PREDICTING ENEMIES

*Ashley S. Deeks**

Actors in our criminal justice system increasingly rely on computer algorithms to help them predict how dangerous certain people and certain physical locations are. These predictive algorithms have spawned controversies because their operations are often opaque and some algorithms use biased data. Yet these same types of predictive algorithms inevitably will migrate into the national security sphere as the military tries to predict who and where its enemies are. Because military operations face fewer legal strictures and more limited oversight than criminal justice processes do, the military might expect—and hope—that its use of predictive algorithms will remain both unfettered and unseen.

This Article shows why that is a flawed approach, descriptively and normatively. First, in the post-September 11 era, any military operations associated with detention or targeting will draw intense scrutiny. Anticipating that scrutiny, the military should learn from the legal and policy challenges that criminal justice actors have faced in managing the transparency, reliability, and lawful use of predictive algorithms. Second, the military should clearly identify the laws and policies that govern its use of predictive algorithms. Doing so would avoid exacerbating the "double black box" problem of conducting operations that are already difficult to legally oversee and contest, using algorithms whose predictions are often difficult to explain. Instead, being transparent about how, when, why, and on what legal basis the military is using predictive algorithms will improve the quality of military decision-making and enhance public support for a new generation of national security tools.

* E. James Kelly, Jr.–Class of 1965 Research Professor of Law, University of Virginia School of Law. Thanks to Professor Emily Berman, Professor Molly Brady, Alex Chohlas-Wood, Professor Geoff Corn, Dr. Rebecca Crootof, Professor John Duffy, Catherine Baylin Duryea, Professor Rachel Harmon, Professor Oona Hathaway, Professor Eric Jensen, Professor Ed Kitsch, Dustin Lewis, Professor Michael Livermore, and Professor Michael Schmitt for very helpful comments. Thanks also to Sarah Grant for excellent research assistance.

INTRODUCTION

Two burgeoning trends, one in the criminal justice arena and one in the military realm, are going to change the way militaries fight wars. In the criminal justice context, federal, state, and local law enforcement officials increasingly rely on computer algorithms to help them predict how dangerous certain people and certain physical locations are, so as to make more objective judgments about whom to keep in custody and how to use policing resources most efficiently. In the military context, leaders in countries such as the United States and China are urging their militaries to employ machine learning and artificial intelligence to enhance their military capabilities and decision-making.[1] This Article anticipates likely developments at the intersection of these trends: an increase in the use of algorithmic tools akin to those developed in the law enforcement context to help the U.S. military improve its detention and targeting operations—in other words, to predict enemies.[2] It argues that the military should be as transparent as possible about the algorithms' legal underpinnings, uses, goals, benefits, and shortcomings. In so doing, the military can help assuage anticipated critiques of the use of these tools and improve the quality of its decisions about when and how to use the algorithms.

Actors in government, science, and business are beginning to rely more heavily on algorithmic decision-making. Many computer algorithms are based on traditional forms of data analysis: they use statistical tools to find relationships between variables and then predict outcomes.[3] One category of algorithms employs machine learning, which are "algorithms and systems that improve their knowledge or performance with experience."[4] For example, computer scientists have created machine learning algorithms to recognize and classify handwritten numbers by training the algorithms on large sets of handwritten samples, then "rewarding" or "punishing" the algorithm depending on its error rate.[5] The system self-corrects by reweighting

[1] For details of the United States' efforts, see Stew Magnuson, DoD Making Big Push to Catch Up on Artificial Intelligence, Nat'l Def. (June 13, 2017), http://www.nationaldefensemagazine.org/articles/2017/6/13/dod-making-big-push-to-catch-up-on-artificial-intelligence [https://p erma.cc/VYX8-JJNG]. For details of China's efforts, see Cade Metz, As China Marches Forward on A.I., the White House Is Silent, N.Y. Times (Feb. 12, 2018), https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html [https://perma.cc/7ETG-8J6A] and Elsa Kania, The Dual-Use Dilemma in China's New AI Plan: Leveraging Foreign Innovation Resources and Military-Civil Fusion, Lawfare (July 28, 2017, 9:30 AM), https://www.lawfareblog.com/dual-use-dilemma-chinas-new-ai-plan-leveraging-foreign-innovation-resources-and-military-civil [https://perma.cc/S5MT-N6UP].

[2] This Article focuses on the U.S. military, but various other militaries will confront the same developments. There is a wealth of artificial intelligence companies in Israel, for instance, and Israel has significant quantities of data about the groups and individuals it is fighting. See Eliran Rubin, Tiny IDF Unit Is Brains Behind Israeli Army Artificial Intelligence, Haaretz, (Aug. 15, 2017), https://www.haaretz.com/israel-news/tiny-idf-unit-is-brains-behind-israeli-army-artificial-intelligence-1.5442911 [https://perma.cc/36K4-T483].

[3] Thomas H. Cormen et al., Introduction to Algorithms 5 (3d ed. 2009).

[4] Peter Flach, Machine Learning: The Art and Science of Algorithms that Make Sense of Data 3 (2012) (emphasis omitted).

[5] This type of machine learning, in which machines learn what to do to maximize a "reward," is known as "reinforcement learning." Many of its core algorithms originally were inspired by the ways in which people and animals learn. Richard S. Sutton & Andrew G.

variables, sometimes in ways that humans cannot identify or understand. This ultimately results in algorithms that produce low error rates when confronted with new handwriting samples that they have never reviewed before.[6] Actors as diverse as doctors, retailers, and computer scientists have applied machine learning tools to a wide range of problems, from diagnosing lung cancers and predicting heart attacks[7] to recommending movies to watch.[8] In many cases, these tools can make more accurate predictions and judgments than humans can.

The promise of accurate predictions built upon large amounts of data has attracted users in the fields of law enforcement and criminal justice. Courts now commonly employ risk assessment algorithms to judge an arrested person's suitability for release on bail or to help determine whether someone convicted of a crime should receive a prison sentence rather than a punishment that does not require confinement.[9] Police are employing computer algorithms that guide their decisions about where to deploy limited resources, based in large part on algorithmic predictions about where particular types of crimes are most likely to occur and who is likely to be involved (as a victim or perpetrator) in particular kinds of crime.[10]

Just as machine learning has begun to play a role in government decision-making about criminal justice and policing, as well as

Barto, Reinforcement Learning: An Introduction 1, 4–5 (2d ed. 2018); Cary Coglianese & David Lehr, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 Geo. L.J. 1147, 1157–58 (2017) (using handwriting example).

[6] Coglianese & Lehr, supra note 5, at 1157–58.

[7] Mohamad Rabbani et al., Role of Artificial Intelligence in the Care of Patients with Nonsmall Cell Lung Cancer, 48(4) Eur. J. Clin. Invest., Apr. 2018, at 2, 6, https://onlinelibrary.wiley.com/doi/epdf/10.1111/eci.12901; Of Prediction and Policy, The Economist (Aug. 20, 2016), https://www.economist.com/news/finance-and-economics/21705329-governments-have-much-gain-applying-algorithms-public-policy [https://perma.cc/34LC-A59F].

[8] Tom Vanderbilt, The Science Behind the Netflix Algorithms That Decide What You'll Watch Next, Wired (Aug. 7, 2013, 6:30 AM), https://www.wired.com/2013/08/qq_netflix-algorithm/ [https://perma.cc/L3MA-RM48].

[9] Rebecca Wexler, When a Computer Program Keeps You in Jail, N.Y. Times (June 13, 2017), https://www.nytimes.com/2017/06/13/opinion/how-computers-are-harming-criminal-justice.html [https://perma.cc/PC4Q-7MXX] (describing the use of algorithms in policing, bail, evidence, sentencing, and parole contexts).

[10] Andrew Guthrie Ferguson, Predictive Policing and Reasonable Suspicion, 62 Emory L.J. 259, 265–69 (2012); City of Chicago, Strategic Subject List, Chicago Data Portal, https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki-r3np [https://perma.cc/QEA9-767W] (last updated Dec. 7, 2017).

administrative decisions about who should be placed on "no fly" lists,[11] so too is machine learning poised to become an integral part of military operations. Machine learning algorithms hold significant promise in finding patterns or detecting anomalies in large quantities of data. It is easy to envision how these types of tools will be useful when trying to predict how a particular person will behave or what enemy forces plan to do next based on thousands of past examples of human behavior.[12] This is particularly true for the types of conflicts the United States has been fighting for the past sixteen years, where enemy forces are non-state actors. In traditional international armed conflicts between states, enemy forces are readily identifiable, and their fighting roles are generally predictable. In conflicts such as those against al Qaeda and the Islamic State, however, it is much harder for the U.S. military to establish the actors' affiliations and intentions, something it must do in order to comply with international law. These problems bear some similarities to the types of problems law enforcement algorithms attempt to address.[13]

[11] Maureen Cooney, U.S. Dep't of Homeland Sec., Report on Effects on Privacy & Civil Liberties 12–13 (2006), https://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_nofly.pdf [https://perma.cc/BXP8-37SQ] (describing use of algorithms to create no-fly lists).

[12] There are a number of examples in which military technology has been transported into policing. See, e.g., Adam Goldman, Trump Reverses Restrictions on Military Hardware for Police, N.Y. Times (Aug. 28, 2017), https://www.nytimes.com/2017/08/28/us/politics /trump-police-military-surplus-equipment.html [https://perma.cc/M6VW-NGLE]; Timothy Williams, Facial Recognition Software Moves from Overseas Wars to Local Police, N.Y. Times (Aug. 12, 2015), https://www.nytimes.com/2015/08/13/us/facial-recognition-software-mov es-from-overseas-wars-to-local-police.html [https://perma.cc/E4 AT-QGFR]. In other cases, the military has employed techniques drawn from law enforcement. See, e.g., John B. Alexander, Convergence: Special Operations Forces and Civilian Law Enforcement, Joint Special Operations Univ. Report 10–6, at 1–3 (July 2010), https://publicintelligence.net/joint-special-operations-university-report-on-convergence-of-special-forces-and-civilian-law-enfo rcement/ [https://perma.cc/ZJ8T-L8EJ] (describing how Special Operations Forces have begun to undertake activities traditionally performed by civilian law enforcement agencies); Rory B. Quinn, Combat Policing: The Application of Selected Law Enforcement Techniques to Enhance Infantry Operations, Marine Corps Command & Staff College (May 9, 2012), http://www.dtic.mil/docs/citations/ADA600538 [https://perma.cc/VWP4-DCVG] Gretchen Peters, Incorporating Law Enforcement Interrogation Techniques on the Battlefield, 2 Combating Terrorism Center Sentinel, July 2009, https://ctc.usma.edu/posts/incorporating-law-enforcement-interrogation-techniques-on-the-battlefield [https://perma.cc/LUK4-VL8 H]. This back-and-forth flow of tools and techniques between law enforcement and the military suggests that if the military develops the types of algorithms discussed in this Article, actors in domestic law enforcement eventually may find a use for those algorithms, for better or worse.

[13] Peters, supra note 12.

More specifically, militaries in armed conflict often need to detain individuals and decide how long to hold them based on the threat they pose. During the conflicts in Afghanistan (beginning in 2001) and in Iraq (beginning in 2003), the U.S. military collectively detained at least 150,000 people.[14] Although the academic and popular literatures have not yet considered the issue, predictive algorithms seem likely to have a significant impact on future detention operations. One important stimulus for this development will be the widespread use of algorithms in the domestic law enforcement context. In light of the requirements of international law, which require states to assess periodically whether to release certain people in their custody,[15] it is easy to envision how state militaries might repurpose the kinds of algorithms crafted in the domestic criminal context to predict individual "dangerousness" in the military detention context.

Further, it seems likely that the military will seek to (or continue to) develop algorithms comparable to those that facilitate "predictive policing" for domestic law enforcement agencies.[16] After all, in both contexts, the goal is to anticipate where undesirable activity will occur and deploy resources to meet or suppress that eventuality. Today's predictive policing algorithms might thus serve as a general model for algorithms that recommend when and where militaries should deploy forces to patrol or to meet an anticipated attack, and which actors are most likely to pose a threat during that deployment. Indeed, in 2015, the

[14] Brendan M. Fischer & Lisa Graves, International Law and the War on Terror (2011), http://watson.brown.edu/costsofwar/files/cow/imce/papers/2011/International%20Law%20and%20the%20War%20on%20Terror.pdf [https://perma.cc/ZKB9-4X6Y] (stating that the United States held over 100,000 prisoners in the American-run detention system in Iraq, and detained 50,000 people in Afghanistan in just the first three years of the war); American Forces Press Service, Camp Bucca Detention Center Closes in Iraq (Sept. 17, 2009), http://archive.defense.gov/news/newsarticle.aspx?id=55880 [https://perma.cc/6YNP-96GY] (suggesting that the United States held about 15,000 detainees at Camp Bucca, Iraq between 2008–09).

[15] See, e.g., Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 43, 78, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 287 [hereinafter Fourth Geneva Convention]. States need not review the status of prisoners of war for potential release. The law on non-international armed conflicts is silent on review requirements, but states such as the United States established periodic review procedures for detainees held in Iraq, Afghanistan, and Guantanamo. See Ashley S. Deeks, Starting from Here, 84 Int'l L. Stud. 161, 164–67 (2008).

[16] I have not found evidence that the U.S. military currently is studying these law enforcement algorithms for inspiration, though it is possible that the military already has developed and begun to deploy comparable algorithms.

Army announced that it was creating a "commander's virtual staff," which seeks to apply artificial intelligence and computer automation to tactical decision-making on the battlefield.[17] To be clear, that project—and this Article—are not about increased weapons autonomy.[18] Rather, both focus on more modest algorithms that produce recommendations about target selection and about where to deploy resources on the basis of which humans—that is, military officials—then must make decisions.[19]

Pentagon leaders have already started to employ predictive algorithms for certain war-related tasks, and the 2018 National Defense Strategy commits the Defense Department to continue to make advances in this area.[20] For instance, in 2006, the military deployed a predictive algorithm that helped anticipate where insurgents in Iraq were placing improvised explosive devices.[21] More recently, military leaders assigned the Pentagon's Algorithmic Warfare Cross-Functional Team the job of creating algorithms to review the Defense Department's many thousands of hours of drone video footage and to identify segments that may contain relevant activity.[22] This team presumably will take advantage of

[17] CERDEC Public Affairs, Army Applies Computer Automation to Operational Decision Making, U.S. Army (May 14, 2015), https://www.army.mil/article/148549/army_applies_computer_automation_to_operational_decision_making [https://perma.cc/SCR8-CBH4].

[18] See generally Vincent Boulanin & Maaike Verbruggen, Stockholm Int'l Peace Research Inst., Mapping the Development of Autonomy in Weapons Systems, (2017), https://www.sipri.org/sites/default/files/2017-11/siprireport_mapping_the_development_of_autonomy_in_weapon_systems_1117_0.pdf [https://perma.cc/A7PE-BRSR] (exploring autonomy in weapon systems).

[19] Charlie Lewis, Capturing Flying Insects: A Machine Learning Approach to Targeting, War on the Rocks (Sept. 6, 2016), https://warontherocks.com/2016/09 /capturing-flying-insects-a-machine-learning-approach-to-targeting/ [https://perma.cc/QJ2R-EEFA] ("Machine learning just assists in identifying, locating, and determining the best method of engagement for a target.").

[20] U.S. Dep't of Def., Summary of the 2018 National Defense Strategy of the United States 7, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf [https://perma.cc/XHW7-SR7Q]; Julian E. Barnes & Josh Chin, The New Arms Race in AI, Wall St. J. (Mar. 2, 2018, 11:47 AM), https://www.wsj.com/articles /the-new-arms-race-in-ai-1520009261, (stating that in its 2017 unclassified budget the Pentagon spent about $7.4 billion on AI and associated fields; this does not account for classified spending).

[21] Walter L. Perry et al., RAND Corp., Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations 73–74 (2013), https://www.ncjrs.gov/pdffiles1/nij/grants/243830.pdf [https://perma.cc/BVJ8-SNRV].

[22] Marcus Weisgerber, The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS, Defense One (May 14, 2017), https://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/

significant advances in facial and voice recognition made possible by machine learning.[23] Machine learning also facilitates pattern detection, which will help the military assess the activities of particular individuals and determine, based on those activities, whether they are members of enemy-organized armed groups. In one recent example, the National Security Agency employed a pattern recognition algorithm that used phone contacts to identify individuals who were closely connected to al Qaeda and who thus might possess useful intelligence.[24] The fact that the military has begun to use algorithms that can detect anomalous behavior on video and can employ large quantities of surveillance data to draw conclusions about personal networks suggests that the day is not far off when the military will turn to algorithms that make recommendations about how long to detain someone, where to patrol, and whom to target.

There will be a variety of hurdles to developing accurate and fair predictive algorithms for military use. The military thus should approach the use of these algorithms with significant caution. It is quite possible that a careful deployment of detention algorithms could result in better decisions about who to continue to detain and who to release by avoiding human biases, facilitating compliance with legal standards, and accou-nting for a wider range of relevant data in the government's possession. It is also possible that a use of reliable "targeting" algorithms might improve military decisions about where and in what

[htt ps://perma.cc/NT6V-8VK6]; Ben Sullivan, America Is Going to Fight ISIS with Algorithms, Motherboard (May 16, 2017, 8:47 AM), https://motherboard.vice.com/en_us/arti cle/3 dxj33/america-is-going-to-fight-isis-with-algorithms [https://perma.cc/Y9AB-9WRD] (stating that the Pentagon will soon deploy machine learning algorithms to help intelligence analysts identify Islamic State fighters in those videos); Memorandum from Robert O. Work, Deputy Sec'y of Def., Establishment of an Algorithmic Warfare Cross-Functional Team (Apr. 26, 2017) (instructing the Team to provide computer vision algorithms for object detection, classification, and alerts, and later to "prioritize the integration of similar technologies into other defense intelligence mission areas").

[23] Barnes & Chin, supra note 20 (noting that AI used in Project Maven "can already find potential enemies in a crowd faster than trained intelligence analysts"); Kate Conger & Dell Cameron, Google Is Helping the Pentagon Build AI for Drones, Gizmodo (Mar. 6, 2018), https://gizmodo.com/google-is-helping-the-pentagon-build-ai-for-drones-1823464533 [https://perma.cc/N5Q5-978T] (describing Google's partnership with the Defense Department to develop AI for analyzing drone footage).

