REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05/08/2019	Master's of Military Studies	SEP 2018 - APR 2019

4. TITLE AND SUBTITLE
Prediction for Protection: The Influence of Predictive Policing on Future Force Protection

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Joers, Christopher R., Major, USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
Dr. Craig Hayden

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
A collection of individual, time, and location-based predictive analytic methods, currently used by police departments throughout the country, offer military commanders improved situational awareness, flexibility, and resource management to conduct security and force protection operations in future expeditionary environments. Having the ability to predict who is most likely to attack at a certain time and location will likely be key to deterring and, if necessary, winning future wars.

15. SUBJECT TERMS
Big Data; Predictive Analytics; Predictive Policing; Anti-Access and Area Denial (A2/AD); Expeditionary Advanced Basing Operations (EABO); Force Protection

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	36	(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Prediction for Protection: The Influence of Predictive Policing on Future Force Protection

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Major Christopher R. Joers

AY 2018-19

Mentor and Oral Defense Committee Member: Dr. Craig Hayden
Approved: _____
Date: 24 April 2019

Oral Defense Committee Member: Mr. JD Work
Approved: _____
Date: 24 April 2019

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Acknowledgements

Thank you to the faculty and staff of Marine Corps University for their continued support and encouragement through this project. To my mentor, Dr. Craig Hayden, and Mr. JD Work, I sincerely appreciate your help, perspectives, and patient guidance.

To my wonderful family, thank you for allowing me time away to research and write this paper. Kiddos, there were often nights and weekends where I could not spend the time with you that I wanted. I look forward to the many bike rides, burgers and fries, and opportunities to go "out and about" that we will enjoy together. Daddy's coming home!

Finally, to my beautiful, loving, and supportive wife: I could not have done this without you. You encouraged me when I was frustrated, motivated me when I needed it, and pressed me to do my best. Most importantly, you are an incredible mom that cared for our children and turned our house into a home. I love you!

Executive Summary

Title: Prediction for Protection: The Influence of Predictive Policing on Future Force Protection

Author: Major Christopher R. Joers, United States Air Force

Thesis: A collection of individual, time, and location-based predictive analytic methods, currently used by police departments throughout the country, offer military commanders improved situational awareness, flexibility, and resource management to conduct security and force protection operations in future expeditionary environments.

Discussion: Police departments across the country are embracing new data-based technologies to make their policing efforts more affordable, efficient, and productive. New information processing capabilities can synthesize more data quicker than ever. As a result, this technology can arm police officers with detailed predictions regarding the timing and location of criminal activity, and it potentially allows them to identify the suspects and victims of that criminal activity. In response, they can tailor their crime-fighting strategies to maximize resources, such as personnel, equipment, and time, while minimizing waste. With the United States returning to a period of great power competition, maintaining freedom of action in a battlespace contested with advanced anti-access and area-denial platforms means the joint force must employ a strategy that ensures maximum dispersion and resiliency without compromising capability and capacity to project power. Having the ability to predict who is most likely to attack at a certain time and location will likely be key to deterring and, if necessary, winning future wars. To that end, this paper seeks to determine to what degree the concepts of big data and predictive policing can contribute to the security of future expeditionary military bases and the protection of expeditionary military forces.

Conclusion: A data and predictive analytics-based approach to security and force protection operations in an expeditionary environment will provide military commanders the situational awareness and flexibility necessary to make decisions more quickly and with better confidence.

Introduction

The first line of the 2018 National Defense Strategy states, "The Department of Defense's (DoD) enduring mission is to provide combat-credible military forces needed to deter war and *protect* the security of our nation."[1] This is not a complex statement, but it is a very powerful one. Protecting the security of the nation is a sacred responsibility placed in the hands of the military, but there are other men and women who also have a mission to protect: police officers. Each police department has its own mission statement, but the Chicago Police Department's mission summarizes them well. It states the department is "committed to *protect* the lives, property, and rights of all people, to maintain order, and to enforce the law impartially."[2] Though the scale of their missions is significantly different, both the military and civilian police departments have a common underlying principle: to safeguard populations. The military accomplishes this by projecting its power globally, relying heavily on expeditionary bases around the world. Police officers operate locally and develop deep connections, for better or for worse, within their communities. Interestingly, it may be a method of policing that helps protect the military's future expeditionary bases.

