. Furthermore, reviewing the progress of AI in games provides a common point of reference for understanding the state of the technology with others in the field. Finally, one can see the AI advances in games and gain some appreciation of where the technology may be headed in more practical settings.

In 1996, IBM's chess-playing computer, Deep Blue, defeated world champion, Garry Kasparov, in the first of six games.[40] Kasparov went on to win that series, but the following year, an upgraded version of Deep Blue defeated Kasparov and Deep Blue retired as the first computer to defeat a standing world champion under tournament conditions.[41] Deep Blue was a significant AI milestone, but did not utilize the machine learning methods available today.[42] Instead, Deep Blue was

---

33. *See, e.g.*, Copeland, *supra* note 32; Parrish, *supra* note 32.

34. Copeland, *supra* note 32; *see* Parrish, *supra* note 32.

35. E. BRUCE GOLDSTEIN, SENSATION AND PERCEPTION 46 (2007).

36. *See, e.g.*, Copeland, *supra* note 32; Parrish, *supra* note 32.

37. *See, e.g.*, Copeland, *supra* note 32; Parrish, *supra* note 32.

38. THE TERMINATOR (Orion Pictures 1984); *see also* TERMINATOR 2: JUDGMENT DAY (Tristar Pictures 1991); TERMINATOR 3: RISE OF THE MACHINES (Warner Bros. Pictures 2003); TERMINATOR SALVATION (Warner Bros. Pictures 2009); TERMINATOR GENISYS (Paramount Pictures 2015).

39. *See, e.g.*, Bobby Azarian, *The Myth of Sentient Machines*, PSYCHOLOGY TODAY (Jun. 1, 2016), https://www.psychologytoday.com/us/blog/mind-in-the-machine/201606/the-myth-sentient-machines [https://perma.cc/6M8W-9RXY].

40. Demis Hassabis, *Artificial Intelligence: Chess Match of the Century*, 544 NATURE 413, 413–14 (2017).

41. *Id.* (Mr. Kasparov accused IBM of cheating and demanded a rematch, and IBM declined).

42. Jo Best, *The Inside Story of How the Jeopardy-Winning Supercomputer was Born, and What it Wants to do Next*, TECHREPUBLIC (Sept. 9, 2013), https://www.techrepublic.com/article/ibm-watson-the-inside-story-of-how-the-jeopardy-winning-supercomputer-was-born-and-what-it-wants-to-do-next/ [https://perma.cc/V6DR-TB2J].

based on "Good Old-Fashioned Artificial Intelligence" or symbolic AI, which relies on a fixed set of behavioral rules.[43]

In 2011, IBM's Watson, a computer system capable of answering questions in natural language, handily defeated *Jeopardy!* champions Brad Rutter and Ken Jennings.[44] Mr. Jennings quipped, "I, for one, welcome our new computer overlords," when Alex Trebek revealed the "Final Jeopardy!" answer.[45] Watson represented a significant advancement in *machine learning*. Rather than relying on a fixed set of behavioral rules like symbolic AI, Watson relied on algorithms parsing through large amounts of data to provide natural language responses to trivia.[46]

Computers have become even more dominant at games in recent years. The ancient Chinese board game, Go, has long been viewed as the most challenging game for AI to conquer due to its complexity.[47] Until recently, despite decades of programming efforts, the best Go-playing computers were only able to play at the level of human amateurs.[48]

Google's AI subsidiary developed AlphaGo to take on the world's greatest Go players.[49] In March 2016, AlphaGo defeated eighteen-time world champion Lee Sedol in four out of five games.[50] AlphaGo used artificial neural networks to learn from a database of 100,000 games, thereby demonstrating deep learning.[51] The following year, Google unveiled AlphaGo Zero, which proved to be exponentially stronger than its predecessor.[52] While the original model relied on a large database of games, AlphaGo Zero was programmed only with the basic rules of Go.[53] Everything else AlphaGo Zero learned was by playing Go against itself

---

43. Sean Dorrance Kelly & Hubert Dreyfus, *Watson Still Can't Think*, N.Y. TIMES (Feb. 28 2011), https://opinionator.blogs.nytimes.com/2011/02/28/watson-still-cant-think/ [https://perma.cc/46U2-Z52N].

44. John Markoff, *Computer Wins on "Jeopardy!" : Trivial, It's Not*, N.Y. TIMES (Feb. 17, 2011), http://www.nytimes.com/2011/02/17/science/17jeopardy-watson.html?pagewanted=all [https://perma.cc/7WK4-48L7].

45. *Id.*; Ken Jennings, *My Puny Human Brain*, SLATE (Feb. 16, 2011), https://slate.com/culture/2011/02/watson-jeopardy-computer-ken-jennings-describes-what-it-s-like-to-play-against-a-machine.html [https://perma.cc/2BM7-4ADC] (Mr. Jennings would later write that "Brad and I were the first knowledge-industry workers put out of work by the new generation of 'thinking' machines . . . but I'm sure [we] won't be the last").

46. Best, *supra* note 42.

47. *See* Hope Reese, *How Google's DeepMind Beat the Game of Go*, TECH REPUBLIC (Feb. 26, 2016), https://www.techrepublic.com/article/how-googles-deepmind-beat-the-game-of-go-which-is-even-more-complex-than-chess/ [https://perma.cc/V695-ASJV]. Go is a strategy-based board game, but more complex than Chess in some important ways. For example, at the beginning of a Chess match, there are 20 possible moves; in Go, the first player has 361 possible moves.

48. *See* Cade Metz, *In Two Moves, AlphaGo and Lee Sedol Redefined the Future*, WIRED (Jan. 27, 2016), https://www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future/ [https://perma.cc/4UT9-SHZQ].

49. *See id.*

50. *Id.*

51. *Id.*

52. *See* Dawn Chan, *The AI That Has Nothing to Learn from Humans*, THE ATLANTIC (Oct. 20, 2017), https://www.theatlantic.com/technology/archive/2017/10/alphago-zero-the-ai-that-taught-itself-go/543450/?utm_source=twb [https://perma.cc/9PKH-S43W].

53. *Id.*

millions of times rather than from a database of games.[54] After three days of self-play, AlphaGo Zero was strong enough to defeat its predecessor 100 times in a row without losing.[55]

Despite their complexity, games are relatively easy for computers to understand because the rules are finite, there is no hidden information, and programmers have access to perfect simulations of the games. The AI used in games does not apply perfectly in the real world. In complex domains (such as warfare in an urban environment), the rules are not finite and human programmers cannot plan for every scenario. One can nevertheless see the potential for AI to be a game-changer in the national security space. Indeed, military commanders at all echelons have shown increased interest in utilizing AI to gain competitive military advantages short of lethal action.[56] For example, DoD's Algorithmic Warfare Cross-Functional Team, Project Maven, is using machine learning with the goal that people and computers will work symbiotically to increase the ability to detect objects.[57] The military potential for AI goes well beyond the identification of objects, however. For example, AI could be used for cybersecurity, for navigation, to create an unpredictable enemy in training events, for survey operations, for logistics, or for minesweeping.[58]

Most practically and in the near term, however, AI will probably only be used to augment human decision-making rather than acting truly autonomously.[59] Perhaps the rise of sentient killer robots is not upon us, but we are at the doorstep of a technological revolution made possible by the availability of enormous

54. *Id.*

55. *Id.*

56. The 2018 National Defense Strategy calls for the DoD to "invest broadly in military application of autonomy, artificial intelligence, and machine learning, including rapid application of commercial breakthroughs, to gain competitive military advantages." DEP'T. OF DEF., SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA 7 (2018), *available at* https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf [https://perma.cc/D5FA-WVT5]. The Defense Advanced Research Projects Agency (DARPA) has numerous initiatives related to artificial intelligence. DEF. ADVANCED RESEARCH PROJECTS AGENCY, INFORMATION INNOVATION OFFICE (I20), https://www.darpa.mil/about-us/offices/i2o [https://perma.cc/PC8J-XVZZ] (last visited Nov. 15, 2019). Each of the military services are forecasting increased investments in artificial intelligence in fiscal year 2019. *See* Brandon Knapp, *Here's Where the Pentagon Wants to Invest In Artificial Intelligence in 2019*, C4ISRNET (Feb. 16, 2018), https://www.c4isrnet.com/intel-geoint/2018/02/16/heres-where-the-pentagon-wants-to-invest-in-artificial-intelligence-in-2019/ [https://perma.cc/BHT3-FFR6].

57. Jonathan Vanian, *Defense Department Is Using Google's AI Tech to Help With Drone Surveillance*, FORTUNE (Mar. 6, 2018), http://fortune.com/2018/03/06/google-department-defense-drone-ai/ [https://perma.cc/DU7A-KZV2].

58. *See, e.g.*, U.S. GOV'T. ACCOUNTABILITY OFFICE, ARTIFICIAL INTELLIGENCE EMERGING OPPORTUNITIES, CHALLENGES, AND IMPLICATIONS (Mar. 2018); MITRE CORPORATION, PERSPECTIVES ON RESEARCH IN ARTIFICIAL INTELLIGENCE AND GENERAL ARTIFICIAL INTELLIGENCE RELEVANT TO DOD (Jan. 2017); Michael Melia, *Navy Tests Ocean Drones in RI's Narragansett Bay*, ASSOCIATED PRESS (Aug. 7, 2012), http://archive.boston.com/news/local/rhode_island/articles/2012/08/07/navy_tests_ocean_drones_in_ris_narragansett_bay/ [https://perma.cc/8GPG-EPEL].

59. Robert D. Hof, *Man and Machine*, MIT TECH. REV. (Mar. 28, 2016), https://www.technologyreview.com/s/600989/man-and-machine [https://perma.cc/EE7B-WEJS].

amounts of data, increased computing power, and large neural networks.[60] Although the concepts discussed here are relatively basic, a lawyer must have a firm grasp on fundamental terms, their common usage, and why AI matters now in order to help clients navigate the challenges posed by this emerging technology and remain in the ethical midfield. As will be discussed below, this will facilitate development of government policy and better inform engagement with programmers and those in the technology industry.