[24] Martin Robbins, Has a Rampaging AI Algorithm Really Killed Thousands in Pakistan?, The Guardian (Feb. 18, 2016), https://www.theguardian.com/science/the-lay-scientist/2016/feb/18/has-a-rampaging-ai-algorithm-really-killed-thousands-in-pakistan [https://perma.cc/A6 MZ-V79C].

locations to conduct operations, rendering those operations both more effective and more precise. But there are a variety of legal and policy challenges to developing and employing detention and targeting algorithms, some of which track the problems with criminal justice algorithms and some of which will be different and more potent in the military context. One particular hurdle arises from the difficulty in translating desired constraints—drawn from international law and policy—into computer code. Even if the military develops predictive algorithms that are not direct descendants of the criminal justice algorithms discussed here, the military nevertheless can learn from the legal challenges that criminal justice actors have faced in managing the reliability, transparency, and lawful use of these types of algorithms.

The military use of predictive algorithms and machine learning tools seems certain to replicate and even exacerbate, at least for the casual observer, many of the critiques that the military has faced over the past fifteen years: a lack of transparency, a willingness to adopt aggressive interpretations of the law, a concern that the military makes detention and targeting decisions based on flawed data, and a perceived dehumanization of lethal action (in the form of drone strikes and increasingly automated decision-making). In choosing to employ predictive algorithms, the military must carefully address each challenge to ensure that the public, both domestic and international, views U.S. military operations as lawful and legitimate. The U.S. government should thus seek to avoid creating a "double black box." That is, the government should avoid operating an "algorithmic black box" inside what many in the public conceive of as the "operational black box" of the military. Indeed, the military should treat the coming machine learning era as an opportunity to thoroughly explain and address in public fora the advantages and challenges that predictive algorithms pose and the legal framework in which they operate, and thus earn support from both the U.S. public and foreign governments, especially military allies.

Part I of this article considers the ways that executive officials, judges, and police departments in the United States currently use algorithms to make choices about detention and policing in the civilian law enforcement setting. Extrapolating from situations in which law enforcement and criminal justice actors have found such predictive algorithms useful, Part II explores how militaries might be attracted to the use of similar algorithms in the detention and operational contexts. It identifies the laws and policies that inform military decisions about detention and release, and analyzes how algorithms might guide those decisions. It also discusses the laws that regulate targeting and examines how militaries might employ predictive policing-type algorithms to inform decisions about where to conduct military operations and, potentially, whom to target. Using the concerns about criminal justice and policing algorithms as a starting point, Part III identifies and analyzes the most significant critiques and challenges that militaries will face as they turn a predictive algorithmic lens on detention and targeting. Part IV draws from lessons learned from deeply opaque military and intelligence activities in the post-September 11 era, and the government's subsequent scramble to be forthcoming about the legal and policy frameworks that undergirded those activities. Based on that experience, this Part argues for a new approach to this important algorithmic development in war-fighting: strategic transparency about law and policy.

I. CRIMINAL JUSTICE AND POLICING ALGORITHMS

Government actors in the U.S. criminal justice system must often make predictions. In assessing whether to release someone on bail, judges try to predict how likely it is that the person will commit another crime if released, and how likely it is that he will voluntarily appear for his trial. When prosecutors are deciding what sentence to seek and judges are deciding what sentence to impose on someone convicted of an offense, one factor that they consider is the likelihood that the person will commit another offense in the future. Parole boards try to predict whether and when it is safe to release someone from prison before he has completed his sentence. In deciding where to patrol on a given shift and how many officers to assign to an area, police try to predict when and where certain serious crimes are most likely to occur. Each of these actors tries to estimate the likelihood that some particular act will transpire, but nonetheless each must make a decision based on incomplete or imperfect information.

In the past several years, prosecutors, judges, police, and parole boards in the federal, state, and local criminal justice systems have begun to employ computer algorithms in an effort to improve the reliability of their predictive decisions.[25] Specifically, they have started to use risk assessment algorithms[26] and machine learning[27] to improve their performance in deciding where to patrol and whether and how long someone should remain detained. Programmers "train" machine learning systems that make individual risk assessments by inputting large amounts of data on individuals. The systems process the examples and "learn" which characteristics are helpful in predicting outcomes such as bail jumping and recidivism. When presented with a new case—such as someone newly arrested—the algorithm can offer a statistical, data-driven prediction about how likely it is that this new individual will (for example) jump bail. Similarly, programmers train systems whose goal is to predict the likelihood of particular types of crimes occurring in particular locations by feeding in large quantities of data about locations, dates, times, and types of past crimes and other neighborhood features.[28]

Some support the use of these algorithms because they can offer predictions that are less biased and more empirically accurate than human judgment standing alone.[29] Although these predictions are

[25] Wexler, supra note 9 (discussing varieties of uses); Electronic Privacy Information Center, Algorithms in the Criminal Justice System, https://epic.org/algorithmic-transparency/crim-justice/ [https://perma.cc/4AUX-C75J] (last visited Sept. 11, 2018) (listing different states' uses of algorithmic tools for sentencing, probation, and parole decisions).

[26] John Monahan defines *risk assessment* as "the process of using risk factors to estimate the likelihood (i.e., probability) of an outcome occurring in a population," where (in the sentencing context) the population is convicted offenders and the outcome is criminal recidivism. John Monahan, Risk Assessment in Sentencing, *in* 4 Reforming Criminal Justice 77, 78–79 (Erik Luna ed., 2017). An *algorithm* is "any well-defined computational procedure that takes some value, or set of values, as input and produces some value, or set of values, as output." Cormen et al., supra note 3, at 5 (emphasis omitted).

[27] See Brent Daniel Mittelstadt et al., The Ethics of Algorithms: Mapping the Debate, Big Data & Soc'y, July–Dec. 2016, at 3 (defining machine learning as "any methodology and set of techniques that can employ data to come up with novel patterns and knowledge, and generate models that can be used for effective predictions about the data").

[28] See Hyeon-Woo Kang & Hang-Bong Kang, Prediction of Crime Occurrence from Multi-Modal Data Using Deep Learning, 12(4) PLoS ONE, April 24, 2017, at 2, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0176244 [https://perma.cc/R9W8-ZLFE].

[29] See, e.g., Anthony Flores et al., False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks," 80 Fed. Probation, Sept. 2016, at 38–39 (arguing that actuarial risk assessments are superior to unstructured professional judgment); Mohana Ravindranath, White House Adviser: AI Could Make Criminal Justice System Fairer, Nextgov (June 7, 2016), http://www.nextgov.com/emerging-tech/2016/06/white-

merely estimates about the likelihood that an event will occur, and not cast-iron forecasts, statistical models that learn from historical data are more scientifically rigorous than human mental models. Others, however, have expressed a variety of concerns about the use of risk assessment algorithms, including worries about the use of flawed or biased data inputs, lack of transparency about how the algorithm is assembled and trained, and the difficulty in holding people accountable for flawed algorithm-driven decisions. This Part first considers the use of algorithmic risk assessments that attempt to predict the future behavior of people who already have been arrested or tried (in the bail, sentencing, and parole contexts). It then examines the use of assessments that anticipate the location of (and possibly the identity of people undertaking) *future* criminal acts. Further, it identifies the types of data that programmers use to create such algorithms, to establish a baseline against which to evaluate comparable algorithms in the military context.

A. Individual Risk Assessment Algorithms

Actors in the criminal justice system often face difficult disposition decisions: Should a judge allow someone to post bail and be released after he is arrested because the judge deems him likely to return for his scheduled court appearances? Should a judge sentence someone convicted of a crime to a term of confinement, or is the person sufficiently unlikely to re-offend, such that the judge should employ an alternative punishment such as community service?[30] Should a parole board conclude that the person whose case it is considering is unlikely to commit another offense if released from prison early and so grant him

house-advisor-ai-could-make-criminal-justice-system-fairer/128888/ [https://perma.cc/NR7N-DYZR].

[30] Richard Berk et al., Forecasting Murder Within a Population of Probationers and Parolees: A High Stakes Application of Statistical Learning, 172 J. Royal Stat. Soc'y Series A, at 2 (2009); Anna Maria Barry-Jester et al., The New Science of Sentencing, The Marshall Project (Aug. 4, 2015, 7:15 AM), https://www.themarshallproject.org/2015/08/04/the-new-science-of-sentencing#.AiGrtDIWg [https://perma.cc/N4BH-5Q3B] (stating that Pennsylvania bases criminal sentences in part on whether individuals are deemed likely to commit additional crimes and is using risk assessments to help judges decide how much prison time to assign). Most of these questions raise classification problems, which require the model to predict whether someone falls into category *X* (high risk) or category *Y* (lower risk). See Coglianese & Lehr, supra note 5, at 1158 (discussing one type of machine learning that addresses classification problems).

parole? Decision-makers in these cases face uncertainty about a future outcome. Many have turned to algorithms to assist them in making these decisions.

Take the specific example of bail assessments. Millions of times a year, a judge decides whether a defendant will await trial in jail or at home.[31] The judge must make that decision based on her assessment of how likely it is that the defendant will flee or commit another crime if he is released.[32] A variety of jurisdictions, including Arizona, Kentucky, New Jersey, Charlotte, Chicago, and Phoenix, now employ computer algorithms to help judges make bail decisions.[33] One recent research study claims to show that using a particular bail-related algorithm would lead to about twenty percent less crime, not by recommending that judges detain *more* people before trial, but by recommending that they detain *different* people.[34] Others have argued in favor of bail algorithms, because actuarial risk assessments are less biased than judges may be.[35] In the parole context, many states employ software such as the Level of Services Inventory-Revised to predict parole recidivism.[36] Algorithms like this learn which characteristics are most helpful in predicting whether someone will re-offend and can make predictions about a particular person, even if the program has not encountered that particular person's information before.[37]

In sentencing, too, judges use risk assessment algorithms to guide their discretion, with the goal of making sentences more uniform and predictable while still remaining sensitive to public safety concerns.[38]

[31] Jon Kleinberg et al., Human Decisions and Machine Predictions, 133 Q.J. Econ. 237, 239 (2018).

[32] Id.

[33] Angele Christin et al., Courts and Predictive Algorithms, N.Y.U Law Data & Society Primer for the Data & Civil Rights Conference, in Washington, D.C., at 3 (Oct. 27, 2015), http://www.datacivilrights.org/pubs/2015-1027/Courts_and_Predictive_Algorithms.pdf [https://perma.cc/48LD-9SCR]; see also Laura & John Arnold Foundation, Public Safety Assessment: A Risk Tool That Promotes Safety, Equity, and Justice (Aug. 14, 2017), http://www.arnoldfoundation.org/public-safety-assessment-risk-tool-promotes-safety-equity-justice/ [https://perma.cc/5F9F-F3M5] (describing the usefulness of the Public Safety Assessment algorithm in bail decisions).

[34] The Economist, supra note 7 (citing Kleinberg study).

[35] Samuel R. Wiseman, Fixing Bail, 84 Geo. Wash. L. Rev. 417, 420–25 (2016) (arguing that judges have incentives to decline to release people on bail).

[36] Christin et al., supra note 33, at 3–4.

[37] See The Economist, supra note 7.

[38] Andrew Guthrie Ferguson, Policing Predictive Policing, 94 Wash. U. L. Rev. 1109, 1121 (2017). For a critique of the use of predictive algorithms for sentencing, see Danielle

Another reason states use these algorithms is to identify low-risk felons, so as to be able to impose non-carceral punishments.[39] A variety of states employ a risk assessment tool called COMPAS, which provides judges with risk scores for defendants, based on their answers to a series of questions.[40] In *Wisconsin v. Loomis*, a Wisconsin judge imposed a long sentence on a defendant, based partly on the fact that COMPAS had assessed the defendant as high risk.[41] The State refused to grant the defendant access to the contents of the algorithm; the U.S. Supreme Court denied his petition for certiorari.[42] Indeed, policing in the right place at the right time can (in theory) lower crime rates, or at least maintain the same crime rate while expending fewer resources. As Professor Andrew Ferguson notes, "sing predictive analytics, high-powered computers, and good old-fashioned intuition, police are adopting predictive policing strategies that promise the holy grail of policing—stopping crime before it happens."[43] Police departments have applied this type of predictive policing to at least two different targets: specific geographic locations and specific people.[44]

For a number of years, various cities have employed machine learning algorithms to identify *specific city blocks* on which particular crimes are most likely to occur.[45] Chicago, for instance, employed a computer

Kehl et al., Algorithms in the Criminal Justice System (2017), https://cyber.harvard.edu/node/99985 [https://perma.cc/EWV4-CL9B].

[39] Kehl et al., supra note 38, at 10.

[40] Jason Tashea, Courts Are Using AI to Sentence Criminals. That Must Stop Now, Wired (Apr. 17, 2017), https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/ [https://perma.cc/C624-ZS7R].

[41] 881 N.W.2d 749, 754–55 (Wis. 2016).

[42] Id. at 757 (noting that defendant objected to his inability to assess the algorithm's accuracy because of its proprietary nature); Loomis v. Wisconsin, SCOTUSblog, http://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/ [https://perma.cc/9LKB-ZP87] (last visited Oct. 20, 2018) (listing the Supreme Court's denial of certiorari dated June 26, 2017).

[43] Ferguson, supra note 38, at 1112; see also Steven M. Bellovin et al., When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning, 8 N.Y.U. J.L. & Liberty 555, 613–14 (2014) (arguing that the success of predictive software makes it likely that police will increase use of data programs).

[44] Andrew Guthrie Ferguson, Predictive Prosecution, 51 Wake Forest L. Rev. 705, 705 (2016) (noting that police are using algorithmic forecasts to identify both places and persons likely to be involved in criminal activity).

[45] Id. at 711 (stating that police departments might use the software to instruct officers to focus attention on particular block-sized areas during free time in their shift); see also Press Release, Chicago Police Department, Mayor Emanuel, Police Department Announce Expansion of Predictive Crime Fighting Strategy (Feb. 21, 2017), https://home.chicagopo

program that identified twenty small city zones that it deemed the most dangerous.[46] Researchers and companies have developed algorithms that predict the occurrence of various property crimes.[47] An algorithm named HunchLab (made by a company called Azavea) identifies crime hotspots, and, according to the company, helps police align patrol activities with the community's priorities and intelligently allocate police resources.[48] Its machine learning algorithm takes into account information such as baseline crime rates, weather and seasons, socioeconomic factors, and sporting events, updating the algorithm for every new police shift.[49] Another type of algorithm helps guide police who are engaged in non-patrol-based intervention strategies, including by identifying vacant properties that could be boarded up to reduce crime.[50]

A second type of predictive policing algorithm identifies *people* who are most likely to be party to a violent incident, either as a perpetrator or as a victim.[51] The Chicago Police Department has used an algorithm to create a "Strategic Subject List," identifying individuals who are most

lice.org/wp-content/uploads/2017/02/21-Feb-17-Mayor-Emanuel-CPD-Announce-Expansion-of-Predictive-Crime-Fighting-Strategy.pdf (discussing Chicago Police Department's predictive policing strategy). For a discussion of the history of predictive policing starting in 2008, see Perry et al., supra note 21, at 3–5.

[46] Monica Davey, Chicago Tactics Put Major Dent in Killing Trend, N.Y. Times, June 11, 2013, at A1.

[47] Leslie W. Kennedy et al., Risk Clusters, Hotspots, and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies, 27 J. Quantitative Criminology 339, 358 (2011).

[48] Hunchlab, http://www.hunchlab.com [https://perma.cc/K9DY-MZLW] (last visited Sept. 11, 2018); see Maurice Chammah, Policing the Future, The Marshall Project (Feb. 3, 2016), https://www.themarshallproject.org/2016/02/03/policing-the-future# [https://perma.cc/V6ZE-YRAN] ("HunchLab . . . represents the newest iteration of predictive policing, a method of analyzing crime data and identifying patterns that may repeat into the future.").

[49] Ferguson, supra note 38, at 1136.

[50] Chammah, supra note 48 ("As predictive policing has spread, researchers and police officers have begun exploring how it might contribute to a version of policing that downplays patrolling—as well as stopping, questioning, and frisking—and focuses more on root causes of particular crimes. Rutgers University researchers specializing in 'risk terrain modeling' have been using analysis similar to HunchLab to work with police on 'interve ntion strategies.' In one Northeast city, they have enlisted city officials to board up vacant properties linked to higher rates of violent crime, and to advertise after-school programming to kids who tend to gather near bodegas in high-risk areas.").

[51] David Robinson & Logan Koepke, Upturn, Stuck in a Pattern: Early Evidence on "Predictive Policing" and Civil Rights 2–3 (2016), https://www.upturn.org/reports/2016/stuck-in-a-pattern/ [https://perma.cc/6Y2Z-5CQC] (describing "place-based" tools and "person-based" tools).

likely to be either the victims or perpetrators of gun violence.[52] The algorithm allowed the Police Department to identify and rank-order 1,400 people among whom violence is most concentrated.[53] The algorithm ranks these individuals according to their chance of becoming involved in a shooting or homicide, based on past criminal offenses, reported gang affiliations, and the criminal justice records of people arrested at the same time as the individual in question.[54] Palantir produced a similar algorithm for the New Orleans Police Department.[55] A different software program, Beware, assigns numerical threat scores and color-coded threat levels (red, yellow, or green) to any person, area, or address that police search.[56]

This type of predictive algorithm is based on the idea that "negative social networks" encourage criminal activity.[57] It thus uses "big data capabilities to develop predictive profiles of individuals based on past criminal activity, current associations, and other factors that correlate with criminal propensity."[58] It is the most controversial type of policing algorithm, at least when applied at the individual level, because it focuses police attention on individuals who may not have actually committed an offense.[59] One article demonstrates that taking into

[52] Jeff Asher & Rob Arthur, Inside the Algorithm That Tries to Predict Gun Violence in Chicago, N.Y. Times (June 13, 2017), https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html [https://perma.cc/7UT9-UGTN]; Robinson & Koepke, supra note 51, at 3; Davey, supra note 46.