Police departments across the country are embracing new data-based technologies to make their policing efforts more affordable, efficient, and productive. New information processing capabilities can synthesize more data quicker than ever. As a result, this technology can arm police officers with detailed predictions regarding the timing and location of criminal activity, and it potentially allows them to identify the suspects and victims of that criminal activity. In response, they can tailor their crime-fighting strategies to maximize resources, such

[1] US Department of Defense, *National Defense Strategy of the United States of America*, (Washington, DC, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, 1.
[2] City of Chicago, "Police – Mission," accessed February 20, 2019, https://www.chicago.gov/city/en/depts/cpd/auto_generated/cpd_mission.html.

as personnel, equipment, and time, while minimizing waste. The military could benefit greatly from this technology, especially when the United States is facing "an ever more lethal and disruptive battlefield, combined across domains, and conducted at increasing speed and reach."[3] Understanding how to posture security and force protection assets in an expeditionary environment will be a key tenet of future conflict. To that end, this paper seeks to determine to what degree the concepts of big data and predictive policing can contribute to the security of future expeditionary military bases and the protection of expeditionary military forces. It is a collection of individual, time, and location-based predictive methods that offer military commanders improved situational awareness, flexibility, and resource management to conduct security and force protection operations.

Predictive Analytics and Big Data

It is first necessary to gain an understanding of the relationship between data and prediction. The term "predictive analytics" is the most appropriate to describe how one can predict future behavior based on data and subsequently spur more effective decisions.[4] It is impossible to predict with 100 percent certainty how an individual will behave. Instead, predictive analytics offers a way to use data to measure probabilities.[5] How likely is a shopper to purchase a specific item based on his internet browsing history, will that teenage driver have an automobile accident, or when and where is the city's next violent crime most expected to occur? The central component to an accurate prediction is the collection and analysis of past data, but this also creates a constraint on any conclusions. The resultant predictions cannot see beyond,

[3] US Department of Defense, *National Defense Strategy*, 3.
[4] Eric Siegel, *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die* (Hoboken, NJ: John Wiley & Sons, 2013), 11.
[5] Andre Andrejevic, *Infoglut: How Too Much Information is Changing the Way We Think and Know* (New York: Routledge, 2013), 23.

and are only as accurate as, the data input into the model.[6] Therefore, quality information and data integrity are of the utmost importance in predictive analytics.

One of the approaches to overcome the potential lapse of integrity is simply to gather vast quantities of data. As the amount of collected information increases, it reduces the influence of erroneous or biased data and results in a more accurate prediction of future events. Data fusion, the "multilevel, multifaceted process dealing with automatic detection, association, correlation, estimation, and combination of data and information from single and multiple sources," is the science behind predictive analytics.[7] Diversity of information results in the identification of more meaningful patterns and trends because the data represents a much larger sample size. Further, accumulating data across broad categories, regardless of its pertinence to a specific area of interest at the time, means it is available for future not-yet-known purposes.[8] A primary benefit of data fusion is the availability of raw and unfiltered data, but there are difficult challenges to ensuring consistent collection, categorization, and interpretation of the data in its various formats.[9] Even worse, though advances in technology have made the collection and analysis of data much easier, they have also resulted in a world that creates more data than ever.

Today, data is much more than a spreadsheet saved on a laptop computer. That computer connects to the internet where one can instantly view pictures from family, friends, and celebrities around the world on various social media websites. It is likely someone used a smart phone to take the picture, which includes a digital stamp indicating the exact date, time, and location when taken. While taking the picture, the photographer was also listening to a

---

[6] Michael Chi, "Big Data in National Security," *Australian Strategic Policy Institute*, August 2017, https://www.jstor.org/stable/resrep04118, 2.
[7] Lawrence A. Klein, *Sensor and Data Fusion: A Tool for Information Assessment and Decision Making* (Bellingham, WA, SPIE Press, 2004), 2.
[8] Andre Andrejevic, *Infoglut*, 36-37.
[9] Benjamin C. Dean, "Big Data: The Latest Tool in Fighting Crime" in "BIG DATA: A Twenty-First Century Arms Race," (Washington DC: Atlantic Council, 2017), www.jstor.org/stable/resrep03719, 34.

customized music playlist by a service that predicts what new songs to add based on the user's preferences. The individual purchased the phone after receiving an unprompted e-mail stating an item he recently viewed at an online retailer was now in stock and on sale.