3. WHAT STANDARDS SHOULD APPLY?

Once terms are better defined, determining what standards should apply will further keep one's client in the ethical midfield. While determining standards for national security use of AI deserves fuller discussion than contemplated by this Article, three fundamental considerations are worth mentioning here: (1) accountability; (2) predictability; and (3) meaningful human control.

The Campaign to Stop Killer Robots and other humanitarian groups have argued that fully autonomous weapons should be outlawed, in part because no adequate system of accountability can be devised.[61] However, international law holds states and individuals responsible under the laws of armed conflict.[62] But even if one agrees with the position put forth by the Campaign to Stop Killer Robots, looking at AI for only lethal purposes through the lens of the law of armed conflict ignores (1) the vast scope of non-lethal national security applications of AI and (2) other potential avenues to render accountability.[63] For example, suppose a device powered by AI collects information on a U.S. person without a legal basis. Who should be held accountable? What if the Silicon Valley technology company that created the device guaranteed that the programming of the machine was such that it would never collect on a U.S. person? The

---

60. *See* Andrew Ng, *Introduction to Machine Learning: Lecture 1, Stan. Univ.*, CS229 Lecture (2011), https://see.stanford.edu/materials/aimlcs229/transcripts/MachineLearning-Lecture01.pdf [https://perma.cc/L8YR-7U7F].

61. Additionally, the United Nations Convention on Certain Conventional Weapons has convened on five occasions since 2014 to discuss lethal autonomous weapons. *See, e.g.*, CAMPAIGN TO STOP KILLER ROBOTS, https://www.stopkillerrobots.org/learn/#problem [https://perma.cc/ER7K-X692] (last visited Nov. 15, 2019); HUMAN RIGHTS WATCH, SHAKING THE FOUNDATIONS: THE HUMAN RIGHTS IMPLICATIONS OF KILLER ROBOTS, (May 12, 2014), https://www.hrw.org/report/2014/05/12/shaking-foundations/human-rights-implications-killer-robots [https://perma.cc/23QP-J842] (outlining several nations calling for a ban); Bonnie Docherty, *The Trouble with Killer Robots*, FOREIGN POL'Y (Nov. 19, 2012, 11:18 PM), http://foreignpolicy.com/2012/11/19/the-trouble-with-killer-robots [https://perma.cc/F883-QDDX].

62. For example, Common Article 1 to the 1949 Geneva Conventions states, "The High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances." *E.g.*, Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 1, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31. Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10 (2001); Edoardo Greppi, *The Evolution of Individual Criminal Responsibility Under International Law*, 81 INT'L REV. RED CROSS 531, 536–37 (1999).

63. *See* DUSTIN A. LEWIS ET AL., HARV. L. SCH. PROGRAM ON INT'L. L. AND ARMED CONFLICT, WAR-ALGORITHM ACCOUNTABILITY 51–82 (Aug. 2016).

company would not be liable under the rules pertaining to intelligence collection.[64] Should the company be held accountable under a products liability regime given that the algorithm did not behave as advertised?[65] Perhaps a broader understanding of accountability should be considered.

Second, the advancement of machine learning gives rise to concerns that decisions made by AI will be opaque and unpredictable.[66] While analysts can mathematically explain how algorithms optimize their objective functions, the complexity of the algorithms make it nearly impossible to describe this optimization in understandable and intuitive terms.[67] However, this butts up against notions of explainable and transparent decision-making in the national security space.[68] To illustrate the quandary, would it be advisable for a military commander to take lethal action on a conclusory finding of an intelligence analyst (whether human or artificial) that a hospital is fully controlled by the enemy if the analyst provided no rationale for reaching this conclusion? Most likely, conclusions reached by machines will be held to a higher standard than humans.[69] Accordingly, until the work product of AI is accepted in the international or intelligence community (which may take decades), either the computer's work must be validated by a human or the computer must be programmed to "show its work" when reaching a decision.[70]

Third, much of the debate surrounding national security use of AI concerns the level of meaningful human control over lethal weapons systems.[71] Human rights groups as well as some senior leaders in the Department of Defense have argued that decisions regarding life or death should never be ceded to a machine.[72]

---

64. *See, e.g.*, Exec. Order No. 12333, United States Intelligence Activities, 3 C.F.R. § 200 (1981); DEP'T OF DEFENSE, DIRECTIVE 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES (Aug. 8, 2016).

65. *See, e.g.*, RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 1 (AM. LAW INST. 1998).

66. John Danaher, *The Threat of Algocracy: Reality, Resistance and Accommodation*, 29 PHIL. & TECH. 245 (2016); Ed Felten, *Accountable Algorithms*, FREEDOM TO TINKER (Sept. 12, 2012), https://freedom-to-tinker.com/2012/09/12/accountable-algorithms/ [https://perma.cc/B9ED-NDKF].

67. Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO. L.J. 1147, 1207 (2017).

68. *See* THE WHITE HOUSE, REPORT ON THE LEGAL AND POLICY FRAMEWORKS GUIDING THE UNITED STATES' USE OF MILITARY FORCE AND RELATED NATIONAL SECURITY OPERATIONS (2016), at ii, *available at* https://www.justsecurity.org/wp-content/uploads/2016/12/framework.Report_Final.pdf [https://perma.cc/GT5Q-T9R6] (last visited Nov. 15, 2019).

69. *See* Karl Fezer, *The Moral Machine*, THE CODEX (Oct. 6, 2016), https://medium.com/thecodex.io/the-moral-machine-65b56f9b3681 [https://perma.cc/CRV9-QXWM] (noting that AI is going to be held to a higher standard than humans).

70. Defense Advanced Research Projects Agency is working on this very project by developing "explainable AI" in order to give the human operator more details about how the machine used deep learning to come up with the answer. DAVID GUNNING, DARPA, EXPLAINABLE ARTIFICIAL INTELLIGENCE (XAI) (2017), https://www.darpa.mil/attachments/XAIProgramUpdate.pdf [https://perma.cc/KCM8-5TQW].

71. *See, e.g.*, Alan L. Schuller, *At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law*, 8 HARV. NAT'L SEC. J. 379, 421 (2017).

72. *See The Problem*, CAMPAIGN TO STOP KILLER ROBOTS, https://www.stopkillerrobots.org/learn/ [https://perma.cc/ZF5T-8KDS] ("Fully autonomous weapons would decide who lives and dies, without further human intervention, which crosses a moral threshold.")

Current Department of Defense policy requires a certain level of supervision over autonomous systems, and software is programed with limits on the actions and decisions delegated to machines.[73] In other words, for now at least, autonomous weapon systems are unlikely to replace human judgment entirely. But, as technology develops, additional questions are raised. Does meaningful human control have to be geographically and temporally contemporaneous, or can meaningful human control stop at the programming phase?[74] Is it more acceptable to cede meaningful human control if the autonomous machine is used to do something *just short* of lethal action? If the technology reaches a point where a machine can *outperform* a human operator, thereby reducing civilian harm and suffering—arguably a fundamental goal of the law of armed conflict[75]—should law or policy still require meaningful human control?

The debate surrounding which standards to apply to national security uses of AI is multifaceted and complex. The previous three paragraphs only touch the surface on a few of the most relevant issues. Nevertheless, national security lawyers can help shape standards that comport with client desires while keeping proposed practices within prevailing understandings of law and policy. This may be accomplished best by staying engaged in the latest development of definitions, standards, and understandings of AI.

B. DISCOURAGE CLAIMS OF "LEGAL BLACK HOLES"

As national security use of AI is still developing and may seem novel, there could be claims of "policy voids" or "legal black holes."[76] National security lawyers can once again learn from the global war on terrorism and guide their client away from potential ethical pitfalls that could arise from the temptations offered by "legal black holes."

Upon capturing members of the Taliban, al Qaeda, and other enemy groups on the battlefields in Afghanistan and Iraq, the Bush administration had to find a place to detain and interrogate these "unlawful combatants."[77] According to

---

73. Dep't of Def., Directive 3000.09, Autonomy In Weapon Systems 4, 13-14 (Nov. 2, 2012), *available at* https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf?ver=2019-02-25-104306-377 [https://perma.cc/FAL5-HN3J] ("Autonomous weapons systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force.")

74. *See generally* Schuller, *supra* note 71, at 420 (arguing that international humanitarian law does not require temporally proximate human interaction with an autonomous weapons system prior to lethal kinetic action).

75. *See, e.g.*, Karima Bennoune, *Towards a Human Rights Approach to Armed Conflict: Iraq 2003*, 11 U.C. DAVIS J. INT'L L. & POL'Y 171, 180 (2004).

76. Consider, for example, cyberspace. "Cyberspace is not a 'law-free' zone where anyone can conduct hostile activities without rules or restraint . . . . To be sure, new technologies raise new issues and thus new questions . . . . But to those who say that established law is not up to the task, we must articulate and build consensus around how it applies and reassess from there whether and what additional understandings are needed." Harold Hongju Koh, *International Law in Cyberspace*, 54 HARVARD INT'L L.J.1, 3 (2012).

77. *See* Kermit Roosevelt, *Why Guantánamo?*, THE JURIST (Oct. 5, 2006, 8:01 AM), https://www.jurist.org/commentary/2006/10/why-guantanamo/ [https://perma.cc/JLZ9-98GK].

government officials at the time, a prison on the U.S. naval base in Guántanamo Bay, Cuba, located outside of the territorial United States, provided a perfect venue.[78] The American military's presence in Guántanamo is based on a lease entered into with the Cuban government in 1903, pursuant to which the United States is granted "complete jurisdiction and control" within the naval base without Cuba ceding sovereignty.[79] This arrangement created a so-called "legal black hole," where it was unclear which legal regime should govern, enabling the U.S. government to argue that neither the U.S. Constitution nor Common Article 3 of the Geneva Convention applied.[80] Accordingly, the argument went, the U.S. government could "do whatever they want[ed]."[81]

Over time, the shortcomings of the "legal black hole" claim became clear, most notably in the U.S. Supreme Court.[82] In a succession of legal opinions, the Court has progressively determined that the law applies even in a place as peculiar as Guantánamo.[83] For example, the Court found that federal courts have jurisdiction over Guantánamo detainees, and that such detainees are entitled to some due process, habeas corpus, and other procedural protections required by customary international law.[84] Collectively, these decisions eroded the Bush administration's assertions of unilateral detention authority and damaged the administration's political credibility at home and abroad.