[53] Robinson & Koepke, supra note 51, at 3 (stating that the Strategic Subjects List rank-ordered between 400 and 1,400 people); Asher & Arthur, supra note 52 (stating that the list reflects "about 1,400 people").

[54] Matt Stroud, The Minority Report: Chicago's New Police Computer Predicts Crimes, But Is It Racist?, The Verge (Feb. 19, 2014, 9:31 AM), https://www.theverge.com/2014/2/19/5419 854/the-minority-report-this-computer-predicts-crime-but-is-it-racist [https://perma.cc/93ZY -LAJV] (noting that the algorithm examines a person's relationship to other violent people and quoting a Yale professor as stating, "It's not just about your friends and who you're hanging out with, it's actually the structure of these networks that matter").

[55] Ali Winston, Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology, The Verge (Feb. 27, 2018, 3:25 PM) (noting that Palantir has patented a crime-forecasting system and has sold similar software to foreign intelligence services to help them predict the likelihood that particular individuals will commit terrorist acts).

[56] Robinson & Koepke, supra note 51, at 4, 10–11.

[57] Ferguson, supra note 38, at 1137, 1141.

[58] Id. at 1137.

[59] Id. at 1114 ("[F]orecasting the precise identity of the future human 'criminal' presents a far more troubling prediction."); Stroud, supra note 54 (quoting critics who claim that the algorithm represents racial profiling).

account the acts of a person's associates when assessing the likelihood that he will be involved in violence comes close to imposing guilt by association.[60] Consider a neighborhood pastor who befriends and tries to help a group of young, troubled men who previously have been arrested. The pastor might receive a "red" coding from Beware, simply because of his high level of association with those young men. This illustrates the challenge of building algorithms that are sufficiently nuanced. Similarly, others critique the use of policing algorithms because it is not clear that they have real predictive value.[61]

B. Algorithmic Inputs

In the computing context, algorithms are computational procedures that take some set of values as inputs and produce some set of values as outputs.[62] Machine learning, a type of computer algorithm that has gathered increased attention and use recently, relies on the idea that computers can learn from experience on a specific task to improve their ability to predict outcomes.[63] As computer scientists expose algorithmic models to new data, the models are able to independently adjust the weights they give to different factors to provide more accurate predictions.[64] Because of the increased availability of vast volumes of data and more powerful, less expensive computational processing, machine learning has expanded exponentially in recent years.[65]

Each of the algorithms described in Section I.B are trained, tested, and re-trained on data. The Level of Service Inventory-Revised, an algorithm that predicts an offender's risk of recidivism for parole purposes, uses as inputs the offender's answers to questions about his "criminal history, education, employment, financial problems, family or

[60] Jeremy Gorner, Chicago Police Use "Heat List" as Strategy to Prevent Violence, Chi. Trib. (Aug. 21, 2013), http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list.

[61] Asher & Arthur, supra note 52; Mick Dumke & Frank Main, A Look Inside the Watch List Chicago Police Fought to Keep Secret, Chi. Sun-Times (May 18, 2017), https://chicago.suntimes.com/news/what-gets-people-on-watch-list-chicago-police-fought-to-keep-secret-watchdogs/ [https://perma.cc/J2X8-7R5N].

[62] Cormen et al., supra note 3, at 5.

[63] Aurelien Geron, Hands-On Machine Learning with Scikit-Learn and TensorFlow 3–4 (2017).

[64] Machine Learning: What It Is and Why It Matters, Analytics Insights, SAS Insights, SAS Institute, Inc., https://www.sas.com/en_us/insights/analytics/machine-learning.html# [https:// perma.cc/6D49-V9LG] (last visited Sept. 11, 2018).

[65] Id.

marital situation, housing, hobbies, friends, alcohol and drug use, emotional or mental health issues, and attitudes about crime and supervision."[66] To a large extent, these factors mirror those that police departments have traditionally used. However, the algorithms are able to refine the weight given to each factor and identify interactions between factors in ways humans cannot, producing a more rigorous, evidence-based analysis. Predictive policing algorithms use a wider variety of data. For the Strategic Subject List in Chicago, factors include the age of the potential victim or offender, whether someone already had been the victim of an assault and battery or shooting, and the person's arrest and conviction records.[67] The widely used COMPAS tool (which does not employ machine learning) assesses "criminal involvement, relationship/lifestyles, personality/attitudes, family, and social exclusion."[68] HunchLab "primarily surveys past crimes, but also digs into dozens of other factors like population density; census data; the locations of bars, churches, schools, and transportation hubs; schedules for home games—even moon phases."[69] It also takes into account the day of the week and the month of the year.[70]

Although there is little information available about the quantity (or quality) of data used by the companies that created these instruments, academic researchers tend to be more forthcoming. For example, researchers in one recent study employed a machine learning algorithm that was trained on the characteristics of over 500,000 defendants arrested in New York City between 2008 and 2013.[71] The goal of the algorithm was to provide a probability of crime risk for a given individual.[72] The study showed that the algorithm would have made qualitatively better predictions about which individuals would offend while out on bail than the judges adjudicating those defendants' cases had made. This study employed a large training set of data, which may

[66] Ferguson, supra note 38, at 1119 (noting that the questions also ask "about school suspensions, dissatisfaction with spouses, use of free time, and mental health").

[67] Asher & Arthur, supra note 52; Stroud, supra note 54.

[68] Kehl et al., supra note 38, at 11.

[69] Chammah, supra note 48.

[70] Id.

[71] Kleinberg et al., supra note 31, at 247–49.

[72] Id. at 239.

be higher than necessary to produce reliable outcomes.[73] Nevertheless, the kinds and quantity of data available for use in criminal justice algorithms are likely to be different—and potentially more robust—than the data available for use in the military context. Part III discusses additional critiques of the quantity and quality of data used to develop algorithms.

II. THE MILITARY'S PREDICTIVE ALGORITHMS

The dominant focus in the academic literature on machine learning and warfare has been on the development and use of lethal autonomous weapons systems—systems that may ultimately be able to identify, track, and kill individuals without human intervention.[74] But computer algorithms generally—and machine learning in particular—are positioned to affect military operations well beyond (and antecedent to) the use of robots that may use force autonomously. Indeed, militaries are likely to develop and use a variety of other, less-lethal machine learning algorithms far sooner than they will develop and comprehensively deploy lethal autonomous weapons systems.[75] One reason why the U.S. military may need only a short time horizon to develop algorithms to make risk assessments of detainees in its custody and to improve its combat operations is that there are obvious models from which to draw: the law enforcement algorithms discussed in Part I.

Yet developing reliable algorithms in the context of detainee reviews will be challenging, not least because of the types of legal and tactical analyses that militaries must undertake in this context. In a non-international armed conflict, state militaries need to make judgments that include whether a detainee is likely to undertake violent acts against

[73] Geron, supra note 63, at 22 (noting that it requires thousands of examples to ensure a machine learning algorithm works properly, and for complex problems it may require millions of examples).

[74] For compilations of recent writings on the issue, see Dustin A. Lewis et al., Bibliography *to* War-Algorithm Accountability (2016), http://blogs.harva rd.edu/pilac/files/2016/09/War-Algorithm-Accountability-Bibliography-Only-August-2016.pdf [https://perma.cc/JE8N-AWLA]; Background Readings, The Ethics of Autonomous Weapons Systems (2014), https://www.law.upenn.edu/institutes/cerl/conferences/ethicsofweapons/background-readings.php [https://perma.cc/WMJ2-2KW7] (last visited Oct. 20, 2018).

[75] For a discussion of the extent to which states already deploy lethal autonomous weapons systems, see Rebecca Crootof, The Killer Robots Are Here: Legal and Policy Implications, 36 Cardozo L. Rev. 1837 (2015).

its armed forces if released; how committed a detainee is to the non-state armed group of which he is a part; and whether he has family and friends who are likely to persuade him to continue to fight or dissuade him from doing so. Those factors will be difficult to quantify in a coherent way in a computer algorithm.

Developing effective and defensible predictive algorithms for use in the tactical and targeting contexts will also be challenging, and the stakes are even higher because people face physical harm or even death. There are a variety of international legal rules that govern who a state may target and in what circumstances, and states may seek to translate these rules into code, so that the predictive algorithm has taken into account the outer limits of permissible force by the time it makes a recommendation. Notwithstanding these challenges, there are multiple contexts in which the military could fruitfully employ predictive algorithms to guide its tactical decision-making, helping officers answer questions about whether to patrol in neighborhood *X* or *Y* or whether a particular building is likely to contain enemy fighters.

A. Detention Algorithms

1. Legal Requirements for Detention Review

International laws of war regulate several situations in which states detain individuals. Most obviously, during international armed conflicts, states detain members of the enemy's armed forces and generally treat them as prisoners of war.[76] Because states may hold prisoners of war until the cessation of active hostilities,[77] state militaries generally do not need to make predictive detention decisions about them. However, states also detain or intern civilian protected persons during international armed conflicts. For instance, the Fourth Geneva Convention provides that states may intern protected persons who are aliens in the territory of a party to the conflict, but "only if the security of the Detaining Power makes it absolutely necessary."[78] Likewise, in occupied territory, the Occupying Power may subject protected persons to internment "[i]f the

[76] Geneva Convention Relative to the Treatment of Prisoners of War art. 4–5, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Third Geneva Convention].

[77] Id. art. 118.

[78] Fourth Geneva Convention, supra note 15, art. 41–42.

Occupying Power considers it necessary, for imperative reasons of security, to take safety measures."[79]

Custodial states are required to periodically review their decisions to intern protected persons. For aliens in the territory of a party to the conflict, interned protected persons are entitled to have their internment reconsidered

> as soon as possible by an appropriate court or administrative board designated by the Detaining Power for that purpose. If the internment . . . is maintained, the court or administrative board shall periodically, and at least twice yearly, give consideration to his or her case, with a view to the favourable amendment of the initial decision, if circumstances permit.[80]

For protected persons in occupied territory, the Occupying Power must allow an interned protected person to appeal his internment and, if the Occupying Power decides to continue to detain him, must provide a "periodical review, if possible every six months, by a competent body" set up by that Power.[81]

Further, the Fourth Geneva Convention reflects that states also may detain individual protected persons who are "definitely suspected of or engaged in activities hostile to the security of the State" without according them the full protections of that Convention."[82] However, the state must grant that individual "the full rights and privileges of a protected person . . . at the earliest date consistent with the security of the State or Occupying Power."[83] Thus, in international armed conflicts, there are several occasions on which a state must review whether an individual in its custody continues to pose a threat.

States also detain fighters and threatening civilians in non-international armed conflicts (that is, conflicts that are not between two or more states). The treaty provisions that regulate non-international armed conflicts—Common Article 3 of the Geneva Conventions and Additional Protocol II to the Geneva Conventions—provide little guidance about whom a state may detain, and contain no requirements

[79] Id. art. 78.
[80] Id. art. 43.
[81] Id. art. 78.
[82] Id. art. 5.
[83] Id.

for periodic reviews of any detentions that occur.[84] Nevertheless, the United States developed extensive review procedures in Iraq, Afghanistan, and Guantanamo for the individuals it detained in non-international armed conflicts.[85] For instance, the Defense Department established Administrative Review Boards for Guantanamo to

> assess whether each enemy combatant remains a threat to the United States and its allies in the ongoing armed conflict against al Qaida and its affiliates and supporters or if there is any other reason that it is in the interest of the United States and its allies for the enemy combatant to remain in the control of DoD. Based on that assessment, the Review Board will recommend whether the enemy combatant should continue to be detained in the control of DoD.[86]

The U.S. government established similar review procedures for detainees held by the Multinational Force in Iraq[87] and by U.S. forces in Afghanistan.[88] Each set of procedures required the government to

[84] John B. Bellinger III & Vijay M. Padmanabhan, Detention Operations in Contemporary Conflicts: Four Challenges for the Geneva Conventions and Other Existing Law, 105 Am. J. Int'l L. 201, 214, 222 (2011); see also Detention in Non-International Armed Conflict: The ICRC's Work on Strengthening Legal Protection, Int'l Comm. of the Red Cross (Apr. 21, 2015), https://www.icrc.org/eng/what-we-do/other-activities/development-ihl/strengthening-legal-protection-ihl-detention.htm [https://perma.cc/V8A4-RMZK] (identifying four key areas in which international law governing detention in relation to non-international armed conflicts falls short, including grounds and procedures for internment and transfers of detainees from one authority to another).

[85] Kathleen T. Rhem, Review Boards Assessing Status of Guantanamo Detainees, U.S. Dep't of Def. (July 8, 2005), http://archive.defense.gov/news/newsarticle.aspx?id=16694 [https://perma.cc/FP42-BHV4]; Deeks, supra note 15, at 163, 166, 167.

[86] Order from Paul Wolfowitz, Dep'y Sec. Def., regarding Administrative Review Procedures for Enemy Combatants in the Control of the Department of Defense at Guantanamo Bay Naval Base, Cuba (May 11, 2004), http://www.legal-tools.org/doc/751bad/pdf/ [http s://perma.cc/57Y8-CNT7].

[87] L. Paul Bremer, Multinational Provisional Authority Coalition Provisional Authority Memorandum No. 3 (Revised): Criminal Procedures 4–5 (June 27, 2004), http://www.refworld.org/pdfid/469cd1b32.pdf [https://perma.cc/PJC5-BEP2] (establishing review procedures for security detainees in Iraq and requiring periodic reviews); see also Brian J. Bill, Detention Operations in Iraq: A View from the Ground, 86 Int'l L. Studs. 411, 420–21 (2010) (describing review procedures).

[88] Sahr Muhammed Ally, Human Rights First, Fixing Bagram: Strengthening Detention Reforms to Align with U.S. Strategic Priorities 4-8 (2009), http://www.humanrightsfirst.org/wp-content/uploads/pdf/Fixing-Bagram-110409.pdf [https://perma.cc/X37L-4DMS] (describing and critiquing Detainee Review Boards). The Defense Department's Detainee Review Boards policy stated:

periodically evaluate whether it needed to continue to hold the person in its custody, in light of the risk the person posed (or did not pose). Other militaries that hold large numbers of detainees in non-international armed conflicts in the future may well establish similar procedures.[89]

In conducting these assessments of the type and level of threat posed by individuals in their custody, states naturally will be concerned about the security of their own forces, the stability of the situation on the ground (including during an occupation), and the safety of civilians. The more likely a person is to pose a threat if released, the less likely a state will be to release him. At the same time, states have both legal obligations and practical reasons to avoid detaining more people than they need to.[90] The uncertainties surrounding the future behavior of the individuals in custody pose challenges that appear similar to the predictive challenges that exist in the criminal justice context.

> [Continued] [i]nternment must be linked to a determination that the . . . internment is necessary to mitigate the threat the detainee poses, taking into account an assessment of the detainee's potential for rehabilitation, reconciliation, and eventual reintegration into society. If, at any point during the detainee review process, a person detained by [Operation Enduring Freedom] forces is determined not to meet the criteria detailed above or no longer to require internment to mitigate their threat, the person shall be released from DOD custody as soon as practicable.

Id. at 3 (quoting Enclosure from Letter from Phillip Carter, Deputy Assistant Sec'y Def. for Detainee Policy to Sen. Carl Levin, Chairman, S. Comm. on Armed Servs. (July 14, 2009) https://www.state.gov/documents/organization/153571.pdf [https://perma.cc/YDK4-D647] (detailing detainee review procedures at Bagram Theater Internment Facility, Afghanistan)).

[89] The United States also established procedures requiring military officers to determine whether someone met the standard for being an unlawful enemy combatant. The Combatant Status Review Tribunals at Guantanamo, for instance, were created for that purpose. Combatant Status Review Tribunals (Sept. 26, 2006), http://archive.defense.gov/news/Oct 200 6/d20061017CSRT.pdf [https://perma.cc/9A6C-NSH8] (noting that a Combatant Status Review Tribunal "is an administrative process structured under the law of war to confirm the status of enemy combatants detained at Guantanamo as part of the Global War on Terrorism"). That requires a somewhat different assessment than a threat assessment, as it is possible for someone to have been an unlawful enemy combatant at the time he was detained but to no longer pose a threat to the United States. This Article discusses in Section II.B whether the military will develop algorithms to help make combatancy-type decisions.

[90] See, e.g., Fourth Geneva Convention, supra note 15, at art. 78 (contemplating that states may only detain civilians "for imperative reasons of security"); Jeffrey Bovarnick & Jack Vrett, Detention Operations at the Tactical and Operational Levels, *in* U.S. Military Operations: Law, Policy, and Practice 307, 310 (Corn et al. ed., 2016) (noting that "detention operations impose a significant logistical burden on friendly forces").

2. Detention Review Algorithms

In light of the legal and procedural requirements just discussed,[91] it is easy to envision that militaries might seek to employ the same types of risk-assessment algorithms to make detention recommendations that domestic criminal justice systems currently employ. Most obviously, militaries might choose to use algorithms to recommend whether, after having initially detained someone for a short period, they should continue to detain that person on a longer-term basis. For a military detainee held in long-term custody, a state might also use a sophisticated, computer-based risk-assessment algorithm to help it decide whether to retain or release that detainee. These decisions are not dissimilar from the decisions made by judges in the bail context and parole boards in the post-sentencing context: Should the state insist on keeping this person in confinement in the near term? If so, at what point should it release him? At bottom, militaries seek maximally accurate predictions about whether someone is likely to return to the fight against them (or, in the Fourth Geneva Convention context, continue to pose a serious threat to the security of their forces).[92]

Would militaries have sufficient data to build a reliable algorithm for these purposes? What kinds of information would a government use to train an algorithm to make predictive recommendations about threat levels?[93] A military in the early stages of an armed conflict would be unlikely to have in its possession detailed information about members of the group it was fighting.[94] However, as the conflict progressed and the

[91] See supra Subsection II.A.1.

[92] See Rhem, supra note 85; Fourth Geneva Convention, supra note 15, art. 78.

[93] Most of the machine learning algorithms discussed here take the form of "[s]upervised machine learning," meaning that the system's authors train the model on a set of examples that are labeled—such as photographs labeled "cat or not-cat." See Emily Berman, A Government of Laws and Not of Machines, 98 B.U. L. Rev. (forthcoming 2018) (manuscript at 7) (on file with the Virginia Law Review Association) Another form of machine learning, "unsupervised" machine learning, occurs when the model's author asks the computer to identify relationships or trends within a data set. Ethem Alpaydin, Machine Learning: The New AI 111–12 (2016) (ebook), *available at* ProQuest Ebook Central. It is possible that, even with limited data, the military might choose to use unsupervised machine learning to detect a variety of patterns, and then decide for itself whether any of those patterns can help it identify people who might be members of an armed group.