The amount of data generated by technology connected to the internet is staggering and, when aggregated, can provide telling insight into what motivates one's behaviors and actions. Research shows the number of items connected to the internet in 2020 will grow to almost 200 billion, enough for twenty-six smart devices per person worldwide.[10] The connected world makes life easier and more convenient, but at the same time it poses a risk to personal privacy, how one associates with others, and one's ability to make independent decisions.[11] To some, these issues are just minor nuisances, an accepted cost of living in a technological society. Yet others view them as undermining the most basic principles of a democratic society. After appreciating how predictive analytics and big data work, it is essential to apply these concepts to the field of law enforcement in order to understand the advantages and challenges of data-driven and predictive policing.

Predictive Policing

If the world is becoming increasingly connected to the internet, it makes sense that law enforcement agencies would look to use the generated data to gain insights into criminal behavior. Detectives today still rely on classic techniques such as interviews, searches, and collecting evidence, but they are employing them in new ways in the digital domain. The forensic search of a suspect's phone can reveal important details about the suspect's actions and intent by reviewing photographs, internet search history, and content of text messages. Data is

[10] Intel, "A Guide to the Internet of Things," accessed January 14, 2019, https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.
[11] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: New York University Press, 2017), 12.

central to solving today's crime, but it also has great potential to prevent it. Police departments across the United States are finding significant benefit in analyzing past data to predict future crime and then acting to prevent it.

Predictive policing broadly concentrates on three different target categories to predict criminal activity: the offender and/or victim, the times, and the locations with a raised probability of experiencing crime. Each of these methods, described in more detail below, use different types of data in slightly unique ways to predict potential crime. A RAND study found strong parallels between classic methods of crime analysis and those of predictive analytics; the only differences involved scalability and sophistication of analytical systems.[12] Technology allows predictive analytics to utilize larger sets of data and produces results much faster, but the practices are based on the same traditional techniques.

Individual-based predictive targeting seeks to forecast who will commit and/or who will be a victim of a crime. It is the product of two analytical practices. The first maps the social network of those individuals identified as having the highest probability of involvement in violent crime, and the second uses an algorithm to further identify those with an even greater risk.[13] Police then develop a targeting list, comprising the highest risk individuals, on which they focus intervention and policing efforts to reduce crime.[14] The interventions could include voluntary interviews to learn more about the at-risk individuals, classes aimed at enlightening them about the potential consequences of their actions and associations, or providing information on local resources and support. However, just because the targeting method places individuals

[12] Walter L. Perry, et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Safety and Justice Program (Washington DC, RAND Corporation, 2013), 9, https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.
[13] Ferguson, *The Rise of Big Data Policing*, 44.
[14] Ibid., 45.

on the high-risk list does not mean the police have probable cause to make an arrest. The list only provides awareness and then allows police departments to prioritize their efforts.

Those involved in law enforcement must recognize the great opportunities offered by and the potential pitfalls inherent in individual-focused predictions. As alluded to above, knowledge of those who are most likely to commit a crime allows police officers to be proactive instead of reactive in attempting to reduce crime. A George Mason University study found that a focused strategy "that emphasizes deterring specific high-risk gang members" has proven successful at reducing crime, and purposeful allocation of law enforcement resources is more effective than random patrols.[15] However, the allure of these benefits also opens the door for potential misuse and abuse of the data.

The high-risk list includes data originating from myriad sources, to include "eyewitness" accounts, anonymous tips, misdemeanor offenses, crime scene investigations, traffic infractions, and police officer interactions on the street. The reality is an individual's personal biases or motives can greatly influence this information. It is imperative police departments have a quality control process to authenticate, categorize, and determine credibility of information in order to create an accurate database from which to make predictions.[16] The quality of the data analysis outputs is only as good as the data gathered. Several police departments have developed policies on how to handle data derived from analysis of social networks. For clarification, in this instance the term social network refers to the interactions between two people, not social media sites such as Facebook or Twitter. These policies seek to ensure law enforcement agencies are applying appropriate protections to uphold the due process rights of those who are on the high-

[15] Cody W. Telep, "Police Interventions to Reduce Violent Crime: A Review of Rigorous Research," Fairfax, VA: Center for Evidence-Based Crime Policy, George Mason University, http://cebcp.org/wp-content/onepagers/InterventionsToReduceCrimeReview_Telep.pdf.
[16] Ferguson, *The Rise of Big Data Policing*, 59.

risk list and the privacy of those who are not.[17] Despite the policies, many argue data-driven, individual-based predictions unfairly target minorities and subsequently reinforce existing biases and prejudicial tendencies.