The United States government experience at Guantánamo Bay shows the fallacy of the legal "black hole" argument. Just because a new technology or technique is utilized to perform an existing task, it does not mean that a whole new

---

78. In late 2001, Department of Justice officials concluded "that the great weight of legal authority indicate[d] that a federal district court could not properly exercise habeas jurisdiction over an alien detained" at Guantánamo Bay. THE TORTURE PAPERS: THE ROAD TO ABU GHRAIB 29 (KAREN J. GREENBERG & JOSHUA L. DRATEL EDS., 2005).

79. Lease of Lands for Coaling and Naval Stations, U.S.-Cuba, art. III, Feb. 23, 1903, T.S. No. 418. In a subsequent treaty, the governments agreed the lease would run for as long as the U.S. government remained at Guantánamo, unless the parties agree otherwise. Treaty Defining Relations with Cuba, U.S.-Cuba, art. III, May 29, 1934, 48 Stat. 1683.

80. *See* Ernesto Hernández-López, *Guantánamo as a 'Legal Black Hole': A Base for Expanding Space, Markets, and Culture*, 45 U.S.F. L. REV. 141, 143 (2010); Gerald L. Neuman, *Closing the Guantánamo Loophole*, 50 LOY. L. REV. 1, 3 (2004); Johan Steyn, *Guantánamo Bay: The Legal Black Hole*, 53 INT'L & COMP. L.Q. 1, 1 (2004).

81. *See Countdown with Keith Olbermann* (MSNBC television broadcast June 22, 2007) (statement of Prof. Neal Katyal, Salim Hamdan's attorney) (transcript available at http://www.nbcnews.com/id/19415786/ns/msnbc-countdown_with_keith_olbermann/t/countdown-keith-olbermann-june/#.VNVdS1PF_lQ [https://perma.cc/Y9UH-BE6P]) ("[T]he administration's argument is that Guantánamo is a legal black hole where they can do whatever they want . . . . These people have no rights whatsoever.").

82. *See*, *e.g.*, Boumediene v. Bush, 553 U.S. 723, 792 (2008); Hamdan v. Rumsfeld, 548 U.S. 557, 635 (2006); Rasul v. Bush, 542 U.S. 466, 473 (2004); Hamdi v. Rumsfeld, 542 U.S. 507, 529 (2004).

83. *See*, *e.g.*, *Boumediene*, 553 U.S. at 792–93; *Hamdan*, 548 U.S. at 567, 594–95, 624–25, 635; *Rasul*, 542 U.S. at 473; *Hamdi*, 542 U.S. at 529–33.

84. *See Boumediene*, 553 U.S. at 792–93 (finding all Guantánamo prisoners have a right to habeas corpus); *Hamdan*, 548 U.S. at 567, 594–95, 624–25 (finding military commissions violated federal law and treaties); *Rasul*, 542 U.S. at 473 (finding federal courts have jurisdiction to consider the legality of foreign nationals captured overseas); *Hamdi*, 542 U.S. at 533 (finding detainees who are U.S. citizens have due process rights).

system of laws or regulations needs to be in place to inform legality or guide behavior. National security lawyers should remember that AI is merely *a technique* used to do something and as such, a full range of established laws, regulations, and rules still apply. To illustrate, novel AI techniques might enable the gathering and analysis of intelligence at unprecedented volume and precision. Nevertheless, the U.S. Constitution, Executive Order 12333, and the Department of Defense intelligence oversight manual still govern the intelligence collection process.[85] Simply put, AI is a means to an end, not an end itself. In order to remain in the ethical midfield, national security lawyers should focus on what their clients seek to *do* as much as the technology their clients seek to *use*.[86]

While there may be some apparent gaps or ambiguities in law or policy when applied to AI, being seduced by the fallacy of a legal black hole could subject national security decision-makers to strategic risk and hurt credibility at home and abroad, as was the case with Guántanamo detainees. To remain in the ethical midfield, national security lawyers should navigate their clients away from so-called legal black holes and find solutions that are most informed by existing (and anticipated) law and policy.

C. TELL THE EMPEROR HE HAS NO CLOTHES

In Hans Christian Andersen's fairytale, *The Emperor's New Clothes*, two weavers promised the emperor a suit that would be invisible to those who are "stupid or unfit for their office"[87] When the emperor paraded around the town in his new clothes, no one admitted that they could not see the clothes until a child cried out, "But he has nothing on!"[88]

There were several instances in the Bush administration when a national security lawyer should have cried out "[b]ut he has nothing on!"[89] Lawyers were often the first to be consulted, sometimes even before top-level subject matter experts.[90] In these instances, the client often transferred their decision-making power to the

---

85. *See generally* U.S. CONST.; Exec. Order No. 12333, 3 C.F.R. § 200 (1981); DEP'T OF DEFENSE, DIRECTIVE 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES (Aug. 8, 2016).

86. In using cyber techniques, for example, national security lawyers must focus on the distinct laws or rules that might govern the means (i.e., rules governing the use of computers or cyberspace for the primary purpose of achieving objectives and effects in or through cyberspace) as well as the ends (e.g., the principles of the law of armed conflict in the event of certain cyber attacks). OFFICE OF GEN. COUNSEL, DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL 1003–4 (2015 & Supp. Dec. 2016).

87. HANS CHRISTIAN ANDERSEN, HANS ANDERSEN'S FAIRY TALES: THE UGLY DUCKLING, THUMBELINA, AND OTHER STORIES 312 (2016).

88. *Id*. at 314.

89. According to Professor Jack Goldsmith, a national security lawyer is often "criticized for being too cautious, for putting on the brakes, for playing it safe in a dangerous world that cannot afford such risk aversion. But he is in the same breath cautioned to give 'sound, accurate' legal advice within the 'confines' of the law. It is often impossible to do both." GOLDSMITH, *supra* note 8, at 92.

90. Gabriella Blum, *The Role of the Client: The President's Role in Government Lawyering*, 32 B.C. INT'L & COMP. L. REV. 275, 286 (2009).

lawyers, thus shirking their responsibility.[91] Compounding the problem is that oftentimes national security lawyers are pressured by their clients to "get to yes" in the name of national security.[92] Particularly when the client is a high ranking official like the President, a cabinet member, or a four-star general, the motivation and pressure, to please the client only increases. As witnessed in the war on terrorism, such temptations can swiftly lead an attorney and his or her clients to stray from the ethical midfield.

The warrantless wiretapping "hospital room showdown" is the stuff of legend.[93] In 2004, the Bush administration was engaged in a broad program of warrantless surveillance without securing congressional approval.[94] The Justice Department's certification of the program was set to expire.[95] At the time, Attorney General John Ashcroft was in the hospital and therefore unable to act on the matter.[96] Although Mr. Ashcroft and other high-ranking officials at the Department of Justice intended to discontinue the surveillance, White House Counsel Alberto Gonzales and President Bush's Chief of Staff Andrew Card went to Mr. Ashcroft's hospital room to get his signature on a document approving the continuation of the program.[97]

Upon learning of their plan, Deputy Attorney General James Comey went to the hospital to confront Gonzales and Card.[98] Mr. Ashcroft told Mr. Gonzales and Mr. Card that Mr. Comey was serving as acting attorney general, and therefore, only Mr. Comey could approve the continuation.[99] The next day, terrorist bombs killed more than 200 train passengers in Madrid, galvanizing the White House to reauthorize the continuation of the warrantless surveillance program without the blessing of the Justice Department.[100] Mr. Comey and others in the Justice

---

91. *Id*. at 286–87.

92. GOLDSMITH, *supra* note 8, at 38.

93. Dan Eggen & Paul Kane, *Gonzales Hospital Episode Detailed, Ailing Ashcroft Pressured on Spy Program, Former Deputy Says*, WASH. POST, May 16, 2007, at A01; David Stout, *Gonzales Pressed Ailing Ashcroft on Spy Plan, Aide Says*, N.Y. TIMES (May 15, 2007), http://www.nytimes.com/2007/05/15/washington/15cnd-attorneys.html [https://perma.cc/7PTM-ZXMJ]; Andrew Zajac & Mark Silva, *Ashcroft Ex-Aide Details Wiretap Infighting, Gonzales Prodded Hospitalized Official*, CHI. TRIBUNE (May 16, 2007), https://www.chicagotribune.com/news/ct-xpm-2007-05-16-0705151141-story.html [https://perma.cc/T2QG-CU9D].

94. Eggen & Kane, *supra* note 93; David Stout, *supra* note 93; Zajac & Silva, *supra* note 93.

95. *Preserving Prosecutorial Independence: Is the Department of Justice Politicizing the Hiring and Firing of U.S. Attorneys? - Part IV: Hearing Before the S. Judiciary Comm.*, 110th Cong. 213–40 (2007) [hereinafter Comey Testimony] (statement of James Comey).

96. *See* Daniel Klaidman et al., *Palace Revolt: They Were Loyal Conservatives, and Bush Appointees. They Fought a Quiet Battle to Rein in the President's Power in the War on Terror. And They Paid a Price for It. A Newsweek Investigation*, NEWSWEEK, Feb. 6, 2006, at 34, 39.

97. *See* Comey Testimony, *supra* note 95.

98. *Id*.

99. *Id*.

100. *The Frontline Interview with Alberto Gonzales*, PBS BROADCASTING (Mar. 3, 2014), http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-alberto-gonzales [https://perma.cc/U8GC-822C].