[94] A similar challenge can arise in the criminal justice context. Because many of those algorithms rely heavily on a person's past criminal record when predicting future behavior, the models are less well-equipped to make accurate predictions regarding people who have just begun to engage in bad behavior. Even if someone has no criminal history, however, the government will have access to information relevant to certain other variables, including

military begins to detain enemy fighters (or threatening civilians), it would accrue more detailed information about tribal relations, neighborhoods, places the fighters live, loyalties and associations, suspicious travel routes, and enemy military tactics and techniques.[95] It also would accrue information about the subsequent behavior of those people it released (including whether those individuals returned to combat).[96] For instance, if the U.S. forces in Iraq had collected detailed and accurate information about the tens of thousands of detainees they held and released between 2003–2009 and had created algorithms similar to criminal justice bail algorithms based on that information, the United States might have been able to improve its decision-making about which detainees to hold (or transfer to the Iraqi government for criminal prosecution) and which to release.[97] Future conflicts involving large numbers of detainees pose similar prospects, both for the U.S. military and other militaries.

At a high level of generality, the Defense Science Board has anticipated that the military will employ computer-based algorithms—and possibly machine learning systems—to assist in making these types of decisions. In a 2016 study, the Board wrote:

age, gender, address, and driving record. Brad Flora, What Do the Cops Have on Me?, Slate (Dec. 4, 2007, 5:53 PM), https://slate.com/news-and-politics/2007/12/what-the-police-can-learn-when-they-run-a-background-check-on-your-name.html [https://perma.cc/T896-QL6K].

[95] The Israeli Defense Forces likely have extensive information about almost every individual they capture, particularly in their conflict with Hamas. Detention review algorithms are therefore likely to be particularly effective in this kind of conflict.

[96] See Barbara Starr, Officials: Detainee Swapped for Bergdahl Suspected of Militant Activities, CNN (Jan. 30, 2015), https://www.cnn.com/2015/01/29/politics/bergdahl-swap-prisoner-militant-activity/index.html [https://perma.cc/Z734-VLFU] (describing U.S. efforts to track certain former detainees).

[97] See Bill, supra note 87, at 411. According to news reports, many individuals who ultimately joined the Islamic State had spent time in U.S. detention in Iraq. Some were radicalized inside the U.S. facilities. Paul Sonne et al., U.S. and Britain Are Divided Over What To Do With Captured ISIS Fighters, Wash. Post (Feb. 14, 2018), https://www.washingtonpost.com/world/national-security/us-and-britain-are-divided-over-what-to-do-with-captured-isis-fighters/2018/02/14/8ad4786e-0f7f-11e8-827c-5150c6f3dc79_story.html [https://perma.cc/R8MS-ZUQR]; Brad Parks, How a US Prison Camp Helped Create ISIS, N.Y. Post (May 30, 2015), https://nypost.com/2015/05/30/how-the-us-created-the-camp-where-isis-was-born/ [https://perma.cc/XE8A-ZFZY]. This illustrates the importance of trying to predict future dangerousness, as well as the importance of understanding whom a state is holding in custody and of making informed decisions about whether to allow or prohibit certain detainees from interacting with each other.

> [The Department of Defense] will increasingly utilize software that learns and adapts for diverse applications. Such software incrementally enriches its database to describe relevant context, environment, threats, user inputs, and mission objectives. It records new input, then integrates and generalizes past experience to make decisions partly based on the accumulated data and experience.[98]

This description captures the type of work an algorithm would perform in the detention-and-release context. Part III discusses some specific challenges and controversies that might follow from the use of such algorithms.[99]

B. Military Operations Algorithms

Section II.A illustrated that the military might find criminal justice algorithms about dangerousness useful when translated into an armed conflict context. This Section argues that the military might draw inspiration from predictive policing algorithms as well, which it might use to guide its decisions about where to most efficiently direct its resources during fighting.[100] The Section first sets out relevant provisions of international law that guide military operations. It then identifies commonalities between predictive policing directed at crime hotspots and individuals associated with violence, on the one hand, and military tactical and targeting decisions, on the other. It anticipates ways in which algorithms used in the former context might inform the creation of algorithms in the latter context.

1. Legal Requirements for Military Operations

Legal requirements play an important role in shaping military operations. A wide variety of treaties and customary norms regulate how states fight armed conflicts.[101] Most critically, the law of armed conflict

[98] Def. Sci. Bd., Dep't of Def., Report of the Defense Science Board Summer Study on Autonomy 32 (2016), https://www.hsdl.org/?view&did=794641 [https://perma.cc/44TG-AHU9].

[99] See infra Part III.

[100] Little information is available about the extent to which the military already employs algorithms in this setting. One goal of this Article is to stimulate a broader public conversation about this possibility.

[101] See, e.g., Third Geneva Convention, supra note 76; Fourth Geneva Convention, supra note 15; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125

establishes rules that identify what types of objects and people a state may target and what factors the state must take into consideration before doing so. According to the principle of distinction, parties to a conflict must distinguish between civilians and civilian objects, on the one hand, and military objectives, on the other; the principle permits the parties to the conflict to direct their attacks only against the latter.[102] Military objectives are those objects which, by virtue of "their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture, or neutralization . . . offer[] a definite military advantage."[103] The principle of proportionality provides that a state may not launch an attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof that would be excessive in relation to the concrete and direct military advantage anticipated.[104] Finally, the principle of precautions states that military commanders must take constant care to spare civilians and civilian objects and that commanders must take feasible precautions to avoid, and in any event to minimize, incidental loss of civilian life, injury to civilians, and damage to civilian objects.[105] These provisions provide key rules to which state militaries must conform their conduct, whether employing algorithms or not.

Several other rules are relevant to military operations in which states might seek predictive guidance from algorithms. Particularly in non-international armed conflicts in which states are fighting an organized armed group, states face steep challenges in identifying which individuals are part of that group. The group's members may rarely wear uniforms or otherwise identify themselves, and some individuals may

U.N.T.S. 3 [hereinafter Additional Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II]; Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Oct. 10, 1980, S. Treaty Doc. No. 103-25 (1995), 1342 U.N.T.S. 137; Jean-Marie Henckaerts & Louise Doswald-Beck, Int'l Comm. of the Red Cross, 1 Customary International Humanitarian Law: Rules (2005) (ebook), https://www.icrc.org/eng/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf [https://perma.cc/KC59-2X35].

[102] Additional Protocol I, supra note 101, art. 48–52(2); Henckaerts & Doswald-Beck, supra note 101, at 3–4.

[103] Additional Protocol I, supra note 101, art. 52(2).

[104] Id. art. 51(5)(b).

[105] Id. art. 57(1).

only support the group sporadically. As a result, states and scholars have recently focused on the rule that civilians maintain their protection from attack "unless and for such time as they take direct part in hostilities."[106] The International Committee of the Red Cross ("ICRC") produced interpretive guidance suggesting that an individual only takes direct part in hostilities when his act inflicts a certain threshold of harm; directly causes harm to the enemy; and is specifically designed to directly cause the harm in support of one party to the conflict and to the detriment of another party.[107] Notwithstanding the ICRC's contribution and other writings on the issue, "[t]here is not a lot of settled law on specifically who[m] states can use force against when fighting an enemy that has an unconventional structure and tries to blend in with the civilian population."[108] Thus, the legal concept is embedded in law of armed conflict treaties, but its application is complicated and disputed.

At least two accountability-related questions arise in the application of these rules. Each accountability question is relevant to—and becomes complicated by—the prospect of using predictive algorithms in the battlefield context. The first question goes to the standard against which a military officer's performance is judged. When a commander must make a proportionality assessment, for example, by what standard will his acts be reviewed if the attack he approved resulted in wildly disproportionate harm to civilians? Generally, we ask what a "reasonable military commander" would have done in that situation.[109] The second question goes to accountability for war crimes. In general, an individual may be held responsible for a war crime when he has committed the material elements of the crime with intent and knowledge.[110] War crimes include violations of the principles of distinction and proportionality.[111]

[106] Id. art. 51(3); Additional Protocol II, supra note 101, art. 13(3).

[107] Nils Meltzer, Int'l Committee of the Red Cross, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law 46 (2009).

[108] Stephen Pomper, The ICRC's Clarification Process on the Notion of Direct Participation in Hostilities Under International Humanitarian Law, Remarks *for* Panel: Direct Participation in Hostilities: Operationalizing the ICRC's Guidance (March 27, 2009), *in* 103 Am. Soc'y Int'l L. Proc. 299, 307 (2009).

[109] Final Report to the Prosecutor by the Committee Established to Review NATO Bombing Campaign Against the Federal Republic of Yugoslavia ¶¶ 50–51 (Int'l Crim. Trib. for the Former Yugoslavia Apr. 30, 2004).

[110] Rome Statute of the International Criminal Court, art. 30, July 17, 1998, 2187 U.N.T.S. 90.

[111] Id. art. 8(2)(b)(i)–(ii), (iv).

As a result of these substantive and accountability rules, it is critical for legal compliance that militaries be able to accurately identify enemy forces and their locations (as well as the locations of civilians and civilian objects). As a strategic matter, it is important to the success of a military campaign to be able to anticipate accurately where those enemy forces will undertake future attacks or other operations, such as training or logistics supply. Presumably, state militaries would therefore welcome the ability to employ predictive algorithms that embed and reflect the requirements of international law and facilitate state compliance with it. At the same time, the complexity of translating these legal concepts into code poses serious challenges to programmers who seek to produce predictive algorithms that operate within the bounds of international law.[112]

2. *Military Tactical Algorithms*

Just as predictive policing algorithms help police identify specific geographic areas in which certain crimes are likely to occur and thus suggest to police where they might most efficiently direct their patrolling resources, so too might it be possible in the near-to-medium term for the military to develop and deploy algorithms that help it identify specific *locations* in which enemy military operations are likely to transpire. This is something that militaries have always needed to do: study predictive indicators to anticipate the enemy's course of action. The job of tactical intelligence officers—then and now—is to know the enemy.[113] Historically, military officers would study enemy doctrine (such as that of the Soviet Army), then apply the doctrine to battlefield terrain and other conditions to predict when, where, and how the enemy

[112] Similar questions have arisen in the debate about lethal autonomous weapons systems. There, the question is whether it is possible to program a robot to directly implement the rules of distinction and proportionality. Human Rights Watch, Losing Humanity: The Case Against Killer Robots 31, 33 (2012). Here, the challenge is slightly less daunting, if we assume that military officials will employ predictive algorithms to *guide* their decision-making but will not *rely exclusively* on the machine prediction to determine the most desirable way to proceed.

[113] See Jimmie L. Slade, Army Intelligence Officer: Prepared for Future Tactical and Strategic Multi-Disciplined Intelligence Tasks? 10, 48 (May 9, 1983) (unpublished thesis U.S. Army Command & Gen. Staff College) http://www.dtic.mil/dtic/tr/fulltext/u2/a136621.pdf [https://perma.cc/6A4W-K37L] (defining tactical intelligence as "[i]ntelligence which is required for the planning and conduct of tactical operations" and that "is used to make operational decisions in the field").

likely would move.[114] This traditional way of predicting enemy activity is derailed when the enemy (including groups such as the Islamic State) lacks that kind of formal doctrine. Predictive algorithms present an attractive substitute for military tactical intelligence analysis where formal enemy doctrine is absent.

Such algorithms might offer predictions about where a group of enemy forces will move next, based on thousands of examples of past enemy operations.[115] These algorithms might also be able to predict the likelihood of an imminent attack during an ongoing conflict based on pattern recognition and anomaly identification.[116] That is, algorithms could learn from bulk data what normal patterns of behavior are and could then distinguish anomalous behavior. For example, machine learning algorithms might be able to help the military identify an upsurge of Twitter usage among individuals known to associate with a particular organized armed group, and predict, based on past surges of Twitter use, the likelihood of a coming attack.[117] At an even more granular level, military algorithms might be able to detect abnormal changes in car and foot traffic that signal an impending attack of which neighborhood residents are aware. Just as police departments are using

[114] See, e.g., Dep't of the Army, Field Manual 100-5, at 2-22 (1976) ("To win battles, awareness of enemy capabilities and intentions is a prerequisite."); id. at 3-3 ("The tactical leader visualizes what terrain can do for the enemy. He then positions or maneuvers his forces on the ground to outwit and outfight the enemy.").

[115] Militaries might well employ these types of algorithms for more offensive purposes, such as to help predict where to most effectively conduct offensive operations against the enemy. In light of this Article's focus on parallels between law enforcement and military algorithms, however, it emphasizes defensive predictive algorithms, which have a closer parallel to the types of goals law enforcement officials pursue.

[116] See Naveen Joshi, Machine Learning for Anomaly Detection, Allerin (May 1, 2017), https://www.allerin.com/blog/machine-learning-for-anomaly-detection [https://perma.cc/KB4B-HWHK] (describing pattern recognition and anomaly detection).

[117] The New York City Police Department uses anomaly detection algorithms to identify sudden outbreaks of crime. Alex Chohlas-Wood et al., Mining 911 Calls in New York City: Temporal Patterns, Detection and Forecasting 2 (2015), https://aaai.org/ocs/index.php/WS/AAAIW15/paper/download/10206/10261 [https://perma.cc/8RYR-ZQ4X]; see also Louis Kratz & Ko Nishino, Anomaly Detection in Extremely Crowded Scenes Using Spatio-Temporal Motion Pattern Models, IEEE Conference on Comput. Vision and Pattern Recognition, June 2009, at 1446, https://pdfs.semanticscholar.org/eabe/8e678a77523cc2e3ae78cf4306a4948b6346.pdf [https://perma.cc/7M6C-B2PM] (discussing anomaly detection in crowded scenes on video); Romain Fontugne, Yosuke Himura & Kensuke Fukuda, Anomaly Detection Method Based on Pattern Recognition, 93 IEICE Transactions on Commc'ns 328, 328 (2010), https://www.researchgate.net/publication/220241234_Evaluation_of_Anomaly_Detection_Method_Based_on_Pattern_Recognition (discussing new anomaly detection method based on pattern recognition).

statistical models to predict where certain crimes are likely to occur, so too will the military benefit from predictions about the source and location of near-term threats.[118]

Some commentators have argued that the use of machine learning in this context will render military operations more effective and infused with fewer cognitive biases. U.S. Army cyber operations officer Charlie Lewis notes:

> [H]umans are slower, less accurate, and cannot process all of the data efficiently. . . . Machine learning used to consolidate big data, apply that data to a strategy, and make decisions in one-millionth of a second transforms the military's ability to target from an antiquated approach suitable to only capturing through constant bearing to one that is adaptable to different enemies and methods of fighting war.[119]

Lewis argues in favor of applying machine learning techniques to military operations, because those techniques will be better and faster than humans at spotting patterns and assimilating all of the information contained in the massive databases in the military's possession.[120] These techniques might also have to game out not only the enemy's "doctrine," but also how the enemy will respond to and alter its doctrine in response to actions the United States has taken. That is, the most effective algorithms will "war game" the enemy's moves in response to U.S. actions in an iterative process.

3. Military Targeting Algorithms

To some extent, the discussions in Sections II.A and II.B have artificially segregated detention and tactical decisions. But those two types of decisions are closely intertwined.[121] When the military is trying

[118] Michael L. Rich, Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment, 164 U. Pa. L. Rev. 871, 875 (2016) (stating that "police departments have recently begun to use statistical models to predict where in their jurisdictions certain crimes are likely to occur") (citing Ferguson, supra note 38, at 265–70 (providing examples)).

[119] Lewis, supra note 19. One example of such a bias could be a flawed expectation that the enemy will conduct itself the same way the U.S military would.

[120] Id. Lewis does not discuss the challenges in collecting data in sufficient quality and quantities.

[121] Matthew C. Waxman, Detention as Targeting: Standards of Certainty and Detention of Suspected Terrorists, 108 Colum. L. Rev. 1365, 1367 (2008) ("Indeed, the challenge of differentiating enemy terrorist fighters from the surrounding civilian population is a common challenge of target identification and the ability to apply force precisely: Is the individual an

to assess a detainee's dangerousness—as discussed in Section II.A—it must ask which of the detainee's actions led the military to detain the person in the first place. This assessment relates closely to whether the person is an enemy fighter (or perhaps a civilian taking direct part in hostilities). If U.S. forces raid a village to stop attacks against it, they may be on a "capture or kill" mission that requires them to identify in advance enemy combatants or members of organized armed groups based on observed patterns of life. Depending on the military's ability to collect information about daily activity in a town, algorithms might be able to identify people undertaking anomalous actions and flag those people for further analysis. As with the Beware program discussed in Part I, the military could apply similar designations (green, yellow, or red) to homes or individuals in urban warfare environments.[122] Those colors might provide the military with valuable information about which individuals merit further examination as possible threats.

This context—identifying people thought to pose a particular risk of harm to others, including the U.S. military, by using information about their past activities and associates—is roughly comparable to the type of individually focused predictive policing algorithm discussed in Section I.B. There are important differences, to be sure. In the policing context, the goal is to deter crimes.[123] In the military context, the goal is to capture or kill enemy combatants. The legal frameworks for the two types of operations are also different in critical ways.[124] Nevertheless, at a higher level of generality, both operations seek to identify and locate individuals who pose threats.

There is some evidence that U.S. military and intelligence agencies already are using algorithms to advance this goal. According to Miranda Bogen, for example, "Drone targeting is increasingly based on

enemy fighter (i.e., a combatant) and therefore subject to the application of force (i.e., capture and detention)?").

[122] Robinson & Koepke, supra note 51, at 10–11.

[123] Michael Rich identifies "automated suspicion algorithms" as programs created through machine learning processes that seek to predict individual criminality. Rich, supra note 118, at 876.