In August 2016, the American Civil Liberties Union and sixteen civil rights privacy, racial justice and technology organizations issued a statement that predictive policing contains an inherent bias against minorities, lacks transparency, and ignores the needs of the community.[18] More specifically, they noted the data driving predictions primarily comes from police responses to reported crime instead of a more inclusive record of all crimes that occur.[19] It is impossible for law enforcement agencies to have knowledge of all criminal activity; therefore, it is useful to recognize how the gathered data may be inadvertently deficient and create hazardous implications. If individuals of a certain race have a higher arrest rate, it is possible police officers will respond differently to a discretionary situation based on a person's skin color instead of his or her actual actions.[20] Predictive targeting, especially when focused on individuals, can easily devolve into a method justifying existing biases.

A second prediction method focuses on *when* a crime is likely to occur. Several data points contribute to analysis in the time domain, including time of day; weather; proximity to events such as pay days, holidays, and verdict announcements; and time between similar types of criminal offenses.[21] It works similarly to the individual-based method by reviewing and

---

[17] Jennifer Bachner, "Predictive Policing: Preventing Crime with Data and Analytics," IBM Center for the Business of Government, Improving Performance Series, John Hopkins University, 2013, http://www.businessofgovernment.org/report/predictive-policing-preventing-crime-data-and-analytics, 24.
[18] American Civil Liberties Union, "Predictive Policing Today: A Shared Statement of Civil Rights Concerns," August 31, 2016, https://www.aclu.org/other/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice.
[19] Ibid.
[20] Andrew Guthrie Ferguson, "Big Data and Predictive Reasonable Suspicion," *University of Pennsylvania Law Review* 163, no. 2 (January 2015): 402, https://www.jstor.org/stable/24247848.
[21] Perry, et al., *Predictive Policing*, 45.

categorizing past criminal activity according to time-based factors to determine if there are trends across multiple variables that can predict when a future crime might occur. A common practice to convert the data into a useful product is the creation of heat maps. Heat maps visually present the data using color intensity to show the relative frequency of criminal activity based on specified criteria such as the time, date, weather, etc.[22] Data that is further from average and more extreme is a darker shade, allowing analysts to easily notice trends that they might otherwise lose in the data.

The trends are more difficult to discern with the addition of multiple variables. A study on commercial breaking and entering crimes in Canada highlights the multi-dimensional nature of time-based factors. It found criminals were more likely to burglarize commercial stores around Christmas holidays when inventory was high, but days with decreased temperatures and increased snowfall served as a deterrent to would-be thieves and burglary rates were lower.[23] While not an extraordinary finding, it helps illustrate how predictive analytics can bring clarity to the complex, and many times dangerous, situations police officers face every day. Knowing when a certain type of crime is likely to occur allows police departments to tailor their support and resources appropriately.

Another aspect of time-based predictions is the use of real-time surveillance. Instead of policing a city with a series of street patrols, technology now allows cameras and drones to provide persistent "eyes and ears" wherever needed. The New York Police Department's (NYPD) Domain Awareness System (DAS) sends the video feeds of 9,000 surveillance cameras throughout lower Manhattan to an automated alert system that identifies suspicious behavior,

[22] Perry, et al., Predictive Policing, 46.
[23] Shannon J. Linning, Martin A. Andersen, and Paul J. Brantingham, "Crime Seasonality: Examining the Temporal Fluctuations of Property Crime in Cities with Varying Climates," *International Journal of Offender Therapy and Comparative Criminology* 61, no. 16 (March 2016): 21-22, https://doi.org/10.1177/0306624X16632259.

identifies and tracks vehicles by license plates, and cross-references this information against criminal and intelligence databases looking for potential hits.[24] At the same time, DAS tracks the real-time location of more than 5,000 NYPD vehicles and shares 911 data, past history of call locations, and other pertinent data via department-issued smartphones and tablets to ensure officers have situational awareness.[25] The connectedness between police officers and data hopefully makes for safer and more informed interactions. Reviewing past recordings can reveal, for example, criminals' patterns of life, times with the most foot traffic in a specified area, and days of the week requiring less law enforcement support. Real-time surveillance can generate quicker and more effective police responses, but the ability to capture persistent video footage and exploit it for preventative purposes is the real boon to predictive policing.