Department responded by submitting their resignation, which led to President Bush holding individual meetings with Mr. Comey and Robert Mueller, then-Director of the Federal Bureau of Investigation.[101] After the meetings, President Bush directed the program be brought into compliance with the law.[102] Mr. Comey got the impression that President Bush was not even aware that the program was, at best, on the fringes of the law.[103] In other words, none of the President's closest advisers had told the emperor he wasn't wearing anything at all.

The ethical problems related to warrantless surveillance and other national security programs during the Bush administration can be attributed to attorneys overzealously seeking to fulfill the desires of the individual "client."[104] This caused the attorneys to provide idiosyncratic advice reflecting the perceived desires of a specific individual within an organization. [105] To remain in the ethical midfield, a national security lawyer must educate the client on mainstream understandings of the law, and if the legal basis for a particular program is on the fringes of the law, national security lawyers have a duty to tell that to the client. Furthermore, lawyers and staff must not accept risk on behalf of decision-makers, without the decision-makers' knowledge. The U.S. Department of Justice's Office of Professional Responsibility concluded that the national security attorneys involved in these programs prioritized their "desire to accommodate the client above [their] obligations to provide thorough, objective, and candid legal advice . . . ."[106]

The *Model Rules of Professional Conduct* are helpful here.[107] First, a national security lawyer must remember that a lawyer employed by an organization represents *the organization*, not individual members of the organization, no matter the individual's rank or position.[108] As such, a lawyer is required to take action to prevent violations of law that "reasonably might be imputed to the organization,

---

101. *See* Comey Testimony, *supra* note 95, at 219–20. According to Mr. Comey: "The program was reauthorized without us, without a signature from the Department of Justice attesting as to its legality. And I prepared a letter of resignation intending to resign the next day, Friday, March the 12th . . . . I believed that I couldn't—I couldn't stay if the administration was going to engage in conduct that the Department of Justice had said had no legal basis. I just simply couldn't stay." *Id*. at 218–19.

102. *See* OFFICE OF INSPECTORS GENERAL, DEP'TS OF DEFENSE, JUSTICE, CIA, NSA, AND OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM at 28 (July 10, 2009). The government has not fully disclosed what changes were made to the program. *See* Eggen & Kane, *supra* note 93.

103. *See* BARTON GELLMAN, ANGLER: THE CHANEY VICE PRESIDENCY 318–20 (2006).

104. *See* GABRIELLA BLUM & PHILIP B. HEYMANN, LAWS, OUTLAWS AND TERRORISTS: LESSONS FROM THE WAR ON TERRORISM 54–56 (2010).

105. *See id.*

106. DEP'T OF JUSTICE, OFFICE OF PROF'L RESPONSIBILITY, INVESTIGATION INTO THE OFFICE OF LEGAL COUNSEL'S MEMORANDA CONCERNING ISSUES RELATING TO THE CENTRAL INTELLIGENCE AGENCY'S USE OF "ENHANCED INTERROGATION TECHNIQUES" ON SUSPECTED TERRORISTS 198, 254 (2009); *see* MODEL RULES OF PROF'L CONDUCT R. 1.13(b) (2018) [hereinafter MODEL RULES].

107. *See generally* MODEL RULES.

108. MODEL RULES R. 1.13.

and that is likely to result in substantial injury to the organization."[109] Second, a national security lawyer must "exercise independent professional judgment and render candid advice" and in doing so, it is within such lawyer's purview to give consideration to relevant "moral, economic, social and political factors" to inform the client of ethical boundaries.[110] Third, particularly in the national security space, lawyers must be mindful of the allocation of authority between lawyer and client: decisions concerning objectives and acceptance of risk ultimately rest with the client.[111]

Beyond looking at the *Model Rules*, remaining in the ethical midfield when advising high ranking officials often requires a great deal of moral courage. It is not easy to look powerful generals or political officials in the eye and tell them that what they want to do may fall outside the law. As discussed in greater detail below, the AI revolution will provide ample opportunity for national security lawyers to tell the emperor he has no clothes. To remain in the ethical midfield, national security lawyers must overcome any fears of being thought of as "unfit for their positions, stupid, or incompetent"[112] and have the moral courage to provide candid advice regardless of how that advice might impact one's career or standing within the organization.

II. WORKING WITH INDUSTRY

"Don't be evil." – Google Code of Conduct[113]

"Wouldn't it be cool if you could shoot somebody in the face at 200 kilometers and they don't even know you're there? That's the kind of man-machine teaming we really want to get after."

—Former Vice Chairman of the Joint Chiefs of Staff [114]

In the early 19th century, after securing its independence from European powers, the United States looked to leverage the vast resources of the land

109. MODEL RULES R. 1.13(b).

110. MODEL RULES R. 2.1.

111. MODEL RULES R. 1.2(a) ("[A] lawyer shall abide by a client's decisions concerning the objectives of representation and . . . shall consult with the client as to the means by which they are to be pursued."); *see also* Charles W. Wolfram, *Toward a History of the Legalization of American Legal Ethics-II The Modern Era*, 15 GEO. J. LEGAL ETHICS 205, 210 (2002) (describing client-centric lawyering as "the bedrock of modern professional orthodoxy"); Blum, *supra* note 90, at 286.

112. ANDERSEN, *supra* note 87.

113. *See Code of Conduct*, GOOGLE INVESTOR RELATIONS, https://web.archive.org/web/20100419172019/https://investor.google.com/corporate/code-of-conduct.html [https://perma.cc/6VPU-6WFT] (last updated Apr. 8, 2009).

114. Aaron Mehta, *Selva: FY19 Budget Sees "Increasing" Investments in AI, Machine Teaming*, DEFENSE NEWS (Jan. 30, 2018), https://www.defensenews.com/congress/budget/2018/01/30/selva-fy19-budget-sees-increasing-investments-in-ai-machine-teaming/ [https://perma.cc/3QDN-QUSQ] (quoting Vice Chairman of the Joint Chiefs of Staff, General Paul Selva).

westward of the original thirteen colonies.[115] But before the territory could be settled, the West first needed to be explored and secured.[116] Starting with the Lewis and Clark Expedition, and followed by military settlements emplaced to protect transportation junctions and resources, the government set the conditions for industry to develop and enjoy the spoils of the transcontinental railroad.[117] Similarly, we are entering the age of commercial exploitation of outer space, which was only made possible because of the government's initial role in exploration and resource investment.[118] In both the creation of the transcontinental railroad and space exploration, the government's leading role in investment enabled it to develop legal regimes and standards ahead of the involvement of commercial actors.[119]

In AI, this situation is reversed and, accordingly, the U.S. government is in a lagging position to shape the development of law and regulation.[120] The U.S. military is also a latecomer to the AI revolution, and government spending on AI is dwarfed by the private industry.[121] According to one practitioner, "unless there is a cataclysmic event on the scale of World War II, it is unlikely that the public appetite for massive government spending on artificial intelligence projects will materialize."[122] Thus, the Department of Defense must rely upon the innovation and investment of the private sector to reap the full benefits of this emerging technology and compete with great power adversaries.

During a September 2017 trip to Silicon Valley, Former Secretary of Defense Mattis remarked that AI has "got to be better integrated by the DoD" in order to

---

115. Jerry Hendrix & Adam Roth, *A Space Policy for the Trump Administration*, CENTER FOR A NEW AMERICAN SECURITY 1 (2017), https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-SpacePolicy-Final5.pdf?mtime=20171023151800 [https://perma.cc/2EQ9-MMX9].

116. *Id*. at 4.

117. *Id*. at 1.

118. *Id*. at 3; *see also* U.S. Commercial Space Launch Competitiveness Act, Pub. L. No. 114-90, 129 Stat. 704 (2015); Spurring Private Aerospace Competitiveness and Entrepreneurship Act of 2015, H.R. Rep. No. 114-119, at 22 (May 18, 2015).

119. Most of the foundational international laws governing space predated commercial space activities. *See, e.g*., Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, opened for signature Dec. 18, 1979, 1363 U.N.T.S. 3; Convention on Registration of Objects Launched into Outer Space, opened for signature Jan. 14, 1975, 28 U.S.T. 695, 1023 U.N.T.S. 15); Convention on International Liability for Damage Caused by Space Objects, opened for signature March 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187; Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, opened for signature Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N. T.S. 205. Similarly, government investment gave way to laws which secured the government use of privately-operated railroads for postal, military, and other purposes. *See, e.g*., Pacific Railroad Act of July 1, 1862, ch. 120, 12 Stat. 489, amended by ch. 216, 13 Stat. 356 (1864).

120. Stew Magnuson, *DoD Making Big Push to Catch Up on Artificial Intelligence*, NATIONAL DEFENSE (Jun. 13, 2017), http://www.nationaldefensemagazine.org/articles/2017/6/13/dod-making-big-push-to-catch-up-on-artificial-intelligence [https://perma.cc/EN3P-FXXJ].

121. *Id*.

122. Scherer, *supra* note 27, at 376.

compete in the era Great Power Competition.[123] Indeed, to fully leverage the benefits of AI and remain a global military leader, the Department of Defense must make substantial investments in this technology and leverage the expertise of Silicon Valley by opening broad channels of communications.[124] And so, it seems that the fate of United States national security could be more dependent than ever on the private sector. Of course, as the U.S. military has learned time and again throughout its history, reliance on the private sector has its challenges.[125]

President Eisenhower warned of unwarranted influence from private industry in the Department of Defense.[126] The relationship that the Department of Defense must nurture with Silicon Valley today, however, is more complex than previous partnerships between government and industry. In addition to cultural differences, Silicon Valley companies are not dependent on the government to stay in business like most companies in the Defense Industrial Base.[127]

To share ideas and mutually shape behavior in the interests of national security, the Department of Defense must recognize and leverage Silicon Valley's

---

123. Robert W. Button, *Artificial Intelligence and the Military*, REAL CLEAR DEFENSE (Sept. 7, 2017), https://www.realcleardefense.com/articles/2017/09/07/artificial_intelligence_and_the_military_112240.html [https://perma.cc/BCR8-3243].