[124] Notably, the legal framework for non-international armed conflicts is more contested than it is for U.S. law enforcement operations. In particular, the rules in non-international armed conflicts regarding who may be detained remain debated and unclear. See Meltzer, supra note 107; The Future of U.S. Detention Under International Law: Workshop Report, 93 Int'l L. Stud. 272 (2017).

algorithmic calculations."[125] The Intelligence Advanced Research Projects Activity ("IARPA") reportedly is working on algorithms to deliver "anticipatory intelligence," which would allow the government to predict an event, crime, or terrorist attack before it happens.[126] The U.S. government may even have asked private companies such as Facebook whether those companies were willing to assign their own users "radicalism scores."[127] Those companies might be able to do so using image and word analysis and perhaps algorithms similar to those by which Facebook identifies suicidal thoughts or sexual predators.[128] Chris Bregler, a former New York University computer scientist now employed by Google is working with the Defense Department

> to enable surveillance cameras to detect suspicious activity from body language, gestures, and even cultural cues . . . . His prototype can also determine whether someone is carrying a concealed weapon; in

[125] Miranda Bogen, Algorithms of War, Slate (Dec. 8, 2015, 3:05 PM), http://www.slate.com/articles/technologyfuture_tense/2015/12/the_dangers_of_enlisting_algorithms_in_statecraft.html [https://perma.cc/NBZ5-ZYK9]; see also Taylor Owen, The Violence of Algorithms, Foreign Affs. (May 25, 2015), https://www.foreignaffairs.com/artic les/2015-05-25/violence-algorithms [https://perma.cc/K7PV-MR8S] (discussing increased use of algorithms for drone targeting and its consequences); Dawn Lim, Air Force Wants Smart System that Can Learn How to Detect Threats from Sensor Data, Nextgov (Aug. 10, 2012), http://www.nextgov.com/defense/2012/08/air-force-wants-smart-system-can-learn-how-detect-threats-sensor-data/57339/?oref=ng-channelriver[https://perma.cc/V3SA-YA27] (stating that Air Force wants to acquire "smart software that can help analysts identify targets from a disparate patchwork of high and low resolution imagery data" that would help detect improvised explosive devices and ground threats).

[126] James Bamford, Washington's Ministry of Preemption, Foreign Pol'y (May 31, 2017, 8:00 AM), https://foreignpolicy.com/2017/05/31/washington-ministry-of-preemption-united-states-intelligence/ [https://perma.cc/Z3ET-NBBD] (describing wide range of data streams that would provide sources of data for these algorithms).

[127] Kashmir Hill, The Government Wants Silicon Valley to Build Terrorist-Spotting Algorithms. But Is It Possible?, Splinter News (Jan. 14, 2016, 1:31 PM), https://splinternetws.com/the-government-wants-silicon-valley-to-build-terrorist-1793854067 [https://perma.cc/94NY-YMU7] (describing a tool from a company that conducts contextual word and relationship analyses and tracks social media users over time to detect individuals who exceed a certain level of radicalization).

[128] Danny Yadron & Julia C. Wong, Silicon Valley Appears Open to Helping US Spy Agencies After Terrorism Summit, The Guardian (Jan. 8, 2016, 8:49 AM), https://www.theguardian.com/technology/2016/jan/08/technology-executives-white-house-isis-terrorism-meeting-silicon-valley-facebook-apple-twitter-microsoft [https://perma.cc/NZZ5-DW9R]; Joseph Menn, Social Networks Scan for Sexual Predators, With Uneven Results, Reuters (July 12, 2012, 1:06 AM), https://www.reuters.com/article/us-usa-internet-predators/social-networks-scan-for-sexual-predators-with-uneven-results-idUSBRE86B05G20120712 [https://perma.cc/5DVZ-4KCQ].

> theory, it could analyze a woman's gait to reveal she is hiding explosives by pretending to be pregnant.[129]

The military might use variants of all of these algorithms to identify particular individuals who are members of armed groups, who are otherwise lawful targets because they are taking direct part in hostilities, or who might offer valuable intelligence if stopped and questioned. Cities pursuing predictive policing algorithms have limited budgets. State militaries, with their vast budgets and capacity to gather broad swaths of data, surely have the ability and incentive to develop algorithms at an exponentially wider and deeper scale.

III. MILITARY ALGORITHMS: PROMISES AND PITFALLS

To this point, the Article has discussed the current and future uses of predictive algorithms in the criminal justice and military contexts. At least some, if not many, uses of these algorithms could prove effective in reducing human biases and improving the quality and accuracy of human judgments. This, in turn, holds out the promise of improving the military's compliance with its international legal obligations by facilitating the systematic, measured assessment of information when making detention and targeting decisions.

Predictive algorithms generally, and machine learning techniques in particular, have come in for criticism as well as praise, though. Some of the critiques apply to the use of algorithms in government decision-making generally. Other critiques are specific to criminal justice. This Part identifies these concerns. Further, in each category of critique, it highlights the ways in which criminal justice and military algorithms likely will prove to be distinct from each other, and why military algorithms merit greater domestic oversight than military decision-making normally receives. In each case, I assume that the military is employing algorithms to guide its decision-making, but that it employs one or more officials or soldiers to make the ultimate decisions about the legality and operational propriety of detention, patrolling, tactical operations, or targeting in a given case. A desirable outcome would be that the military only employ computer algorithms that increase the

[129] Dana Liebelson, Why Facebook, Google, and the NSA Want Computers That Learn Like Humans, Mother Jones, Sept.–Oct. 2014, http://www.motherjones.com/media/2014/09/deep-learning-artificial-intelligence-facebook-nsa/ [https://perma.cc/AWT9-T46Y].

overall accuracy of its decision-making and that the military use these systems in a way that will obtain public support.

A. Quality of Data

Algorithms rely heavily on data. The quantity of data on which they are trained can render the algorithms' predictions more accurate: more examples allow machine learning algorithms to fine-tune their predictions.[130] But the quality of the data also is critical. If the data is outdated,[131] contains entry errors, or is simply factually incorrect,[132] the algorithm will fail to make accurate predictions about a new input. In the criminal justice context, a programmer might use data drawn from databases that inadvertently include duplicate records or that reflect addresses that were mis-recorded by police officers.[133] This would produce mis-weighted—and therefore inaccurate—predictions.

Likewise, an attempt to use an algorithm for one purpose when it was developed for a different purpose is likely to lead to flawed outcomes, even if the original quality of the data was high. For example, the U.S. military developed an anti-ballistic missile ("ABM") computer program that would operate in the upper atmosphere against Patriot anti-aircraft missiles. The ABM program was developed to fire on any target in that area, because all targets in the upper atmosphere were reasonably

[130] Dave Gershgorn, Can the NSA's Machines Recognize a Terrorist?, Popular Sci. (Feb. 16, 2016), http://www.popsci.com/nsas-skynet-might-not-be-able-to-tell-what-makes-terrorist [https://perma.cc/QR34-ST52]. The military appears to be aware of the need for large quantities of data to develop reliable AI systems. See Lara Seligman, The Cable, Foreign Pol'y (July 23, 2018), https://foreignpolicy.com/2018/07/23/consequences-for-iran-the-world-after-helsinki-qa-with-the-air-forces-top-weapons-buyer/ [https://perma.cc/PU46-MSDA] ("There is no reason[] that systems that have to work in some kind of autonomous mode can't have AI in them, for example surveillance drones. The issue is going to be scale. You have to put in the infrastructure and data curation that is necessary to do learning at a macro level, that means all of the data that our military produces needs to be stored in a way that can be discovered by other machines the way the internet was.").

[131] Gershgorn, supra note 130.

[132] Professor Frank Pasquale gives an example of a big data "star chamber" in which data about a person is wrong but where it is very hard for her to learn about and unwind the errors that follow from algorithmic decisions based on the initial error. The RSA, Frank Pasquale on Big Data, YouTube (July 14, 2015), at 3:09–5:35, https://www.youtube.com/watch?v=TeR0cusa yWk.

[133] Ferguson, supra note 38, at 1146, 1151.

deemed hostile.[134] However, the military later employed that same ABM program, which remained biased toward firing, in a different, lower-atmosphere context in which not all targets were necessarily hostile. As a result, the Defense Department shot down two friendly aircraft.[135]

In the military contexts discussed in Part II, the quality of data is likely to be a significant issue. One problem is that the individuals responsible for collecting the data that programmers will use to develop detention or operational algorithms may lack adequate incentives to do so carefully. For instance, a team in Iraq that was dedicated to removing improvised explosive devices ("IEDs") tried to use big data and algorithms to help stop such attacks.[136] However, the military forces that gathered the data placed a low priority on data collection, because their focus understandably was on avoiding or surviving particular IED attacks.[137] Another problem might be that the military collects only some categories of data and not others. In the IED context, IEDs that exploded produced less information than IEDs that failed to explode, leading to the irony that the U.S. government possessed better information about less effective weapons.[138] It is common that decision-makers often possess only selective pieces of information, either because they have not collected or are unable to obtain a full set of facts. Nevertheless, in the algorithmic context, this may pose a particular problem because people may treat recommendations from computer algorithms as more accurate or scientific than they actually are.[139]

A different data quality problem is likely to arise in the detention context. In contrast to the relatively high level of detail that computer scientists have about, say, people released on bail in the United States who reoffend, the military is likely to have far less granular information about the foreign resident population, at least at the beginning of the conflict. Recall that the researchers reporting on their improved bail

[134] Sydney J. Freedberg, Jr., Artificial Stupidity: Fumbling the Handoff from AI to Human Control, Breaking Defense (June 5, 2017, 7:05 PM), http://breakingdefense.com/2017/06/artificial-stupidity-fumbling-the-handoff/ [https://perma.cc/5H3P-APS4].

[135] Id.; see also Joshua Kroll et al., Accountable Algorithms, 165 U. Pa. L. Rev. 633, 681–82 (2017) (describing how choices about which data models should consider can create problems).

[136] Kelsey Atherton, When Big Data Went to War—And Lost, Politico (Oct. 11, 2017, 5:03 AM), http://www.politico.com/agenda/story/2017/10/11/counter-ied-warfare-data-project-00 0541 [https://perma.cc/X67B-6TBQ].

[137] Id.

[138] Id.

[139] See infra Section III.E (discussing automation bias).

algorithm for New York City employed a machine learning algorithm that was trained on the characteristics of more than 500,000 defendants arrested in New York City over the course of five years.[140] The researchers had access to the defendants' prior criminal records, their age, the most serious offense for which each defendant was arrested, and whether the defendant ultimately was re-arrested prior to the case resolution.[141] They also were able to test their algorithm on 200,000 other defendants' cases.[142] Other risk assessment algorithms such as COMPAS employ data such as past offenses, substance abuse, gang relationships, family and personal history, current living situation, education, work history, and arrests of and drug use by friends.[143] More generally, these algorithms are developed and used within a single society, rather than cross-culturally.

It will be far more difficult for the military to gather information at such a granular level and in such significant quantities about enemy neighborhoods, demographics, family and personal history, or employment. The algorithms it creates thus are likely to be less reliable in their predictions about individuals' future dangerousness. The best that the military is likely to be able to do is to collect information about enemies, insurgents, and others whom they have detained (or, as in the bail case, released and been able to track), to create an algorithm based on that fresh but relatively modest quantum of data. At that point, the military could then use the algorithm to inform decisions about whether to detain or release.

Further, the military presumably would want the algorithm to take into account whether the situation on the ground had changed during the time that the person was detained and whether the person is associated with a group that will remain permanently hostile to the United States (such as al Qaeda) or a group that is only fighting the United States opportunistically (such as the Mahdi Army was in Iraq). If the military seeks to employ data collected in past conflicts to help craft algorithms for the next conflict, it must take great care to use only past records that

[140] Kleinberg et al., supra note 31, at 247–48.

[141] Id. at 247.

[142] Id. at 248.

[143] Northpointe, Inc., COMPAS Risk Assessment Form, *in* Northpointe Suite Version 8.1.18.12 (2011), *available from* Julia Angwin, ProPublica, https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html [https://perma.cc/NC9Y-FBYF] [hereinafter COMPAS Risk Assessment Form].

are accurate and to avoid making easy assumptions about how individual behavior in one conflict will translate to a different conflict.[144] At the very least, the military will need to be able to defend its use of specific algorithms as "reasonable," in view of the legal accountability standard that asks what a "reasonable military commander" would have done in a given situation.[145]

To be clear, military intelligence always relies on information inputs, some of which will be more reliable and of higher quality than others. One way to ensure that military decision-making remains within the law is to treat algorithmic predictions as one (possibly important) data point in a broader intelligence analysis process. The weight that a military official gives a predictive recommendation should depend on how confident the official is about the accuracy of the computer predictions based on past performance and about how well that prediction aligns with external data points used by the military official's team in its overall intelligence analysis. At the very least, the military has an ethical and professional responsibility to ensure that any predictive algorithms on which it relies have been carefully tested and, to the greatest extent possible, periodically re-tested for accuracy.

B. Biases in Data

One of the most significant critiques of predictive algorithms stems from the fact that it is easy to inadvertently embed biases in the data on which the algorithms are trained.[146] Those building the algorithms (or those providing the data to the computer scientists) might choose data that contains gender, racial, or economic biases, which the algorithm will then replicate in its outputs. Assume, for instance, that a company builds a bail algorithm using data that takes into account how many times someone has been arrested when predicting how likely it is that he will reoffend if released on bail.[147] If the police in a given neighborhood

[144] Indeed, there might be two or more conflicts taking place inside a single area at a given time. For instance, in Iraq in the 2004–08 period, the United States was fighting al Qaeda as well as Shiite militias. The military would have to decide whether to craft distinct algorithms for these different groups, which pose different kinds of recidivist threats to the United States. I thank Sarah Grant for bringing this point to my attention.

[145] See supra note 109 and accompanying text.

[146] Ferguson, supra note 38, at 1148–49.

[147] A different type of bias could arise for "hot spot" algorithms, which employ data from police departments. That data will be biased towards those areas where police presence is already concentrated or where residents actually report crimes, because they believe police

arrest African-American men at a disproportionately higher rate than other racial groups engaged in the same activities, the algorithm will predict that African-American men will be more likely to reoffend when out on bail, even if that is not statistically true. In this example, police bias has skewed the data used to build the algorithm. A senior White House adviser in the Office of Science and Technology under President Obama noted that the data being employed in sentencing algorithms is "profoundly flawed."[148] Algorithmic biases arise in a variety of contexts but are particularly troubling where the algorithmic prediction affects a person's life or liberty.

In the criminal justice algorithm context, critiques generally revolve around racial biases.[149] In future military detainee risk assessment algorithms, other types of biases might find their way into the data. For example, a scientist building an algorithm to assess the level of risk posed by an Afghan or Yemeni detainee must be aware that possessing a weapon has reduced significance for the level of risk that a person poses, given how common it is for men to carry weapons in Afghanistan and Yemen. Computer scientists might inadvertently build a wide range of biases into algorithms unless they are keenly aware of the cultural meaning of actions in the detainee's country of origin and the area of conflict, where an action's meaning might be radically different from the meaning of the same action in the United States. Any such algorithms would very likely provide predictions that would work to the

will take steps to address the problem. The data will not necessarily reflect absolute levels of crime.

[148] Ravindranath, supra note 29.

[149] Compare Julia Angwin et al., Machine Bias, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/3VCF-W92W] (finding that COMPAS, an algorithm used to predict criminal defendants' likelihood of recidivism, "was particularly likely to falsely flag black defendants as future criminals"), and Laura Hudson, Technology Is Biased Too. How Do We Fix It?, FiveThirty Eight (July 20, 2017), https://fivethirtyeight.com/features/technology-is-biased-too-how-do-we-fix-it/ [https://perma.cc/26WV-XFNF] (arguing that data used in predictive algorithms such as COMPAS embed the racial biases of the criminal justice system in algorithmic decision-making), with Flores et al., supra note 29, at 38–40 (arguing that the analysis of COMPAS relied upon by Angwin et al. "failed to show that the COMPAS itself is racially biased, let alone that other risk instruments are biased"), and William Dieterich et al., Northpointe, COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity, Northpointe (July 8, 2016), http://go.volarisgroup.com/rs/430-MBX-989/images/ProPublica _Commentary_Final_070616.pdf [https://perma.cc/4A4N-JK3F] (reflecting response by company that produced COMPAS, claiming to refute Angwin et al.'s findings).

detriment of the military's compliance with international law and defensible detainee review policies.

C. Insufficient Transparency

Another challenge inherent in the use of machine learning is that it is often difficult for the algorithm's human user to understand precisely why the program made a particular prediction. In the context of the game of Go, an algorithm called AlphaGo Zero discovered and preferred specialized sequences of moves that it invented itself, resulting in a style of play that humans found baffling and "distinctly non-human."[150] Writing about "no fly list" algorithms, Danielle Citron notes that the list's "[system] administrators are unable to understand the logical and factual bases for the inferences made by the program."[151] There may be multiple layers of non-transparency: the inability to know that an actor is employing an algorithm;[152] the inability to obtain access to the data (or information about the types of data) on which a programmer trained an algorithm; the inability to know the algorithm's code;[153] and the inability to know or learn how the algorithm weighed values to reach an outcome, due to the highly complex nature of some machine learning processes (such as neural networks).[154]

There is a further challenge in writing algorithms: the difficulty in translating a desired policy or legal constraint into computer code. In this case, the code itself will be discoverable, but it may be very hard for all but the most expert coders to understand what types of legal,

[150] The Latest AI Can Work Things Out Without Being Taught, The Economist (Oct. 21, 2017), https://www.economist.com/news/science-and-technology/21730391-learning-play-go-only-start-latest-ai-can-work-things-out-without [https://perma.cc/K6K7-VPWD].

[151] Danielle Keats Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249, 1277 (2008).

[152] Winston, supra note 55 (noting that because the New Orleans Police Department's use of predictive algorithms was not public, "important questions about its basic functioning, risk for bias, and overall propriety were never answered").

[153] See, e.g., Wexler, supra note 9 (discussing how companies producing criminal justice technologies often insist on keeping their algorithms private for trade secret reasons). Kroll et al. explain that simply revealing source code is not generally a helpful way to improve transparency because it is unintelligible to non-experts. Kroll et al., supra note 135, at 638. Kroll et al. also note that machine learning "is particularly ill-suited to source code analysis because it involves situations where the decisional rule itself emerges automatically . . . sometimes in ways no human can explain." Id.