Just as the individual-based targeting method raised potential concerns, the time-based method has similar privacy and oversight challenges. One of the biggest anxieties over real-time surveillance is that in order to collect data on a particular individual, the surveillance will also collect on everyone else.[26] The prospect of being under constant surveillance is likely to affect an individual's sense of freedom. As an example of this, surveillance "may inhibit individuals' freedom of assembly or freedom of expression" over concerns of attribution with social movements, protests, or demonstrations.[27] Additionally, citizens want to know that police are not abusing the troves of data and video footage collected for predictive purposes. Transparency and oversight are two related issues law enforcement agencies can struggle to balance as they attempt to keep the public informed while maintaining confidentiality regarding their policing

[24] Ferguson, *The Rise of Big Data Policing*, 86.
[25] The City of New York Police Department, "Technology – NYPD," accessed January 20, 2019, https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/technology.page.
[26] Ferguson, *The Rise of Big Data Policing*, 98.
[27] Rachel L. Finn and David Wright, "Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications," *Computer Law & Security Review* 28 (2012): 186, https://www.dhi.ac.uk/san/waysofbeing/data/data-crone-finn-2012.pdf.

efforts. Transparency and oversight, which serve as trust-building mechanisms, assure the public that they are aware of and can openly rebuke any misconduct while also holding officials accountable at future elections.[28] Involving the public in the implementation of predictive policing, regularly updating them on data collection and protection methods, and describing the safeguards in place to ensure their privacy rights are crucial to a successful program.

The third predictive targeting method is location-based and, arguably, presents the greatest potential to assist law enforcement in predicting and deterring crime. Predicting the location of future crime is a classic analytical approach that big data has amplified and made more scientific than ever. Renown criminologist, Dr. David Weisburd, used statistical data to suggest that there is a law of crime concentration, which states, "for a defined measure of crime at a specific microgeographic unit, the concentration of crime will fall within a narrow bandwidth of percentages for a defined cumulative proportion or crime."[29] Weisburd's data showed that across seven U.S. cities and one Israeli city, 25% of the criminal activity occurred between just 0.4 and 1.6% of the city's street segments and 50% occurred between 2.1 and 6%.[30] These striking numbers demonstrate that criminal activity is highly concentrated, and therefore likely predictable, even down to the street-level.

The concentrated nature of specific types of crime makes location-based targeting especially attractive for predictive models. Among the most traditional and basic methods is the kernel density estimation (KDE). It plots historical criminal activity on a map and uses a mathematical function to produce a three-dimensional contour showing the density of activity in

[28] H. Akin Ünver, *Politics of Digital Surveillance, National Security and Privacy*, Cyber Governance and Digital Deomcracy, (Istanbul, Turkey: Centre for Economics and Foreign Policy Studies, April 2018), 15, https://www.jstor.org/stable/resrep17009.
[29] David Weisburd, "The Law of Crime Concentration and the Criminology of Place," *Criminology* 53, no. 2 (2015): 138, https://doi.org/10.1111/1745-9125.12070.
[30] Ibid., 143.

a particular location.[31] A larger contour represents an area with more activity, and police can deploy resources appropriately to deter additional crime. Another popular approach is risk terrain modeling (RTM). This model assigns a value for all factors that may contribute to the risk of criminal activity, such as nearby bars, public transportation hubs, or police stations, and produces a map identifying the composite risk values of locations likely to experience criminal activity in a specific geographic area of interest.[32] Notably, this is not simply a map highlighting the locations of previously reported criminal activity; it depicts the areas that have the highest concentration of factors that make criminal activity likely.[33] Finally, the street network-based method is a proposed model, based on Weisburd's law of crime concentration, that seeks to replace grid square criminal analysis with a networked street-level methodology. Understanding where crime is occurring at the street level can make police patrols much more efficient and effective in a deterrence role. An added benefit is the ability to supplement the location-based data with timestamps, allowing one to receive daily predictions on what street block a crime is most likely to occur *and* when.[34]