124. Robert Work, who served as the Deputy Secretary of Defense during the Obama Administration, warned "the U.S. military can either lead the coming revolution, or fall victim to it." Sintia Radu, *The Future of War May Be Virtual*, U.S. NEWS (Mar. 20, 2018), https://www.usnews.com/news/best-countries/articles/2018-03-20/the-us-military-wants-to-lead-the-innovation-game-in-vr [https://perma.cc/E2YE-88AK]. According to Eric Schmidt, former chairman of the Defense Innovation Board, "[a]rtificial intelligence is the new frontier, and the Defense Department must invest in this breakthrough or be in danger of not being competitive in the future." Jim Garamone, *America in Danger of Losing Lead in AI, Innovation Board Chair Says*, DEP'T OF DEFENSE NEWS (Nov. 1, 2017), https://www.defense.gov/News/Article/Article/1360302/america-in-danger-of-losing-lead-in-ai-innovation-board-chair-says/ [https://perma.cc/TG3H-WDZD].

125. *See, e.g.*, Dwight D. Eisenhower, Farewell Address (Jan. 17, 1961), *available at* https://www.ourdocuments.gov/doc.php?flash=false&doc=90&page=transcript [https://perma.cc/7CUF-DKTZ]; Michael J. Trebilcock & Edward M. Iacobucci, *Privatization and Accountability*, 116 HARV. L. REV. 1422, 1444 (2003); Spencer Ante, *The Other U.S. Military*, BUS. WK., May 31, 2004, at 76; David Barstow, et al., *Security Companies: Shadow Soldiers in Iraq*, N.Y. TIMES, Apr. 19, 2004, at A1; James Dao, *Private Guards Take Big Risks, for Right Price*, N.Y. TIMES, Apr. 2, 2004, at A1; Seymour M. Hersh, *Chain of Command: How the Department of Defense Mishandled the Disaster at Abu Ghraib*, NEW YORKER, May 17, 2004, at 38; Kenneth Bredemeier, *Thousands of Private Contractors Support U.S. Forces in Persian Gulf*, WASH. POST, Mar. 3, 2003, at E1; Kathleen Day, *In Haiti, Covering the Bases: Pentagon Cuts Give Private Firms Opportunity To Provide Services to Military*, WASH. POST, Sept. 23, 1994, at D1; Anthony Faiola & Scott Wilson, *U.S. Took Risks in Aiding Peru's Anti-Drug Patrols*, WASH. POST, Apr. 29, 2001, at A1; Juan Forero, *Role of U.S. Companies in Colombia Is Questione*d, N.Y. TIMES, May 18, 2001, at A3; Bradley Graham, *Ex-GIs Work To Give Bosnian Force a Fighting Chance*, WASH. POST, Jan. 29, 1997, at A1.

126. *See* Eisenhower, *supra* note 125. The business of Silicon Valley is far different from the defense industrial business envisioned by Eisenhower. "[W]e must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist." *Id.*

127. *See* Linell A. Letendre, *Google. . .It Ain't Ford: Why the United States Needs a Better Approach to Leveraging the Robotics Industry*, 77 A.F. L. REV. 51, 56–57 (2017). Google alone is worth over twice the sum of the entire Defense Industrial Base, with the purchasing power to buy any traditional defense firm with on-hand cash. Furthermore, the combined research and development investments for the top five defense companies is less than half of Google's annual R&D. *Id.*

expertise while also acknowledging the potential pitfalls of working with an industry motivated primarily by profit.[128] First, the Department of Defense should carefully consider the warnings of the dangers of AI from tech industry leaders. Second, national security lawyers should recognize the risks of working with industry while also working to understand and assuage the tech industry's concerns about working with the Department of Defense.

A. IDENTIFY LEGITIMATE "CASSANDRAS"

> "By far, the greatest danger of Artificial Intelligence is that people conclude too early that they understand it."[129]
>
> —Devansh Lala

In a January 2015 open letter, Stephen Hawking, Steve Wozniak, Elon Musk, and other tech luminaries warned of the existential threats posed by AI.[130] In separate communications, Mr. Hawking, Mr. Wozniak, and Mr. Musk all prophesized that AI could spell the end of the human race.[131] Mr. Musk ominously predicted that we are "summoning a demon," and proposed greater federal government regulation and international oversight "just to make sure that we don't do something very foolish."[132]

In Greek mythology, Apollo, the god of war, gifted Cassandra with the ability to tell the future.[133] But when Cassandra rebuffed Apollo's romantic advances, Apollo cursed Cassandra, ensuring that her prophecies would not be believed.[134] Cassandra was left with the ability to predict tragic events, but was helpless to do

---

128. *See, e.g.*, U.S. Gov't Accountability Office, GAO-17-291, DEFENSE CONTRACTING: DOD Needs Better Information on Incentive Outcomes (2017), *available at* https://www.gao.gov/assets/690/685723.pdf [https://perma.cc/7BHB-UWLV]; Dan Briody, THE HALLIBURTON AGENDA: THE POLITICS OF OIL AND MONEY (2004).

129. Devansh Lala, *Artificial Intelligence: Understanding the Hype*, TOWARDS DATA SCIENCE (Jun. 22, 2017), https://towardsdatascience.com/artificial-intelligence-understanding-the-hype-daee0df04695 [https://perma.cc/FS6J-243Z].

130. *See* Open Letter, Autonomous Weapons: An Open Letter from AI & Robotics Researchers (July 28, 2015), https://futureoflife.org/open-letter-autonomous-weapons/ [https://perma.cc/Q44V-L6XJ].

131. *See* Rory Cellan-Jones, *Stephen Hawking Warns Artificial Intelligence Could End Mankind*, BBC NEWS, Dec. 2, 2014, http://www.bbc.com/news/technology-30290540 [https://perma.cc/MGM2-8VWF]; Peter Holley, *Apple Co-Founder on Artificial Intelligence: "The Future Is Scary and Very Bad for People,"* WASH. POST (Mar. 24, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/03/24/apple-co-founder-on-artificial-intelligence-the-future-is-scary-and-very-bad-for-people/) [https://perma.cc/9ECY-6F86] ("If we build these devices to take care of everything for us, eventually they'll think faster than us and they'll get rid of the slow humans to run companies more efficiently."); Samuel Gibbs, *Elon Musk: Artificial Intelligence Is Our Biggest Existential Threat*, GUARDIAN (Oct. 27, 2014), http://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat [https://perma.cc/2PGF-QLUX].

132. Greg Kumparak, *Elon Musk Compares Building Artificial Intelligence to "Summoning the Demon,"* TECHCRUNCH (Oct. 26, 2014), https://techcrunch.com/2014/10/26/elon-musk-compares-building-artificial-intelligence-to-summoning-the-demon/ [https://perma.cc/NY7R-ZNGR].

133. EDITH HAMILTON, MYTHOLOGY 292 (1942).

134. *Id.*

anything to stop them.[135] In their book, *Warnings: Finding Cassandras to Stop Catastrophes*, Richard A. Clarke and R.P. Eddy attempt to detect "a real Cassandra among the myriad of pundits" by investigating the experts who warn of future disasters, genetic engineering, giant meteor strikes, and other potentially emergent threats today.[136]

One of the experts featured in *Warnings*, Eliezer Yudkowsky of the Machine Intelligence Research Institute, examines AI.[137] According to Yudkowsky, once AI is able to reprogram itself, it will be too late to implement safeguards.[138] Yudkowsky believes that "fear, greed, biases, and national security priorities" will trump any exercise of caution.[139] Yudkowsky proposes a global Manhattan Project dedicated to the safe and ethical development of AI "[b]efore we open a door we can never again close."[140]

Leaders in government and industry have been quick to dismiss the aforementioned fears surrounding AI, categorizing these concerns as exaggerated or uninformed.[141] But, in light of the Department of Defense's mandate to remain in the ethical midfield, perhaps we should not be so quick to ignore these trepidations. Even though Mr. Musk and Mr. Wozniak do not serve in government, their stature in the technology industry demands that the issues they raise be given careful consideration. Considering that leaders in the private sector—who stand to profit most from the AI boom—are the ones calling for *greater* regulation over its development, perhaps national security lawyers should listen to their concerns.[142]

In the global war on terrorism, the U.S. government failed to listen to Cassandras to the detriment of national security. In 2011, President Obama withdrew all troops from Iraq—despite the protests of some civilian advisers and military commanders—leading to the rise of the Islamic State of Iraq and Syria (ISIS).[143] This is also discussed in *Warnings*, where the former U.S. ambassador to Syria, Robert Ford, is identified as a Cassandra for advocating for the support

---

135. *Id*.

136. *See* RICHARD A. CLARKE & R.P. EDDY, WARNINGS: FINDING CASSANDRAS TO STOP CATASTROPHES 5 (2017).

137. *Id*. at 202.

138. *See id*. at 205.

139. *Id*. at 207.

140. *Id*. at 216.

141. *See, e.g*., Tom Simonite, *Elon Musk's Freak-Out over Killer Robots Distracts from Our Real AI Problems*, WIRED (July 17, 2017), https://www.wired.com/story/elon-forget-killer-robots-focus-on-the-real-ai-problems/ [https://perma.cc/B6QM-VRUZ].

142. *See* Natalia Kukushkina, *How Facebook, Apple, Microsoft, Google, and Amazon Are Investing in AI*, HACKERNOON (May 28, 2019), https://hackernoon.com/how-facebook-apple-microsoft-google-and-amazon-are-investing-in-ai-f58b5706e34a [https://perma.cc/WH4P-6ZEN]; Open Letter, Autonomous Weapons: An Open Letter from AI & Robotics Researchers (July 28, 2015), https://futureoflife.org/open-letter-autonomous-weapons/ [https://perma.cc/Q44V-L6XJ]; Holley, *supra* note 131; Gibbs, *supra* note 131; Kumparak, *supra* note 132.