[154] See Larry Hardesty, Explained: Neural Networks, MIT News (Apr. 14, 2017), http://news.mit.edu/2017/explained-neural-networks-deep-learning-0414 [https://perma.cc/EA28-KBNU] (describing how neural networks work).

interpretive, or value judgments the programmer (who rarely will be a lawyer or policymaker) had to make during that translation process.

Lack of transparency along these different axes produces several problems in the military context. First, the military actors employing algorithms that produce recommendations generally will want to understand the bases on which the algorithm has made the recommendation it did. Absent what is called "explainable artificial intelligence" (or "Xai"), officials may not trust, and therefore will lose all advantage from possessing, the algorithm.[155] As one recent report put it:

> A lack of knowledge regarding the data being used (e.g. relating to their scope, provenance and quality), but more importantly also the inherent difficulty in the interpretation of how each of the many data-points used by a machine-learning algorithm contribute to the conclusion it generates, causes practical as well as principled limitations.[156]

When military officials cannot understand how and why a program reaches the recommendation it does, their overall comfort level with using the algorithm may diminish. (Of course, their discomfort may be counterbalanced against an "automation bias," discussed below.)[157] To address this concern, the military might choose to emphasize in doctrine that it is acceptable to ignore or give little weight to an algorithmic prediction where the officials do not believe that they can articulate the basis for the prediction itself.

Second, it may be especially challenging to try to translate legal concepts such as "distinction" and "proportionality" into computer code. The meaning and application of these concepts is hotly debated, even among lawyers who share common vocabularies and experiences.[158]

[155] David Gunning, Explainable Artificial Intelligence (XAI), Program Information, Defense Advanced Research Projects Agency, https://www.darpa.mil/program/explainable-artificial-intelligence [https://perma.cc/FT9F-VQKW] (discussing explainable AI and explainable machine learning as a concept).

[156] Mittelstadt et al., supra note 27, at 4.

[157] See infra Section III.E.

[158] See William H. Boothby, Direct Participation in Hostilities—A Discussion of the ICRC Interpretive Guidance, 1 J. Int'l Humanitarian L. Studs. 143 (2010) (describing distinction-related debate about when a civilian may be deemed to be directly participating in hostilities and thus be targetable); Dale Stephens & Michael W. Lewis, The Law of Armed Conflict—A Contemporary Critique, 6 Melb. J. Int'l L. 55, 62–63 (2005) (discussing complexities of the concept of proportionality).

Even if the military intends to employ a recommendation from a predictive algorithm as only one of a variety of data points to inform a decision, the military presumably would favor an algorithm that makes recommendations that are intended to fall inside the bounds of what the law requires.[159] For example, the military would presumably favor an algorithm that predicted whether a civilian was likely to continue to pose an "imperative threat to security" than an algorithm that predicted whether a civilian was likely to pose a "scintilla of a threat to security."[160] The former algorithm takes into account the international legal standard with which the military must comply, whereas the latter uses a much lower and legally irrelevant standard. The military still must extrinsically apply the legal standard during its overall analysis, but there are advantages to having an algorithm factor in legal considerations intrinsically as it develops its predictions.

Third, it will be difficult for the algorithms' users—as well as those affected by the algorithms' recommendations—to check for mistakes or challenge errors in the data inputs or in the algorithms' calculations. This has proven problematic in the criminal justice context. There have been cases in which an algorithm's owner refuses, for trade-secret reasons, to disclose why and how the algorithm evaluates people and deems them to pose a risk.[161] There also are cases in which the government refuses, under the guise of national security, to reveal why (or even whether) someone was placed on a "no fly" list.[162] It is likely to

[159] See supra Subsection II.B.1.

[160] Fourth Geneva Convention, supra note 15, art. 78 (using standard of "imperative reasons of security").

[161] Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 Stan. L. Rev. 1343, 1349–50 (2018). In one case, for instance, the company that manufactures the Beware system, which ranks people as red, yellow, or green based on predicted criminal threat level, refused to tell the Fresno, California City Council (or the police officers using the system) how its algorithm designated some people as "red," because the company would not reveal its algorithm. Robinson & Koepke, supra note 51, at 10–11.

[162] Citron, supra note 151, at 1275 (stating that individuals have no way to know whether they are in the Terrorist Screening Center's "No Fly" database). In the administrative law context, "transparency requires that agencies ensure that their decisions are 'clearly articulated' and 'the rationales for these decisions are fully explained, and the evidence on which the decisions are based is publicly accessible.'" Coglianese & Lehr, supra note 5, at 1206 (quoting Cary Coglianese et al., Transparency and Public Participation in the Federal Rulemaking Process: Recommendations for the New Administration, 77 Geo. Wash. L. Rev. 924, 926 (2009)). There is no similar requirement in the laws of armed conflict. The Fourth Geneva Convention anticipates that security internees have the right of appeal but contains

be even more challenging in the military context, where a person affected by an algorithmic recommendation may have no idea that such an algorithm exists and, even upon learning about the algorithm, may face steep technological and language hurdles to understanding its purpose and operation.[163] The hurdles to a person's ability to legally challenge the use of the algorithm in the first place are discussed below.[164]

There is reason to be optimistic that the military will insist on some level of explicability for its algorithms, based on the directions that its research seems headed.[165] That means there might also be reason to expect that those affected by the algorithmic recommendations (such as detainees who continue to be held for threat reasons) would be able to glean some limited information about why the algorithm operated the way it did. Extensive transparency seems highly unlikely, however, particularly where it might pose a security risk to reveal the data that went into the creation of a given algorithm.

D. Insufficient Oversight and Accountability

One persistent concern about the use of algorithms is that it can be challenging to oversee whether they are being used appropriately and to determine whom to hold accountable for algorithmic errors or other types of misuse. This type of accountability question arises in the criminal justice context. Consider a situation in which a judge relies on an algorithmic recommendation to sentence a defendant to a longer sentence than she otherwise might have, even though it turns out that the algorithm was flawed. Should we blame the algorithm writer, the

no express requirement that the detaining power share threat information with the internees. Fourth Geneva Convention, supra note 15, art. 43, 78.

[163] Mittelstadt et al., supra note 27, at 6 ("However, data subjects retain an interest in understanding how information about them is created and influences decisions taken in data-driven practices. This struggle is marked by information asymmetry and an 'imbalance in knowledge and decision-making power' favouring data processors." (citation omitted)).

[164] See infra Subsection IV.A.2.

[165] Sydney Freedberg, Jr., Artificial Stupidity: Learning to Trust Artificial Intelligence (Sometimes), Breaking Defense (July 5, 2017, 2:26 PM), http://breakingdefense.com /2017/07 /artificial-stupidity-learning-to-trust-the-machine/ [https://perma.cc/Q2AL-6STT] (discussing the importance of understanding and trusting what an AI machine is doing, even if it comes at the cost of performance loss); Gunning, supra note 155 (discussing the Department of Defense's interest in developing explainable artificial intelligence).

company for which she works, the judge, or the judicial system that has provided the judge with the algorithmic tool?

This accountability debate has been highly salient in the context of lethal autonomous weapons systems, where groups such as Human Rights Watch have argued that it is unclear who to hold responsible for attacks by fully autonomous robots.[166] Another set of authors has characterized the question of algorithmic accountability in the military context as a question about how to fulfill the "'duty to account . . . for the exercise of power' over—in other words, holding someone or some entity answerable for—the design, development, or use (or a combination thereof) of a war algorithm."[167] In the detention and targeting algorithm context, is it the engineer who developed the program?[168] The members of the armed forces who compiled the data that the engineer used to train the algorithm? Or higher-level officials in the Defense Department who authorized military officers to use algorithm?[169] Even if there will be few opportunities to impose algorithmic accountability in the detention and targeting context if an error occurs, at the very least the military will need to determine the source of the error to improve the reliability of that algorithm. In addition, there are increasing numbers of initiatives within engineering communities to inculcate ethical values into the design of algorithms; the military should actively seek to support these initiatives.[170]

A second, related concern is whether affected individuals have the ability to legally challenge the use of algorithms in specific cases, such as where a person has a reasonable belief that the algorithm has provided a flawed recommendation and the government has acted on

[166] Human Rights Watch, Losing Humanity: The Case Against Killer Robots 4, 42–45 (20 12) (discussing possibility of holding responsible the manufacturer, military commander, programmer, and the robot itself).

[167] Lewis et al., supra note 74, at viii (citation omitted).

[168] See Geoffrey S. Corn, Autonomous Weapons Systems: Managing the Inevitability of "Taking the Man Out of the Loop," *in* Autonomous Weapons Systems: Law, Ethics, Policy 209, 224–35 (Nehal Bhuta et al. eds., 2016) (arguing in favor of placing greater responsibility on the actors who developed and approved the algorithm).

[169] See Lewis et al., supra note 74, at 26–29 (discussing Department of Defense directives assigning responsibility for the conduct of autonomous weapon systems in part to officials authorizing the use of such weapon systems).

[170] See, e.g., Ethics in Action, Inst. Electrical & Electronics Engineers, https://ethicsinaction.ieee.org/ [https://perma.cc/UYR5-D5UZ] (presenting initiatives for the ethical design of autonomous systems, predictive algorithms, and artificial intelligence) (last visited Sept. 11, 2018).

that recommendation. In the criminal justice context, various criminal defendants have challenged their sentences or parole denials on the grounds that the decision-makers relied on a flawed algorithm.[171] Most prominently, the U.S. Supreme Court recently denied certiorari in *Wisconsin v. Loomis*, in which the defendant argued that the judge had violated the defendant's due process rights by relying on the COMPAS algorithm at sentencing.[172] The company claimed proprietary rights to the software and thus made it impossible for the defendant to challenge the accuracy and scientific validity of the algorithm's assessment.[173]

In non-international armed conflicts, there often will be even fewer available fora in which individuals affected by military algorithms may challenge their detention, because international law does not require states to establish such fora. Further, as discussed infra in Part IV, external oversight of military activities is far less robust than oversight of law enforcement activities, both as a legal and practical matter. In the criminal justice context, there are usually clear avenues for defendants to challenge actions taken against them, using tools such as the Fourth and Fourteenth Amendments and, in particular, the exclusionary rule. Yet even here, courts have declined to scrutinize the state's and judge's use of algorithms.[174] Nor have they required companies to provide the algorithms to the defendants. In the military context, where detention and targeting play out in armed conflicts in foreign countries, there are far fewer legal protections for detainees and people who are (or whose relatives have been) military targets and very few opportunities for Article III courts to oversee the military's exercise of power. As a result, the costs of getting it "wrong" are lower for the military and are higher for affected individuals. It is easy to imagine how difficult it will be to obtain satisfactory levels of oversight of the use of detention and targeting algorithms, both because of reduced legal protections and

[171] See Wexler, supra note 161, at 1369–70 (discussing cases in which criminal defendants have challenged the use of algorithms associated with sentencing and parole).

[172] 881 N.W.2d 749, 753 (Wis. 2016); SCOTUSblog, supra note 42.

[173] Brief for the United States as Amicus Curiae at 13, Loomis v. Wisconsin, 137 S. Ct. 2290 (2017) (No. 16-6387), https://www.justice.gov/sites/default/files/brief s/2017/05/30/16 -6387_loomis_ac_pet.pdf [https://perma.cc/CDB5-GFU8].

[174] The United States itself conceded that "[a] sentencing court's use of actuarial risk assessments raises novel constitutional questions" and that "the lack of transparency [about the algorithm could] raise serious issues." Id. at 12.

because detainees and the families of those targeted will lack the knowledge and resources to evaluate the process.[175]

E. Automation Biases

Some studies have illustrated that individuals experience "automation bias," which constitutes an undue willingness to accept a machine's recommendation or a failure to act because a machine has not prompted one to do so.[176] Professor Frank Pasquale has criticized the use of risk assessment algorithms in the criminal justice context in part because judges are susceptible to automation bias.[177] He argues, "Judges are all too likely to assume that quantitative methods are superior to ordinary verbal reasoning, and to reduce the task at hand (sentencing) to an application of the quantitative data available about recidivism risk."[178] Others worry that the judicial use of algorithms will make judging more rote over time, because when people receive advisory guidelines, they tend to follow them rather than to use their own judgment.[179]

This type of bias is just as likely—if not more likely—to appear in the military context. One literature review notes that workload, task complexity, and time constraint, all of which place a person's cognitive resources under pressure, increase the amount of automation bias a person suffers.[180] Military operations typically occur under greater time

[175] See Mittelstadt et al., supra note 27, at 6.

[176] Kate Goddard et al., Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators, 19 J. Am. Med. Inform. Assoc. 121, Jan.–Feb. 2012, https ://www.ncbi.nlm.nih.gov/pmc/articles/PMC3240751/ [https://perma.cc/ 2JAT-QRSG]; see also Citron, supra note 151, at 1271 ("Eligibility workers' intuitive trust in computer systems tends to reduce the value of human participation in mixed systems . . . . Operators of automated systems tend to trust a computer's answers."); id. (referring to human "automation bias"); Raja Parasuraman & Dietrich H. Manzey, Complacency and Bias in Human Use of Automation: An Attentional Integration, 52 Hum. Factors 381 (2010), https://www.researchgate.net/publication/47792928 [https://perma.cc/96XD-2ZTM] (concluding that both expert and inexpert participants suffer from complacency and bias in human interaction with automated systems); Robinson & Koepke, supra note 51, at Executive Summary (describing people's tendency to unduly trust computer predictions).

[177] Frank Pasquale, Secret Algorithms Threaten the Rule of Law, MIT Tech. Rev. (June 1, 20 17), https://www.technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law / [https://perma.cc/AYM5-GSH3].

[178] Id.

[179] Associated Press, Artificial Intelligence is Coming for Both Judges and Defendants, N.Y. Post (Jan. 31, 2018), https://nypost.com/2018/01/31/artificial-intelligence-is-coming-for-both -judges-and-defendants/ [https://perma.cc/QWB8-SB2U].

[180] Goddard et al., supra note 176, at 124–25.

pressure than criminal justice decision-making. Depending on the type of operation, military operators might be asked to undertake several complex tasks at once. Further, the average military operator is presumably more familiar and comfortable with technology than the average judge. From this we might conclude that the military operator willingly would place even more confidence in a computer recommendation than a judge would.

F. Public Perceptions

A final challenge that the use of predictive algorithms generally (and machine learning algorithms in particular) must overcome, at least at this stage of their development, is a generalized public distrust of their use.[181] Some of this may stem from a perception that the use of predictive algorithms to make decisions that affect people's lives is dehumanizing. In the criminal justice context, for instance, algorithmic models lack access to all of the softer types of data that humans have access to—such as a judge's perception about a defendant's sense of regret (or lack thereof) at a sentencing hearing. Other sources of distrust include reports about the use of biased algorithms[182] and high-profile stories about egregious algorithmic mistakes, such as when Amazon's machine learning algorithm began to recommend bomb-making products to be sold together.[183] In the military context, some have argued that only humans, exercising human capabilities, should be responsible for restraining another person's liberty or taking another person's life.[184] In this view, we should be skeptical about accepting recommendations from machines to conduct these acts. At the very least, the military should decide that it will not rest its decision-making entirely on a recommendation from a predictive algorithm.

[181] Vyacheslav Polonski, People Don't Trust AI—Here's How We Can Change That, Sci. Am. (Jan. 10, 2018), https://www.scientificamerican.com/article/people-dont-trust-ai-heres-how-we-can-change-that/ [https://perma.cc/8FLB-XUGD].

[182] See, e.g., COMPAS Risk Assessment Form, supra note 143.

[183] Paul Sandle, Amazon Reviewing Website After Algorithm Suggests Bomb-Making Ingredients, Reuters (Sept. 20, 2017), https://www.reuters.com/article/us-britain-security-amazon-com/amazon-reviewing-website-after-algorithm-suggests-bomb-making-ingredients-idUSKCN1BV1WK [https://perma.cc/33SS-95UZ].

[184] Human Rights Watch, supra note 166.

IV. OPENING THE BLACK BOX

Part III identified specific ways in which the military's use of predictive algorithms will be more complicated than the criminal justice system's use of these algorithms. But there is a deeper, more systemic difference as well. Military operations, which generally happen overseas and which often require high levels of classification, tend to operate in much more of a legal and operational "black box" than criminal justice processes, which are generally public and are governed by the Constitution, highly developed domestic statutes, and ample case law. This is one reason why the military might expect—indeed, might hope—that its growing turn to predictive algorithms and machine learning systems will remain mostly out of the public eye.[185] But it is for precisely this reason that the military, the public, and Congress should resist keeping the United States' use of predictive algorithms obscured. For the result would be to nestle the "black box" of machine learning algorithms inside the existing "black box" of military operations.[186] This approach risks subverting the values of reasoned decision-making and government accountability.

Instead, the military should pursue a different approach, one that entails a much greater focus on transparency. Doing so will require it to fight its institutional instincts but will pay dividends. One key lesson from the post-September 11 era—which saw the use of highly classified and highly controversial tools such as secret detention facilities, renditions, and enhanced interrogation techniques—is that deep secrecy and efforts to conceal the strategic direction of military (and intelligence) operations often boomerang back against the United States. In the post-September 11 era, it resulted in diminished cooperation from allies and serious reputational damage.[187] The military should learn that

[185] The U.S. military is not the only state military for which this is true. Israel may also favor legal ambiguity about its operations. See Yoni Eshpar, Legal Transparency as a National Security Strategy, 5 Mil. & Strategic Aff. 3, 15 (2013), http://www.inss.org.il/wp-content/u ploads/systemfiles/MASA5-1Eng4_Eshpar.pdf [https://perma.cc/W2WK-GCCT] ("Legal ambiguity appears to be the preferred choice [for the Israeli military] not only for diplomatic and security reasons, but also as a political necessity.").

[186] For an early use of the description of algorithms as "black boxes," see Frank Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information (2015).

[187] See e.g., Nicholas Fandos, Senate Confirms Gina Haspel to Lead C.I.A. Despite Torture Concerns, N.Y. Times (May 17, 2018), https://www.nytimes.com/2018/05/17/us /politics/haspel-confirmed.html [https://perma.cc/34RN-MGZQ] (quoting Gina Haspel as conceding that the CIA's detention and interrogation program "did damage to our officers

lesson here, clarifying publicly the laws, policies, and principles that will inform its use of predictive algorithms (and perhaps artificial intelligence more broadly), while continuing to protect specific, detailed data, predictions, and military operations.

Being transparent about why the military chooses to use predictive algorithms, what advantages these algorithms (and particularly machine learning) offer, how the military plans to ensure that their use is consistent with the law, what the costs of using them will be, and how the military intends to mitigate those costs will go a long way toward attracting public and allied support for this latest turn in warfare. We know that reason-giving in a democracy, including by administrative agencies and courts, can enhance the legitimacy of decisions, improve the quality of decisions, evidence respect for the decision-maker's audience, and ensure that public officials offer public-regarding justifications for their choices.[188] The military should give public reasons for its use of predictive algorithms and measured explanations about how it intends to use them, as doing so would produce some of the same advantages that courts and administrative agencies derive from public reason-giving.[189]

A. The September 11 Black Box

It seems fair to describe U.S. counter-terrorism practices in the years immediately following the September 11 attacks as a black box. Especially between 2001 and 2006, the U.S. government conducted a range of very highly classified military and intelligence operations

and our standing in the world"); Douglas A. Johnson, Alberto Mora & Averell Schmidt, The Strategic Costs of Torture, Foreign Affs. Sept.–Oct. 2016, at 121, 122, https://www.foreignaffairs.com/article s/united-states/strategic-costs-torture [https://perma. cc/DQ9Y-DYR7] (stating that the United States' use of torture "hindered cooperation with U.S. allies" and "undermined U.S. diplomacy").

[188] Martin Shapiro, The Giving Reasons Requirement, 1992 U. Chi. Legal F. 179, 180–81 (1992); Glen Staszewski, Reason-Giving and Accountability, 93 Minn. L. Rev. 1253, 1278 (2009); Edward H. Stiglitz, Bureaucratic Reasoning 11–16 (unpublished manuscript) (on file with author) (describing various virtues of reason-giving).

[189] See Ashley S. Deeks, The Obama Administration, International Law, and Executive Minimalism, 110 Am. J. Int'l L. 646, 661 (2016) ("One fairly might take the view that the world's dominant military power should be more forthcoming about its legal theories and defend them publicly with more reason-giving."); Eduardo Jordão & Susan Rose-Ackerman, Judicial Review of Executive Policymaking in Advanced Democracies: Beyond Rights Review, 66 Admin. L. Rev. 1, 52 (2014) (noting that reason-giving is a partial compensation for deficits of legitimacy that affect independent agencies).

against al Qaeda and, to a lesser extent, the Taliban. At the time, the U.S. government saw itself as facing an unprecedented threat and concluded that it needed to employ a host of novel and controversial tools in order to defeat further similar attacks.[190] Many of these programs tested the outer limits of the law. The government kept these programs highly classified not only to advance operational security, but also presumably to avoid legal controversies that would have quickly arisen if the government had made the programs public.[191]

1. Opaque Programs

The United States employed a variety of tools to capture, detain, interrogate, and target members of al Qaeda. First, the United States used renditions to transport detainees from one country to another; in some cases the detainees suffered harsh treatment from the receiving state.[192] Second, the CIA opened several "secret sites" in foreign countries, at which CIA employees held and interrogated high-value detainees and denied those individuals access to visits by the ICRC.[193]

[190] President George W. Bush, President Discusses Creation of Military Commissions to Try Suspected Terrorists (Sept. 6, 2006), https://georgewbush-whitehouse.archives.gov/news/releases/2006/09/20060906-3.html [https://perma.cc/6Q8M-A4HJ] (discussing the need to "wage an unprecedented war against an enemy unlike any we had fought before") [hereinafter Military Commissions Discussion].

[191] See, e.g., Anne D. Miles, Cong. Research Serv., R43906, Perspectives on Enhanced Interrogation Techniques (2016), https://fas.org/sgp/crs/intel/R43906.pdf [https://perma.cc/HMZ4-8NTA] (describing range of views on CIA's interrogation techniques); Jack Goldsmith, The Terror Presidency 182 (2007) (stating that the White House found it easier to pursue the Terrorist Surveillance Program in secret because it was not on solid legal footing); Ashley S. Deeks, A (Qualified) Defense of Secret Agreements, 49 Ariz. St. L.J. 713, 758 (2017) (noting that it likely violated the domestic and international legal obligations of CIA partner states to host the CIA's secret detention facilities); Massimo Calabresi, Senate Torture Report Describes CIA Interrogation Program, Time (Dec. 9, 2014), http://time.com/3625453 /torture-report-senate-cia-interrogation/ [https://perma.cc/8KEU-KH5H] (quoting President Obama as stating, "These techniques did significant damage to America's standing in the world and made it harder to pursue our interests with allies and partners").

[192] Max Fisher, A Staggering Map of the Fifty-Four Countries That Reportedly Participated in the CIA's Rendition Program, Wash. Post (Feb. 5, 2013), https://www.washingtonpost.com/news/worldviews/wp/2013/02/05/a-staggering-map-of-the-54-countries-that-reportedly-participated-in-the-cias-rendition-program/?utm_term=.917f363be3a4 [https://perma.cc/HN7 3-4HDB].

[193] Paul Reynolds, Report Claims CIA Used "Torture", BBC News (Mar. 16, 2009, 4:17 PM), http://news.bbc.co.uk/2/hi/americas/7945783.stm [https://perma.cc/79XV-4DHC] (noting that the ICRC was denied access to the detainees until the U.S. government transferred them to Guantanamo).

Third, the government used harsh interrogation techniques against high-value members of al Qaeda, techniques that exceeded those that the military and intelligence operators had used previously.[194] Fourth, using what now is commonly called "targeted killings," the United States began in 2002 to target and kill members of al Qaeda in regions such as Yemen and Pakistan, which were not then areas of active military hostilities.[195] Fifth, the United States transferred hundreds of individuals to a detention facility at Guantanamo Bay Naval Base with the expectation that those detainees would not be able to file habeas corpus petitions.[196]

These programs eventually came to light in a variety of ways. Some were revealed through leaks.[197] Some became public through a combination of journalists' and foreign citizens' investigations, as when "plane spotters" recorded the flight patterns of small aircraft that seemed to mirror suspected CIA rendition paths.[198] In some cases, affected individuals sued in federal court to challenge their detention[199] or treatment.[200] In yet other cases, the government altered its own policies sua sponte, as when the government closed the CIA's secret sites and transferred a number of high-value members of al Qaeda from those sites to Guantanamo.[201] Regardless of how these programs came to light, they each proved highly controversial once made public and reminded

[194] See S. Rep. No. 113-228, at xix (2014).

[195] Eben Kaplan, Q&A: Targeted Killings, N.Y. Times (Jan. 25, 2006), http://www.nytimes.com/cfr/international/slot3_012506.html?pagewanted=print [https://perma.cc/W9Z6-JYRK] (discussing 2002 targeting of senior al Qaeda leader Abu Ali al-Harithi in Yemen and 2006 strike against targets in northern Pakistan, among other examples).

[196] Memorandum from Patrick F. Philbin & John C. Yoo, Deputy Assistant Attorneys General, Office of Legal Counsel, Dep't of Justice, to William J. Haynes II, General Counsel, Dep't of Defense, (Dec. 28, 2001) (advising Haynes that the "great weight of legal authority indicates that a federal district court could not properly exercise habeas jurisdiction over an alien detained at [Guantanamo Bay]").

[197] See, e.g., Dana Priest, CIA Holds Terror Suspects in Secret Prisons, Wash. Post (Nov. 2, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/11/01/AR2005110101644.html [https://perma.cc/W9DG-C8TB] (revealing existence of CIA "black sites").

[198] Scott Shane, C.I.A. Expanding Terror Battle Under Guise of Charter Flights, N.Y. Times (May 31, 2005), https://www.nytimes.com/2005/05/31/us/cia-expanding-terror-battle-under-guise-of-charter-flights.html [https://perma.cc/2KU4-5N4N].

[199] Boumediene v. Bush, 553 U.S. 723, 732 (2008); Hamdi v. Rumsfeld, 542 U.S. 507, 511 (2004).

[200] Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1073 (9th Cir. 2010) (en banc); El-Masri v. United States, 479 F.3d 296, 299 (4th Cir. 2007).

[201] Military Commissions Discussion, supra note 190.

many commentators that national security secrecy can serve to conceal programs that the public might not support.

2. *Systems Perpetuating Opacity*

The U.S. system contains a variety of legal and political structures and doctrines that perpetuate the Executive's dominance in the national security sphere relative to the other branches of government. Many of these systems and doctrines concomitantly perpetuate the opacity and unreviewability of the Executive's national security decisions. From an inter-branch perspective, checks and balances are notoriously weak in the context of executive decision-making about national security issues. Because so much military and intelligence activity is classified, Congress and the public have difficulty learning about the substance of and rationales behind the decisions the Executive has made.[202] Even when Congress has a well-specified oversight role and has enacted statutes that require the Executive to provide it with specific information,[203] the Executive still retains dominant control over national security information.[204]

The courts, too, play a limited role in overseeing executive actions and checking excessive uses of power. Courts tend to be highly deferential to the Executive in foreign affairs and national security, because they worry about their own technical incapacity and lack of

[202] See, e.g., 158 Cong. Rec. S6793–94 (daily ed. Nov. 14, 2012) (statement of Sen. Wyden) ("I can recall numerous specific instances where I found out about serious government wrongdoing . . . only as a result of disclosures by the press."); Press Release, Sen. Ron Wyden, Wyden: The Public Must Know How Many Americans Are Swept Up In Warrantless Surveillance Under FISA 702 (Mar. 15, 2017), https://www.wyden.senate.gov/news/press-releases/wyden-the-public-must-know-how-many-americans-are-swept-up-in-warrantless-surveillance-under-fisa-702 [https://perma.cc/T32F-6RW3] (stating that Sen. Wyden has pressed intelligence leaders "for years" to reveal how many Americans are "caught up" under a surveillance program aimed at overseas targets).

[203] See, e.g., 50 U.S.C. § 3091(a)(1) (2012) (requiring the Executive to keep the congressional intelligence committees "fully and currently informed of the intelligence activities of the United States"); § 3093(b)(1) (requiring the Executive to keep the House and Senate intelligence committees "fully and currently informed of all covert actions").

[204] For a recent example of the Executive's position on this issue, see Letter from Donald F. McGahn II, Counsel to the President, The White House, to Rep. Devin Nunes, Chairman, House Permanent Select Committee on Intelligence (Feb. 2, 2018), https://lawfareblog.com/document-nunes-memo [https://perma.cc/B9AJ-9SQE] (reminding Congress that "it is the President's responsibility to classify, declassify, and control access to information bearing on our intelligence sources and methods and national defense") (citing Dep't of Navy v. Egan, 484 U.S. 518, 527 (1988)).

democratic accountability.[205] Even where plaintiffs try to use the courts to challenge executive decisions, a variety of doctrines and privileges—including standing, ripeness, the political question doctrine, and the state secrets privilege—often preclude litigation on the merits. For instance, a court concluded that individuals were barred by the political question and standing doctrines from challenging U.S. government efforts to target an American citizen in Yemen.[206] Other courts rejected challenges by detainees who claimed to have been subject to rendition and mistreatment by the CIA, based on the state secrets privilege.[207] As a result, we have come to rely on additional (though less predictable) tools such as leaks, inter-agency tensions, and pressure from foreign allies to help check an Executive that is only lightly accountable.

Putting aside the merits of these court decisions, the broader point is that intelligence and military activities are difficult to challenge judicially and can be difficult for Congress to oversee.[208] There are, of course, important exceptions, and executive branch complacency about judicial deference has at times proven costly,[209] but the overall impression often is that these activities operate from within a black box. And in many cases reasonable people may disagree about the merits of those activities. Notwithstanding the fact that shining light on the activities might prompt difficult public discussions, the government has sometimes concluded that there is strategic value in being more transparent about what happens inside the national security black box.

B. Opening the Strategic Black Box

One unintended and ironic consequence of the U.S. efforts to keep its post-September 11 detention and interrogation programs so secret is that they faced a particularly harsh spotlight when they became public. Not only did the secrecy allow programs to continue that would have lacked support among various corners of the U.S. citizenry, but it also arguably

[205] See, e.g., Al-Aulaqi v. Obama, 727 F. Supp.2d 1, 51–52 (D.D.C. 2010).

[206] Id. at 9.

[207] Mohamed v. Jeppesen Dataplan, 614 F.3d 1070, 1092 (9th Cir. 2010) (en banc); El-Masri v. United States, 479 F.3d 296, 313 (4th Cir. 2007).

[208] See, e.g., Amy B. Zegart, The Domestic Politics of Irrational Intelligence Oversight, 126 Pol. Sci. Q. 1 (2011).

[209] See, e.g., Hamdan v. Rumsfeld, 548 U.S. 557, 567 (2006); Rasul v. Bush, 542 U.S. 466, 473 (2004).

intensified the legal and policy criticisms that followed.[210] Further, the spotlight on U.S. detention and war-fighting endures.[211] One way to manage this spotlight is to confront it directly by explaining both the law and policies that undergird these operations. Officials in the second term of the Bush administration and in both terms of the Obama administration pursued this approach along several axes. By outlining the governing law, policies, and principles, the administrations made inroads toward reducing challenges to and skepticism of some of these programs.[212] (The government terminated the use of some of the post-September 11 programs entirely, such as the use of harsh interrogation techniques[213] and secret sites.)[214]

This move toward greater transparency—at least at a level of generality that does not reveal operational details—should resonate with a military (and an intelligence community) that is embarking on the use of artificial intelligence, machine learning, and predictive algorithms. Although the goal of many algorithms is to increase the reliability of government prediction and decrease decisional biases, this Article has shown that the use of algorithm-driven decision-making raises thorny questions about the transparency of the algorithms, the values inherently embedded in the algorithms, the ability of the military to use algorithms in a manner consistent with legal rules, and the difficulty in deciding whom to hold accountable for decisions based on those algorithms. Part II illustrated that detention and targeting are two of the areas in which

[210] See President John F. Kennedy, The President and the Press: Address Before the American Newspaper Publishers' Association (Apr. 27, 1961), https://www.jfklibrary.org/Research/Research-Aids/JFK-Speeches/American-Newspaper-Publishers-Association_1961042 7.aspx [https://perma.cc/7UMB-PRT2] (arguing that "the dangers of excessive and unwarrant ed concealment of pertinent facts far outweighed the dangers which are cited to justify it").

[211] See, e.g., Lawrence Hurley, U.S. Court Blocks Transfer of American Detainee Held in Iraq, Reuters (May 7, 2018), https://www.reuters.com/article/us-usa-court-detainee/u-s-court-blocks-transfer-of-american-detainee-held-in-iraq-idUSKBN1I82E2 [https://perma.cc/UF5Y-4RZ8]; Warren Strobel & Jonathan Landay, Exclusive: As Saudis Bombed Yemen, U.S. Worried About Legal Blowback, Reuters (Oct. 10, 2016), https://www.reuters.com/article/us-usa-saudi-yemen/exclusive-as-saudis-bombed-yemen-u-s-worried-about-legal-blowback-idUSKCN12A0BQ [https://perma.cc/QQP4-4V37].

[212] Eshpar, supra note 185, at 11–12 (noting that "criticism of the administration's legal and ethical record by the Congress, the media, and human rights organizations remained limited for most of Obama's first term").

[213] Exec. Order No. 13,491, 3 C.F.R. 2009 Comp., 199 (2010).

[214] Id. at 201 (ordering the CIA to close any detention facilities it was operating); Military Commissions Discussion, supra note 190 (announcing closure of CIA secret sites).

the military is likely to use predictive algorithms, including machine learning algorithms. The thread that unifies the critiques outlined in Part III is a lack of transparency—about what types and quality of data the military is using; about whether and how the military will attempt to build legal requirements into computer code; and about how the military will address automation bias to avoid relying on predictive algorithms where the situation does not warrant it.

Faced with looming developments in artificial intelligence, the military should build on the lesson that the Bush and Obama administrations ultimately learned: there are advantages to be gained by publicly confronting the fact that new tools pose difficult challenges and tradeoffs, by giving reasons for their use, and by clarifying how the tools are used, by whom, and pursuant to what legal rules. What follows are some examples of efforts by those administrations to unpack the black box of law and policy in the counter-terrorism context. These examples illustrate that the government can pursue a significant level of transparency in the national security space without imposing undue costs on how military programs function.

1. The Legal Framework

One source of anxiety surrounding the U.S. use of force against members of al Qaeda and other forces associated with that group was an uncertainty about what legal theories undergirded the United States' armed conflict with a non-state group. In a speech to a European audience in 2006, then-State Department Legal Adviser John Bellinger described an "intensive and ongoing dialogue with European government officials about U.S. counterterrorism laws and policies, especially those relating to the detention, questioning, and transfer of members of al Qaida and the Taliban."[215] Some imagined that the legal claims were broader than they actually were, while others had not been informed about the U.S. legal arguments.[216] Years later, members of the U.S. Congress who sat on the intelligence committees and who favored the targeted killing policy argued that the Obama administration should increase transparency about the policy and its legal underpinnings.

[215] John B. Bellinger III, Legal Adviser, U.S. Dep't of State, Legal Issues in the War on Terrorism, Address Before the London School of Economics, (Oct. 31, 2006), https://2001-2009.state.gov/s/l/rls/76039.htm [https://perma.cc/CU4P-3UZT].

[216] Id.