143. *See, e.g*., Rebecca Kaplan, *Leon Panetta Criticizes Obama for Iraq Withdrawal*, CBS NEWS (Oct. 2, 2014), https://www.cbsnews.com/news/leon-panetta-criticizes-obama-for-iraq-withdrawal/ [https://perma.cc/HTU7-DHPJ].

of the moderate Syrian opposition, which may have curbed the spread of ISIS.[144] Despite Ambassador Ford's status as the Foreign Service's leading expert on Arab affairs, his recommendations were met with resistance by the Obama administration.[145] The failure to identify this legitimate Cassandra led to the rise of a determined and resistant enemy that still plagues the United States to this day.[146]

Dr. Hawking warned that AI is "likely to be either the best or worst thing ever to happen to humanity, so there's huge value in getting it right."[147] Getting it right starts with finding and remaining in the ethical midfield. National security lawyers can again look to the *Model Rules* for guidance. Rule 1.1 requires a lawyer to "provide competent representation."[148] To comply with this duty of competence in the AI space, a lawyer must stay abreast of changes in technology.[149] This, of course, is easier said than done with the rapid advancement in technologies observed recently. National security lawyers must engage with technical experts in the industry to have both awareness and understanding to keep pace with technological trends in order to provide the best legal advice. This may be accomplished by attending conferences, reviewing trade publications, or partaking in regular dialogue with industry experts. Perhaps in the future, the Department of Defense could routinely include attorneys in the Training With Industry Program, where DoD personnel are assigned to for-profit private sector organizations in professional, technical, or executive management areas.[150]

B. BEWARE OF SNAKE OIL SALESMEN

Snake oil salesmen were pervasive throughout the American West in the 1800s, selling dubious medicines with exaggerated marketing hype.[151] As often

---

144. CLARKE & EDDY, *supra* note 136, at 70.

145. *See id*. at 73.

146. *See, e.g*., Liz Sly & Zakaria Zakaria, *With ISIS striking back in Syria, a U.S. withdrawal would be a 'disaster,' Kurds warn*, WASH. POST (Apr. 5, 2018), https://www.washingtonpost.com/world/syrian-kurds-warn-of-a-disaster-if-us-troops-leave/2018/04/05/0b5619e0-386e-11e8-af3c-2123715f78df_story.html?utm_term=.ba9630e1a5a8 [https://perma.cc/H2GD-49FB] (noting that ISIS is showing signs of renewed strength).

147. Andrew Griffin, *Stephen Hawking: Artificial Intelligence Could Wipe Out Humanity When It Gets Too Clever As Humans Will Be Like Ants*, THE INDEPENDENT (Oct. 8, 2015), https://www.independent.co.uk/life-style/gadgets-and-tech/news/stephen-hawking-artificial-intelligence-could-wipe-out-humanity-when-it-gets-too-clever-as-humans-a6686496.html [https://perma.cc/2GNX-LBRP].

148. MODEL RULES R. 1.1.

149. *See id*. "Competent representation" is defined as "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." *Id*. "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." MODEL RULES R. 1.1 cmt. 8 (emphasis added).

150. DEP'T OF DEF., INSTRUCTION NO. 1322.06, FELLOWSHIPS, LEGISLATIVE FELLOWSHIPS, INTERNSHIPS, SCHOLARSHIPS, TRAINING-WITH-INDUSTRY (TWI), AND GRANTS PROVIDED TO DOD OR DOD PERSONNEL FOR EDUCATION AND TRAINING (2016), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/132206p.pdf [https://perma.cc/9ZAX-7PMP] (last visited Oct. 19, 2019).

151. *See* Lakshmi Gandhi, *A History of "Snake Oil Salesmen,"* NPR (Aug. 26, 2013), https://www.npr.org/sections/codeswitch/2013/08/26/215761377/a-history-of-snake-oil-salesmen [https://perma.cc/7XJU-NDWH].

depicted in Western movies, the snake oil salesmen would leave town before their customers realized the products they bought were worthless.[152] The fervor surrounding AI in the tech industry—and now government—has spawned many modern snake oil salesmen.

Much of the rise of AI in the tech industry can be attributed to mere speculation and buzz rather than actual scientific advancement. Because "artificial intelligence" and related terms like "deep learning" and "machine learning" are poorly understood and defined, companies can create an impression of competence and promote "intelligent" capabilities.[153] According to Oren Etzioni, CEO of the Allen Institute for Artificial Intelligence, "IBM Watson is the Donald Trump of the AI industry—outlandish claims that aren't backed by credible data. Everyone—journalists included—knows that the emperor has no clothes, but most are reluctant to say so."[154] To remain in the ethical midfield when engaging with industry, attorneys should help their clients realize that AI is not some magical elixir that can solve every problem. For example, deep learning typically requires large data sets for training, which few actors have amassed or can access, and it takes extensive processing power to train and run a neural network.

The United States government learned some hard lessons by working with industry in combat zones overseas. Since September 11, 2001, the U.S. government has increasingly turned to private military companies (PMCs) to fulfill staffing shortfalls caused by the increased demands of the military in the Middle East.[155] Although the United States has employed PMCs throughout history, reliance on their use ballooned during the reconstruction efforts in Afghanistan and Iraq.[156] But unlike the support roles that contractors traditionally filled, the roles

---

152. *See* Chip Hines, *The Medicine Show Syndrome—Are We Guilty?*, ON PASTURE (Jan. 13, 2014), https://onpasture.com/2014/01/13/the-medicine-show-syndrome-are-we-guilty/ [https://perma.cc/L68Z-CKAZ].

153. *See, e.g.*, Jennings Brown, *Why Everyone Is Hating on IBM Watson—Including the People Who Helped Make It*, GIZMODO (Aug. 10, 2017), https://gizmodo.com/why-everyone-is-hating-on-watson-including-the-people-w-1797510888 [https://perma.cc/ML73-KX9F].

154. *Id.*

155. *See* Dana Priest & William M. Arkin, *Top Secret America: National Security Inc.*, WASH. POST, July 20, 2010, *reprinted in* Global Policy Forum (July 20, 2010), https://www.globalpolicy.org/pmscs/50502-top-secret-america-national-security-inc.html [https://perma.cc/4HPV-NQSR].

156. *See* JENNIFER K. ELSEA & NINA M. SERAFINO, CONG. RESEARCH SERV., RL32419, PRIVATE SECURITY CONTRACTORS IN IRAQ: BACKGROUND, LEGAL STATUS, AND OTHER ISSUES 2 (2007), https://www.everycrsreport.com/files/20070621_RL32419_5a52f397d7dd85ef70da6cd25f0f0398325990f8.pdf [https://perma.cc/A7US-FSBF]. In 2007, the number of PMCs in Iraq was estimated at between 20,000 and 30,000. *Id.* By the end of the year, approximately 180,000 civilians were working under U.S. contracts. T. Christian Miller, *Contractors Outnumber Troops in Iraq*, L.A. TIMES (July 4, 2007), https://www.latimes.com/archives/la-xpm-2007-jul-04-na-private4-story.html [https://perma.cc/LL7X-26HH]. By October 2012, there were a total of 113,376 Department of Defense contractors in Afghanistan. David Isenberg, *Contractors in War Zones: Not Exactly "Contracting,"* TIME (Oct. 9, 2012), http://nation.time.com/2012/10/09/contractors-in-war-zones-not-exactly-contracting/ [https://perma.cc/Q7DJ-NZYR]. This figure alone exceeded the number of U.S. service members in Afghanistan and does not even account for additional State Department contractors. *Id.* From FY2008-FY2011, contractors in Iraq and Afghanistan represented 52% of the total force, averaging 190,000 contractors to 175,000 uniformed personnel. *Id.*

of PMCs in the post-September 11 era involved tasks that had both strategic and tactical consequences.[157] Private military companies played significant roles in some of the biggest scandals in the global war on terrorism.[158] In 2004, contractors from CACI International[159] and Titan were implicated in perpetrating severe human rights violations—including torture, rape, and murder—against detainees at the Abu Ghraib prison.[160] In 2007, a team of Blackwater contractors killed seventeen Iraqi civilians and wounded twenty-seven others at Nissour Square in downtown Baghdad.[161]

The pervasive use of PMCs in combat environments has been widely criticized for many reasons.[162] Fundamentally, a private company is motivated primarily by business profits, which necessarily calls their judgment into question when there are competing national security interests.[163] Second, privatization reduces "accountability," including difficulty establishing criminal jurisdiction over contractors, lack of contract oversight, and the ability of contractors to refuse orders from military commanders without criminal consequence.[164] Further, using PMCs to perform military functions can damage the reputation of the United States in countries where the military is deployed, often impacting mission accomplishment.[165] Finally, PMCs are susceptible to improperly performing "inherently governmental functions," duties reserved exclusively by law for U.S. government personnel.[166] Although working with industry to develop technology has clear differences from employing private military contractors in hostile

157. *See, e.g.*, GEORGE C. LOVEWINE, OUTSOURCING THE GLOBAL WAR ON TERRORISM 51–76 (2014).

158. *See* Seymour M. Hersh, *Torture at Abu Ghraib*, NEW YORKER (May 10, 2004), https://www.newyorker.com/magazine/2004/05/10/torture-at-abu-ghraib [https://perma.cc/5XDP-VMHN]; Charlie Savage, *Charges Voided for Contractors in Iraq Killings*, N.Y. TIMES (Jan. 1, 2010), https://www.nytimes.com/2010/01/01/us/01blackwater.html [https://perma.cc/7NXX-CRBY].

159. Originally "California Analysis Center, Inc."

160. *See* Hersh, *supra* note 158.

161. *See* Memorandum from Majority Staff on Additional information about Blackwater USA to the Committee on Oversight and Government Reform (Oct. 1, 2007), http://i.a.cnn.net/cnn/2007/images/10/01/blackwater.memo.pdf [https://perma.cc/48XB-R5SJ]. According to this U.S. Congressional memorandum, between 2005 and 2007 Blackwater guards were involved in nearly 200 shootings in Iraq. *Id.*

162. *See, e.g.*, U.N. Human Rights Council, Rep. of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of People to Self-Determination, ¶ 62, U.N. Doc. A/HRC/36/47 (Jul. 20, 2017).

163. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (1977), art. 47, June 8, 1977, 1125 U.N.T.S. 3; *see also* P.W. Singer, *Outsourcing War*, FOREIGN AFFS. (2005), https://www.brookings.edu/articles/outsourcing-war/ [https://perma.cc/6MYV-9JJL] (stating private contractors earn two to ten times more than military soldiers).

164. *See* Martha Minow, *Outsourcing Power: How Privatizing Military Efforts Challenges Accountability, Professionalism, and Democracy*, 46 B.C. L. REV. 989, 1017, 1024 (2005).

165. *Id.* at 1023.

166. *See, e.g.*, COMM'N ON WARTIME CONTRACTING IN IRAQ AND AFGHANISTAN, TRANSFORMING WARTIME CONTRACTING: CONTROLLING COSTS, REDUCING RISKS (2011); Jessica Coomes, Debate Over Private Security Contractors, Inherently Governmental Functions Continues, 93 Fed. Cont. Rep. (BNA) No. 197 (June 22, 2010); Office of Fed. Procurement Policy, Publication of the Office of Federal Procurement Policy (OFPP) Policy Letter 11-01, Performance of Inherently Governmental and Critical Functions, 76 Fed. Reg. 56,227 (Sept. 12, 2011).

environments overseas, national security lawyers can guard against straying beyond the ethical midfield by remembering these criticisms when leveraging private companies for AI.

Finally, even if the government approaches Silicon Valley with skepticism, it will pale in comparison to the skepticism Silicon Valley harbors towards the Department of Defense.[167] Despite the clear need for reliance on Silicon Valley in order for the United States to compete with near-peer adversaries (e.g., China and Russia) in the AI space, the government should not expect notions of patriotism or national security to compel companies like Google or Apple into service.[168] For example, in April 2018, 3,100 Google employees signed a petition stating that "Google should not be in the business of war," calling for Google to discontinue support to the DoD's algorithmic warfare initiative, Project Maven.[169] On its face, Google's "Do No Evil" mantra contrasts greatly with Former Secretary Mattis's call for the Department of Defense to "increase lethality."[170]

But lost in the competing rhetoric is the realization that national security objectives of the United States serve to *stop* evil wherever it may exist in the world, especially against those who wish to do harm to the United States.[171] Also failing to garner front page news are Department of Defense efforts to reduce human suffering, which, if more widely known, may allay concerns among tech companies who fear betraying their core values by supporting defense programs.[172] Furthermore, if Silicon Valley companies participate in important national security initiatives, they may be better positioned to provide a check on the very government ambition that some in Silicon Valley seem to fear.

If the U.S. national security establishment is to fully leverage the promises of the AI revolution, it must rely upon the awesome investments and advances by private companies in the tech industry. As discussed above, in addition to many benefits, this relationship comes with costs and challenges. To help clients remain in the ethical midfield, national security lawyers must constantly learn from industry and assess the appropriate role of industry in government, while facilitating engagement with industry to mitigate mutual skepticism.

---

167. *See, e.g.*, Kevin Roose, *Why Napalm Is a Cautionary Tale for Tech Giants Pursuing Military Contracts*, N.Y. TIMES (Mar. 4, 2019), https://www.nytimes.com/2019/03/04/technology/technology-military-contracts.html [https://perma.cc/SA43-CVVB].

168. *See generally* Letendre, *supra* note 127.

169. Scott Shane & Daisuke Wakabayashi, *'The Business of War': Google Employees Protest Work for the Pentagon*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html [https://perma.cc/ZM9X-ZKEM].

170. *Id*; *see also* DEP'T OF DEF., SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA (2018), https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf [https://perma.cc/CTB7-2W22].

171. *See, e.g.*, SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY, *supra* note 170, at 1 (noting that the Department of Defense's mission is "to *deter* war and protect the security of our nation") (emphasis added).

172. OFFICE OF GEN. COUNSEL, DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL 18 (2015 & Supp. Dec. 2016).

III. PAYING ATTENTION TO OUR ADVERSARIES

As Former Secretary Mattis urged, remaining morally strong in the face of adversity requires preparation.[173] In order to best prepare ourselves to stay within ethical boundaries in AI, national security lawyers must keep abreast of our adversaries' developments in the field. At the unveiling of the 2018 National Defense Strategy (NDS), Secretary Mattis warned that "[o]ur competitive advantage has eroded in every domain of warfare."[174] Furthermore, the 2018 NDS represents a significant shift in focus from countering terrorism to countering adversarial great powers, specifically China and Russia.[175] We can draw again from lessons learned in the first sixteen years of the global war on terrorism.

In his first term, President Obama announced plans for complete withdrawals of U.S. military forces from Iraq by the end of 2011 and from Afghanistan by the end of 2016.[176] Concurrently, the Administration announced a "pivot" or rebalancing of U.S. military attention from those two countries to the Asia-Pacific region.[177] China's ever-increasing global influence coupled with continued aggressive overtures from North Korea demanded a strong U.S. military presence in the region in order to counter the threats that both China and North Korea posed to U.S. national security interests.[178] By 2012, however, ISIS had infiltrated large portions of Syria.[179] By 2014, less than three years after President Obama first withdrew all U.S. military forces from Iraq, ISIS had seized large swaths of the country, including the key cities of Fallujah and Mosul.[180] In light of these developments, President Obama scaled back on the pivot to Asia and authorized

---

173. Mem. for All Dep't of Def. Employees from James Mattis, Sec'y, Dep't Def. Secretary, Department of Defense (Aug. 4, 2017), *available at* https://assets.documentcloud.org/documents/3913969/ETHICAL-STANDARDS-for-ALL-HANDS-OSD009354-17-FOD.pdf [https://perma.cc/2UCH-LPFN].

174. Steve Blank, *The National Defense Strategy: A Compelling Call for Defense Innovation*, WAR ON THE ROCKS (Feb. 12, 2018), https://warontherocks.com/2018/02/national-defense-strategy-compelling-call-defense-innovation/ [https://perma.cc/YFM5-MFNB].

175. *See* SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY, *supra* note 170, at 7.

176. *See* Thom Shanker, *Obama's Campaign Promises on Ending the War in Iraq Now Muted by Reality*, N.Y. TIMES (Nov. 4, 2008), http://www.nytimes.com/2008/12/04/world/americas/04iht-04military.18385946.html [https://perma.cc/3LN7-JQZU]; Mark Landler, *U.S. Troops to Leave Afghanistan by End of 2016*, N.Y. TIMES (May 27, 2014), https://www.nytimes.com/2014/05/28/world/asia/us-to-complete-afghan-pullout-by-end-of-2016-obama-to-say.html [https://perma.cc/4NRC-PETZ].

177. Elisabeth Bumiller, *U.S. Pivots Eastward to Address Uneasy Allies*, N.Y. TIMES (Oct. 24, 2011), http://www.nytimes.com/2011/10/25/world/asia/united-states-pivots-eastward-to-reassure-allies-on-china.html [https://perma.cc/WG2V-BXVN].

178. DEP'T OF DEF., SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA 1 (2018), https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf [https://perma.cc/CTB7-2W22].

179. *See* David Ignatius, *How ISIS Spread in the Middle East*, THE ATLANTIC (Oct. 29, 2015), https://www.theatlantic.com/international/archive/2015/10/how-isis-started-syria-iraq/412042/ [https://perma.cc/MD7U-T7QL].

180. *See* Liz Sly & Ahmed Ramadan, *Insurgents Seize Iraqi City of Mosul as Security Forces Flee*, WASH. POST (June 10, 2014), http://www.washingtonpost.com/world/insurgents-seize-iraqi-city-of-mosul-astroops-flee/2014/06/10/21061e87-8fcd-4ed3-bc94-0e309af0a674 story.html [https://perma.cc/PZ7T-VN9M].

limited combat missions in both Iraq and Syria.[181] Meanwhile, the failed pivot only emboldened North Korea and China, which redoubled its efforts to extend its sphere of influence beyond East Asia.[182]

Contemporaneously, Russia was also emerging as a threat while our attentions were elsewhere.[183] During a 2012 presidential debate, President Obama famously mocked Mitt Romney when Mr. Romney called Russia, rather than al Qaeda, our biggest geopolitical threat.[184] Only two years later, Russia deployed special forces soldiers (or "little green men") to Ukraine with the intent of annexing Crimea.[185] By 2016, President Obama's last year in office, there was substantial evidence that the Russian government had interfered in the U.S. Presidential election.[186] Arguably, while the United States was so fixated on violent extremist organizations like al Qaeda and ISIS, it lost focus on the ambitions and activities of near-peer adversaries, like Russia and China.

Today, the United States lags behind China and Russia in terms of national AI strategy.[187] While the United States government and the Department of Defense continues to figure out the place of AI in society and government, our adversaries

---

181. *See* Christi Parsons and W.J. Hennigan, *President Obama, Who Hoped to Sow Peace, Instead Led the Nation in War*, L.A. TIMES (Jan. 13, 2017), http://www.latimes.com/projects/la-na-pol-obama-at-war/ [https://perma.cc/MUJ8-SC4Z]. What's more, in addition to continuing the war in Afghanistan into the foreseeable future, President Obama committed U.S. forces to armed conflict and counterterrorism missions in Somalia, Libya, Yemen, and elsewhere. *Id.*

182. Simon Tisdall, *Barack Obama's 'Asian pivot' Failed. China is in the Ascendency*, THE GUARDIAN (Sept. 25, 2016), https://www.theguardian.com/commentisfree/2016/sep/25/obama-failed-asian-pivot-china-ascendant [https://perma.cc/7LMF-7JW7].

183. Jeffrey Scott Shapiro, *Obama was Wrong about Russia*, WASH. TIMES, Apr. 30, 2014, https://m.washingtontimes.com/news/2014/apr/30/shapiro-wrong-about-russia/ [https://perma.cc/TEF8-QB2D].

184. *Id.* ("The 1980s are now calling to ask for their foreign policy back, because the Cold War's been over for 20 years.").

185. *See* Steven Pifer, Opinion, *Watch Out for Little Green Men*, BROOKINGS (July 7, 2014), https://www.brookings.edu/opinions/watch-out-for-little-green-men/ [https://perma.cc/BN5D-M7BS]; Kathy Lally, Will Englund & William Booth, *Russian Parliament Approves Use of Troops in Ukraine*, WASH. POST (Mar. 1, 2014), http://www.washingtonpost.com/world/europe/russian-parliament-approves-use-of-troops-in-crimea/2014/03/01/d1775f70-a151-11e3-a050-dc3322a94fa7_story.html [https://perma.cc/WAA8-4VJZ].

186. *See generally* OFF. OF DIR. OF NAT'L INTEL., ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT U.S. ELECTIONS (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [https://perma.cc/X6E8-Z74D]; Karoun Demirjian, *Senate Intelligence Committee Leaders: Russia Did Interfere in 2016 Elections*, WASH. POST (Oct. 4, 2017), https://www.washingtonpost.com/powerpost/senate-intelligence-committee-leaders-russia-did-interfere-in-2016-elections/2017/10/04/1459291c-a91f-11e7-850e-2bdd1236be5d_story.html?utm_term=.8f1015caf2f0 [https://perma.cc/3C9G-YQM2].

187. *See, e.g.*, Zachary Cohen, *US Risks Losing Artificial Intelligence Arms Race to China and Russia*, CNN (Nov. 29, 2017), https://www.cnn.com/2017/11/29/politics/us-military-artificial-intelligence-russia-china/index.html [https://perma.cc/922S-X4AZ]; Owen Churchill, *China's AI Dreams*, NATURE (Jan. 17, 2018), https://www.nature.com/articles/d41586-018-00539-y [https://perma.cc/2KPZ-QWQJ]; Elsa B. Kania, *Artificial Intelligence and Chinese Power*, FOREIGN AFFAIRS (Dec. 5, 2007), https://www.foreignaffairs.com/articles/china/2017-12-05/artificial-intelligence-and-chinese-power [https://perma.cc/3T6C-X47N]; Nick Whigham, *Robotics scientist warns of terrifying future as world powers embark on AI arms race*, NEWS.COM.AU (Feb. 13, 2017), https://www.news.com.au/technology/innovation/inventions/robotics-scientist-warns-of-terrifying-future-as-world-powers-embark-on-ai-arms-race/news-story/d61a1ce5ea50d080d595c1d9d0812bbe [https://perma.cc/6KUX-EBNW].

have already made it a national priority.[188] During the first ever Congressional hearing on AI in September 2016, Senator Ted Cruz warned: "Ceding leadership in developing artificial intelligence to China, Russia and other foreign governments will not only place the United States at a technological disadvantage but it could also have implications for national security."[189]

In July 2017, the Chinese State Council released a comprehensive strategy directing a whole-of-government approach and strongly encouraging big companies like Alibaba and Baidu to invest heavily in AI.[190] China views AI as the key to its global economic domination and national security and has made it a national imperative to become the world leader in AI by 2030. [191] Former Deputy Secretary of Defense Robert Work has called the issuance of this strategy by China a "Sputnik moment."[192] Russia, also, has made AI a national priority.[193] Last September, Vladimir Putin remarked: "Whoever becomes the leader in this sphere will become the ruler of the world. Artificial intelligence is the future not only of Russia but of all of mankind. There are huge opportunities, but also threats that are difficult to foresee today."[194]

Admittedly, advocating for the development of a national AI strategy is not squarely within the purview of a national security lawyer. But the sense that the United States is behind its near-peer adversaries will make some in government desperate to do anything to catch up.[195] Violation of basic human rights seemed warranted under the enhanced interrogation program to stop the so-called "ticking time bomb."[196] The temptation to cut corners will be all the more difficult to resist if our adversaries ignore international norms (which both China and Russia are wont to do) in their employment of AI technology.[197] In keeping with the focus of the 2018 NDS, paying attention to China's and Russia's respective developments in AI must be a part of the equation; doing so will keep national security lawyers prepared and serve us all well in playing the ethical midfield.

---

188. Whigham, *supra* note 187. *But see* Artificial Intelligence Initiative Act, 116 S. 1558 (2019).

189. Press Release, Ted Cruz, Sen. Cruz Chairs First Congressional Hearing on Artificial Intelligence (Nov. 30, 2016), https://www.cruz.senate.gov/?p=press_release&id=2902 [https://perma.cc/ZW5D-4WKS].

190. Churchill, *supra* note 187; Kania, *supra* note 187.

191. Churchill, *supra* note 187; Kania, *supra* note 187.

192. Cohen, *supra* note 187.

193. Radina Gigova, *Who Vladimir Putin Thinks Will Rule the World*, CNN (Sept. 2, 2017), https://www.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html [https://perma.cc/7XTZ-MXQH].

194. *Id*.

195. *See supra* Section II.B.

196. David Luban, *Liberalism, Torture, and the Ticking Bomb*, 91 VA. L. REV. 1425, 1440–41 (2005).

197. *See* Farhood Manjoo, *It's Time to Panic About Privacy*, N.Y. TIMES (Apr. 10, 2019), https://www.nytimes.com/interactive/2019/04/10/opinion/internet-data-privacy.html [https://perma.cc/ZKB4-HTY9] ("Here is the stark truth: We in the West are building a surveillance state no less totalitarian than the one the Chinese government is rigging up"); Christina Larson, *China's Massive Investment in Artificial Intelligence Has an Insidious Downside*, SCIENCE (Feb. 8, 2018), https://www.sciencemag.org/news/2018/02/china-s-massive-investment-artificial-intelligence-has-insidious-downside [https://perma.cc/9VVN-AJQF].

CONCLUSION

Although accounting the failures leading up to the terrorist attacks of September 11, 2001 is a complex undertaking, one of the root causes was an intelligence gap attributable to poor information-sharing practices among government agencies.[198] By missing the signs of imminent attack, the United States found itself on the defensive from the outset of the global war on terrorism. This created an environment permeated by fear, where those in federal and state government were desperate to prevent the next attack.[199] This desperation helped decision-makers justify a drift away from the ethical midfield and deeply-held American values, including moral leadership, due process, and the prohibition of torture.

How would we (the United States government) have prepared ahead of time if we knew that September 11, 2001, was going to happen and result in a global war on terrorism? Would we have increased the size and upgraded the equipment and training of the military in order to face a determined, global enemy? Would we have improved intelligence sharing practices? Would we have considered and developed more thoughtful legal frameworks governing the use of force, interrogation, and intelligence collection? Indeed, with the benefit of hindsight, it is easy to acknowledge now that the legal foundations of many post-September 11, 2001 national security decisions were "sloppily reasoned, overbroad, and incautious."[200] But in a modest defense of the national security lawyers in the arena at the time, the pressures, exigencies, and perceptions in the days, months, and years immediately following the attacks of September 11, 2001 mitigate at least some of the suboptimal legal advice rendered.[201]

The AI revolution upon us may not have the immediate and tragic aftermath wrought by September 11, 2001, but it has the potential to have similar Rubicon-crossing consequences in the national security space. And unlike September 11, 2001, where the attack was a surprise, we know with some degree of certainty that the AI revolution *will happen*. Former Secretary Mattis urged that "to ensure each of us is ready to do what is right, without hesitation, when ethical dilemmas

198. *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT (2004), http://govinfo.library.unt.edu/911/report/911Report.pdf [https://perma.cc/TDB8-3F95].

199. *See, e.g.*, ASHCROFT, *supra* note 9, at 133 ("We simply can't let this happen again. Prosecution cannot be our priority. If we lose the ability to prosecute, that's fine; but we have to prevent the next attack. Prevention has to be our top priority. . . . The chief mission of U.S. law enforcement is to stop another attack and apprehend any accomplices and terrorists before they hit us again. If we can't bring them to trial, so be it.").

200. GOLDSMITH, *supra* note 8, at 10.

201. Interview by Melissa Block and Madeleine Brand with John Yoo, Professor, Univ. of Cal., Berkeley, on NPR (Jan. 19, 2010), https://www.npr.org/templates/story/story.php?storyId=122734173 [https://perma.cc/YZ59-4QKV] (According to John Yoo: "The only thing I regret was just the pressure of time that we had to act under. The problem was we had to make all these decisions in such a short period of time under the pressure of circumstances. And, of course, one would always like the luxury to have more time to think it through . . . .").

arise, we must train and prepare ourselves and our subordinates."[202] Now is the time to begin (or continue) preparing for the impact of AI on national security law and its practitioners.

To conclude, this Article considered three ways by which national security lawyers might help their clients prepare for the AI revolution. First, national security lawyers can help shape advice and policy by (a) learning about the technology, and defining terms and standards; (b) steering clients away from so-called legal black holes; and (c) when appropriate, telling the client what he or she might not want to hear: "no." Second, national security lawyers can help weigh appropriate relationships with the technology industry by (a) identifying and learning from bona fide experts; and (b) appreciating some of the mutual skepticism between Silicon Valley and government. Finally, national security lawyers can stay abreast of our adversaries' AI developments to forestall temptations to take shortcuts later to catch up. By considering this framework and reflecting on the hard lessons learned by national security lawyers in the global war on terrorism, national security lawyers may keep clients in the ethical midfield while leveraging this new technology in order to achieve our Nation's national security objectives.

202. Memorandum from the Deputy Sec'y of Defense of the U.S. Dep't. of Defense to All Dep't. of Defense Emp.'s (Aug. 4, 2017), https://assets.documentcloud.org/documents/3913969/ETHICAL-STANDARDS-for-ALL-HANDS-OSD009354-17-FOD.pdf [https://perma.cc/R4T5-XNRX].