Senator Dianne Feinstein, then chairwoman on the Senate Select Committee on Intelligence, asked the administration to "make public its legal analysis on its counterterrorism authorities."[217] She argued that "for both transparency and to maintain public support of secret operations, it is important to explain the general framework for counterterrorism actions."[218]

Both the second Bush administration and the Obama administration ultimately responded to insistent calls for greater clarity about the legal framework for fighting al Qaeda. First, the administrations' senior national security officials—including senior legal officials from the Departments of Defense and State and from the CIA, as well as senior counterterrorism officials from the Obama White House—made a concerted effort to give public speeches that delineated the legal boundaries of the United States' use of force against al Qaeda.[219] Second, at the end of the Obama administration, the White House released a sixty-six-page report on the legal and policy frameworks that guide the United States' use of military force and other national security operations.[220] In that context, President Obama noted:

> Decisions regarding war and peace are among the most important any President faces. It is critical, therefore, that such decisions are made pursuant to a policy and legal framework that affords clear guidance internally, reduces the risk of an ill-considered decision, and enables the disclosure of as much information as possible to the public, consistent with national security and the proper functioning of the

[217] Peter Finn, Political, Legal Experts Want Release of Justice Dept. Memo Supporting Killing of Anwar al-Awlaki, Wash. Post (Oct. 7, 2011) https://www.washingtonpost.com/world/national-security/political-legal-experts-want-release-of-justice-dept-memo-supporting-killing-of-anwar-al-awlaki/2011/10/07/gIQABCV9TL_story.html [https://perma.cc/TL4J-KMUV].

[218] Sari Horwitz & Peter Finn, Holder Expected to Explain Rationale for Targeting U.S. Citizens Abroad, Wash. Post (Mar. 4, 2012) https://www.washingtonpost.com/world/national-security/holder-expected-to-explain-rationale-for-targeting-us-citizens-abroad/2012/03/04/gIQACz41qR_story.html [https://perma.cc/7VDE-R8U4].

[219] Kenneth Anderson & Benjamin Wittes, Speaking the Law: The Obama Administration's Addresses on National Security Law 5 (2015); Bellinger, supra note 215.

[220] The White House, Report on the Legal and Policy Frameworks Guiding the United States' Use of Military Force and Related National Security Operations (2016), https://www.justsecurity.org/wp-content/uploads/2016/12/framework.Report_Final.pdf [https://perma.cc/2WR4-3YDY].

> Government, so that an informed public can scrutinize our actions and hold us to account.[221]

The report delineated the relevant international and domestic law and articulated how that law applied in six key theaters of conflict.[222]

The Obama administration also clarified what the legal rules were *not*. One way it did so was by declassifying and releasing certain Department of Justice memos that approved the use of enhanced interrogation techniques and the President's power to transfer captured members of al Qaeda to foreign governments.[223] Obama had revoked the conclusions of some of these memoranda early in his first term when he issued an executive order revoking executive directives issued to the CIA "concerning detention or the interrogation of detained individuals," to the extent that those directives were inconsistent with his mandate that all interrogations be consistent with Common Article 3 of the Geneva Conventions.[224]

Through these tools, the Executive worked hard to delineate the legal boundaries and underpinnings for its military operations, with the goal of advancing both accountability and decisional quality. Although this legal transparency surely did not persuade all critics that the United States' interpretations of the law were the best possible interpretations, the United States' decision to clearly assert its legal positions forced the government to engage in a genuine dialogue with critics, while also clarifying U.S. views inside the executive branch.

2. *The Policy Framework*

The Obama administration similarly clarified the content of U.S. policies in a few important, controversial areas. Perhaps most salient was its decision to publicize U.S. policies and procedures for using force against al Qaeda and associated forces outside areas of active

[221] Id. at i.

[222] Id. at i–iii.

[223] See Selected Opinions of the Office of Legal Counsel, Fed'n of Am. Scientists, https://fas.org/irp/agency/doj/olc/index.html [https://perma.cc/TM8F-HZGK] (last visited Sept. 11, 2018) (listing opinions disclosed by the Obama Administration in 2009).

[224] Exec. Order No. 13,491, 3 C.F.R. 2009 Comp., 199 (2010); see also Memorandum from David J. Barron, Acting Assistant Att'y Gen., to the Att'y Gen. (Apr. 15, 2009), https://fas. org/irp/agency/doj/olc/withdraw-0409.pdf [https://perma.cc/HMK8-5BXK]. (notifying the Attorney General that the Office of Legal Counsel was withdrawing various interrogation memoranda, which no longer represented the views of that office).

hostilities.[225] Known colloquially as the "targeted killing policy," the document described key policy limitations that the administration imposed on itself when employing targeted killings away from battlefields such as Afghanistan.[226] Through these policies, the United States imposed standards on itself that exceeded the requirements of international law. These policies stated, for instance, that the United States would require "near certainty" that the terrorist target is present, "near certainty" that non-combatants will not be injured or killed, and that no other reasonable alternatives exist to effectively address the threat to U.S. persons.[227] The administration presumably adopted these policies because it recognized that the use of targeted killings is controversial internationally (and, to a lesser extent, domestically) and because it wanted to illustrate to the public how seriously it took decisions to target individuals.[228] Similarly, the Obama administration issued an executive order that required the Director of National Intelligence to make public aggregate data about civilian casualties that occurred during targeted killings.[229] In 2016, the Director released a summary of how many non-combatant deaths had occurred in the context of these targeted killings between January 20, 2009, and December 31, 2015.[230]

In 2012, the Department of Defense undertook a different kind of policy transparency in a directive related to weapons autonomy. The directive establishes "guidelines designed to minimize the probability and consequences of failures in autonomous and semi-autonomous

[225] Press Release, The White House, Fact Sheet: U.S. Policy Standards and Procedures for the Use of Force in Counterterrorism Operations Outside the United States and Areas of Active Hostilities (May 23, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism [https://perma.cc /K3CG-WT3Y].

[226] Id.

[227] Id. International law does not prohibit states from conducting strikes that incidentally harm or kill non-combatants, subject to the rule of proportionality. See Henckaerts & Doswald-Beck, supra note 101, at 46.

[228] Quinta Jurecic, Obama's Term-End Thoughts on Targeted Killing, Lawfare (Oct. 17, 2016, 9:42 AM), https://www.lawfareblog.com/obamas-term-end-thoughts-targeted-killing [https://perma.cc/SQA6-N95Y] (describing and critiquing President Obama's perceptions of the moral dilemmas he faced in authorizing targeted killings).

[229] Exec. Order No. 13,732, 3 C.F.R. 2016 Comp., 499 (2017).

[230] Press Release, Office of the Dir. of Nat'l Intelligence, Summary of Information Regarding U.S. Counterterrorism Strikes Outside Areas of Active Hostilities (July 1, 2016), https://www.dni.gov/files/documents/Newsroom/Press%20Releases/DNI+Release+on+CT+Strikes+Outside+Areas+of+Active+Hostilities.PDF [https://perma.cc/2DCF-JU4U].

weapon systems that could lead to unintended engagements."[231] It also sets out the basic policy that autonomous and semi-autonomous weapons systems "shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force."[232] In the context of the debates that were then (and still are) ongoing about whether, when, and how states should be allowed to deploy fully autonomous weapons systems on the battlefield, this directive reflected an effort to lower public anxiety by signaling that the United States intended to keep a "man in the loop" for most military decision-making and to take the lead among states in setting out a public policy on the issue.[233]

C. Transparency for Algorithms

Section IV.B described executive efforts in the years following September 11, 2001, to bring greater transparency to U.S. legal claims, internal procedures, and policy decisions. Many of these efforts were intended to show that there were clear legal parameters underlying U.S. operations, established and replicable processes in place to lead to reasoned decision-making, and accountability (up to the President, in the case of targeted killings) for these decisions. The government pursued "strategic transparency" in both senses of the term (that is, being transparent in strategic ways, and being transparent about strategy, though not about specific, on-the-ground operations). First, it decided that transparency about its legal and policy claims would redound to the government's strategic advantage.[234] Second, it was transparent about its

[231] Dep't of Def., Directive, No. 3000.09, Autonomy in Weapon Systems, at para. 1(b) (Nov. 21, 2012), http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf [https://perma.cc/322X-7LGH].

[232] Id. at para. 4(a).

[233] See, e.g., Michael W. Schmitt & Jeffrey S. Thurnher, "Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict, 4 Harv. Nat'l Sec. J. 231, 241 (2013) (noting that the U.S. Defense Department is "exceptionally sensitive to the human interface issue"); Dustin A. Lewis, Gabriella Blum, & Naz K. Modirzadeh, Research Briefing, War-Algorithm Accountability 26 (2016), https://pilac.law.harvard.edu/war-algorithm-accountability-report/ [https://perma.cc/B9SG-TANG] (noting that the directive is "one of the most technically specific state approaches to autonomy in relation to weapons systems").

[234] President Barack Obama, Remarks by the President on Review of Signals Intelligence, Address to the U.S. Dep't of Justice (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [https://perma.cc/U9DY-U9JP] ("[O]ur global leadership demands that we balance our security requirements against our need to maintain the trust and cooperation among people and

strategies in fighting the conflict with al Qaeda, though it was not transparent about the detailed operational decisions it made while pursuing that strategy. We know, therefore, why the United States thinks it legally may use force inside Somalia against members of al Shabaab, but we do not know ex ante—and should not expect to know—when the military might decide to conduct such operations, in what specific locations, and against which al Shabaab members. Coupling transparency about the legal and policy frameworks with opacity about specific military operations strikes the right balance among the values of reasoned decision-making, government accountability, and operational efficacy.

The United States should adopt a similar approach to its use of predictive algorithms and machine learning tools. The military's instinct often is to hunker down and hide behind classification,[235] judicial deference, the standing doctrine, and the political question doctrine. In the context of predictive algorithms, it should fight those instincts, just as it did in the autonomous weapons context.[236] Pursuing a transparent approach to predictive algorithms would mean explaining to the public why the military has decided to use predictive algorithms and, increasingly, machine learning tools to facilitate its decision-making. It also would entail a public discussion about what the costs and benefits are to using these tools and how the military will attempt to mitigate those costs. Further, it would require the military to explain how it

leaders around the world. For that reason, the new presidential directive that I've issued today will clearly prescribe what we do, and do not do, when it comes to our overseas surveillance."); Robert S. Litt, Gen. Counsel, Office of the Dir. of Nat'l Intelligence, Keynote Remarks at American University Washington College of Law: Freedom of Information Day Celebration (Mar. 18, 2014) ("[P]ublic confidence in the way that we conduct our admittedly secret activities is essential if we are to continue to be able to anticipate and respond to the many threats to our nation.").

[235] See, e.g., David Pozen, Note, The Mosaic Theory, National Security, and the Freedom of Information Act, 115 Yale L.J. 628, 635 (2005) ("Defense and intelligence agencies have been among the most vocal critics of FOIA and have typically had the lowest disclosure rates.") (citations omitted).

[236] A recent update to a U.S. Army and Marine Corps manual indicates a growing understanding within the military that the public closely monitors its fighting in certain contexts. U.S. Dep't of the Army & U.S. Marine Corps, ATP 3-06/MCTP 12-10B, Urban Operations 1–90 (2017) ("Soldiers/Marines are likely to have their [urban warfare] activities recorded in real time and shared instantly both locally and globally. In sum, friendly forces must have an expectation of observation for many of their activities and must employ information operations to deal with this reality effectively. Their challenge is to balance transparency with operations security . . . .").

intends to ensure that its use of predictive algorithms is consistent with—and possibly even helps it improve its compliance with—its international law obligations. Although the military is unlikely to reveal the actual content of its algorithms, this type of transparency will help the military address many of the critiques anticipated in Part III. This is particularly true if the military articulates how it will test the quality of its data, avoid training its algorithms on biased data, and train military users to avoid falling prey to undue automation biases.[237]

There is a wealth of advantages to be gained by some level of transparency surrounding algorithms. One advantage relates to the quality of decision-making. Opening up decisions about the use of algorithms and, possibly, the algorithms' contents can lead to higher quality decisions because a wider range of actors would contribute knowledge and expertise. For instance, the military can produce sounder policy and legal frameworks by bringing in a wider number of stakeholders inside the U.S. government, including the Departments of Justice and State. Allies and private-sector computer scientists will also be better positioned to help the United States improve its use of algorithms. By initiating conversations with its military allies about predictive algorithms, the United States might not only learn from the experiences of peers that are working on these issues but may also have the chance to influence the direction of allies' doctrines.[238] Further, being transparent about actual algorithmic challenges and costs might attract useful input and troubleshooting from computer scientists in academia and the public sector.

Another advantage is that the United States can better shape the direction of the law related to algorithmic use. For instance, the United States might be able to persuade allies to say more publicly about their own approaches, thus evincing more examples of state practice and shaping the nature of the international discussion about these tools. The

[237] See Eshpar, supra note 185, at 18 ("Military officials and security experts have the power to convey the fact that obeying the law and maintaining values are first-rate strategic assets.").

[238] See Heather M. Roff & P.W. Singer, The Next President Will Decide the Fate of Killer Robots—and the Future of War, Wired (Sept. 6, 2016, 7:00 AM), https://www.wired.com/2016/09/next-president-will-decide-fate-killer-robots-future-war/ [https://perma.cc/5BLM-3DSR] (arguing in the autonomous weapons context that the United States should "try to build consensus among its partners and allies about what shared policies in this area ought to be . . . . This is valuable not just for each individual nation and the broader alliance, but also to create a key building block for the bigger global debate.").

U.S. government has pursued this approach in the cyber context. As a former State Department legal adviser put it:

> States should publicly state their views on how existing international law applies to State conduct in cyberspace to the greatest extent possible in international and domestic forums. Specific cyber incidents provide States with opportunities to do this, but it is equally important—and often easier—for States to articulate public views outside of the context of specific cyber operations or incidents. Stating such views publicly will help give rise to more settled expectations of State behavior and thereby contribute to greater predictability and stability in cyberspace.[239]

Translating this approach to the algorithmic context, the United States could, for example, articulate how its use of predictive algorithms interacts with international law requirements, whether by attempting to code international law restrictions into the algorithms or by ensuring that human decision-makers continue to evaluate their acts under detention and targeting laws in a non-algorithmic way. This would both emphasize the U.S. government's commitment to international law compliance and stabilize the expectations of other states.[240]

A third advantage to strategic transparency is that it offers the military the opportunity to diffuse objections and arguments at an early stage. Several audiences are important here: Congress, the courts, U.S. allies, and non-governmental organizations. Strategic transparency would facilitate the military's ability to bring Congress into its corner. The military could learn an important lesson in how *not* to proceed by reviewing the unfavorable treatment that Facebook and Google lawyers received during congressional testimony because of their companies'

[239] Brian J. Egan, Legal Adviser, U.S. Dep't of State, International Law and Stability in Cyberspace, Remarks Before the Berkeley Center for Law and Technology (Nov. 10, 2016), *in* 35 Berkeley J. Int'l L. 169, 172 (2017).

[240] See Stephen Smith, Austl. Minister of Def., Address to the Third Plenary Session of the Twelfth International Institute for Strategic Studies' Shangri-La Dialogue on Military Modernization and Strategic Transparency (June 1, 2013), https://web.archive.org/web/20130803023049/http://www.minister.defence.gov.au:80/2013/06/01/minister-for-defence-speech-military-modernisation-and-strategic-transparency-singapore/ [https://perma.cc/BW38-BQQW] (discussing how a military's transparency about its strategic intentions, defense policy, capabilities, and modernization can build confidence and reduce insecurity between states).

opaque use of algorithms.[241] Being forthcoming with Congress about the tools on the table and the military advantages that attach to the use of predictive algorithms—including in the detention and targeting context—will avoid that kind of backlash. The courts are another important audience. When the Executive is clear about which underlying laws and procedures govern specific activities, and where those procedures are regularized, the Executive tends to receive more deference from the courts.[242] Setting forth a clear legal basis and standards for the use of predictive algorithms may also help inoculate the government against future litigation, or will at least flesh out the most salient legal critiques at early stages of the government's development of predictive algorithms. Additionally, a more open approach to discussing the use of these technologies with non-governmental organizations might mitigate some of their most intense critiques and foreclose their efforts to use litigation to change the military's practices, particularly if they believe the military has taken some of their concerns into account.

All this is not to argue that the military will be able to be completely transparent about the content of its algorithms. As in other areas of national security, there are legitimate concerns that full disclosure of the workings of an algorithm will disclose too much information to actors who seek to harm us. Some aspects of the "algorithmic black box" will remain. Thus, observers may not be able to directly review whether the military has in fact avoided training its algorithms on biased data, or has used sufficient high-quality data for such training. Only the military itself (and perhaps members of the National Security Council) will be

[241] See, e.g., Hamza Shaban, Craig Timberg & Elizabeth Dwoskin, Facebook, Google and Twitter Testified on Capitol Hill. Here's What They Said, Wash. Post (Oct. 31, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/31/facebook-google-and-twitter-are-set-to-testify-on-capitol-hill-heres-what-to-expect/ [https://perma.cc/5783-2GME] (describing aggressive questioning by Senators about companies' lack of transparency about their business models and the manipulation they experienced during the 2016 election).

[242] See Derek Jinks & Neal Kumar Katyal, Disregarding Foreign Relations Law, 116 Yale L.J. 1230, 1247–49 (2007) (arguing that courts should only give the executive deference where the executive has engaged in a deliberative process that produces reasoned analysis); Dawn Johnsen, Judicial Deference to President Trump, Take Care (May 8, 2017), https://takecareblog.com/blog/judicial-deference-to-president-trump [https://perma.cc/QQN2-MCK4] ("[J]udicial deference generally embodies assumptions that the president's actions reflect regular processes behind-the-scenes, that the decisions are informed by expertise and judgment and are made in good faith.").

able to judge those decisions. Nevertheless, publicly articulating the standards and processes to which the military will hold itself can play a significant role in prompting care inside the executive branch about the use of these types of algorithms.

CONCLUSION

The use of predictive algorithms by the military in wartime poses greater challenges than the criminal justice system's use of predictive algorithms, though the challenges of wartime algorithms may be less likely to come into public view. By virtue of the secrecy of many military operations and a historical resistance to exposing the inner workings of military decision-making to the public, it is possible—if the normal way of doing business prevails—that few specific uses of predictive algorithms (and problems that arise therefrom) may come to light. On the other hand, because of the black box nature of many military operations, some members of the U.S. public, foreign governments, and non-governmental organizations are likely to be suspicious and critical of any uses of algorithms that become known. Instead of relying on that operational black box, the military should seek to be as forthcoming as possible about its development, testing, and use of predictive algorithms, especially ones that employ machine learning to make recommendations about detention and targeting. In short, it should commit itself to strategic transparency. Being open about the goals of these algorithms, their benefits, their shortcomings, and their consistency with international law requirements will play a critical role in addressing and mitigating whatever discomfort may exist with military predictive algorithms.