Location-based predictions are not perfect, and they have limitations that law enforcement agencies must be careful to not ignore. First, standardizing how an officer categorizes the type and location of crime is critical, especially for models that attempt to predict down to the street level. Any data-driven metric poses a risk of exaggeration to make results look better, but inaccurate data can negatively affect the predictive reliability of the models.[35]

---

[31] Ned Levine, "Crime Mapping and the *CrimeStat* Program," *Geographical Analysis* 38, no. 1 (January 2006): 47, https://doi.org/10.1111/j.0016-7363.2005.00673.x.
[32] Joel M. Caplan, Leslie W. Kennedy, and Joel Miller, "Risk Terrain Modeling: Brokering Criminological Theory and GIS Methods for Crime Forecasting," *Justice Quarterly* 28, no. 2 (April 2011): 365, https://doi.org/10.1080/07418825.2010.486037.
[33] Ibid., 365.
[34] Gabriel Rosser, et al., "Predictive Crime Mapping: Arbitrary Grids or Street Networks," *Journal of Quantitative Criminology* 33, no. 3 (2017): 589, https://doi.org/10.1007/s10940-016-9321-x.
[35] Ferguson, *The Rise of Big Data Policing*, 73.

An unintentional example is when a police officer witnesses criminal activity on one block, but the suspect runs until he is stopped on a nearby block and an illegal concealed weapon is discovered; what is the crime, where did it occur, and how should the officer document it?[36] A second limitation is that location-based predictions methods do not work equally across all types of crime. For example, research shows that street crimes are a better predictor of future street crimes because there is a stability and consistency to the location where they occur when compared to other types of crime such as violence-based crimes, breaking and entering, and vehicle crimes.[37] Finally, there are concerns about biases against neighborhoods with high minority and poor populations, similar to those discussed in the individual-based predictions section. Unfortunately, deep-seated connections between race, residential segregation, and community conditions play an inextricable role in the location of violent crime.[38] Police departments have a responsibility to ensure personal and institutional biases do not create unwarranted consequences for specific locations and populations.

Force Protection in the Expeditionary Environment

Law enforcement agencies around the world have implemented policing strategies incorporating big data and predictive analytics to prevent crime, but these concepts have potential beyond policing. The United States military is returning to a period of great power competition, influenced by new technologies such as big data, artificial intelligence, and autonomy that will change the character of war.[39] Dr. Colleen McCue states, "If knowledge is

[36] Ferguson, The Rise of Big Data Policing, 73.
[37] Spencer Chainey, Lisa Thompson, and Sebastian Uhlig, "The Utility of Hotspot Mapping for Predicting Spatial Patterns of Crime," *Security Journal* 21, no. 1-2 (Feb 2008): 23-25, https://doi.org/10.1057/palgrave.sj.8350066
[38] Ruth D. Peterson and Lauren J. Krivo, "Race, Residence, and Violent Crime: A Structure of Inequality," *Kansas Law Review* 57, no. 4 (April 2009): 928-929, https://kuscholarworks.ku.edu/bitstream/handle/1808/20100/7.0-Peterson_Final.pdf?sequence=1&isAllowed=y.
[39] US Department of Defense, *National Defense Strategy*, 3.

power, then foreknowledge can be seen as battlespace dominance or supremacy."[40] Harnessing the ability to predict who is most likely to attack at a certain time and location is critical to deterring and, if necessary, winning future wars. Military commanders rely on information and data more than ever to inform decisions that have life or death consequences. Fighting an adversary with comparable, or in some cases better, technological capabilities means the US will rely on quick, well-informed decisions to overcome the challenges posed in future conflict.

The Secretary of Defense, Chairman of the Joint Chiefs of Staff, and the Service Chiefs have spent significant effort to develop a joint understanding of what challenges the US military will face in future conflicts. Among the most daunting is maintaining the ability to project power in a contested anti-access and area denial (A2/AD) environment. A 2017 *Joint Force Quarterly* article explains that the Joint Concept for Access and Maneuver in the Global Commons (JAM-GC), signed in October 2016, is a classified document that addresses how the US military "must be able to maintain access to and maneuver through portions of the global commons, project power, and defeat an adversary attempting to deny freedom of action via the employment of A2/AD capabilities."[41] The services are advancing the concept with their own versions specifying how they will address the challenges unique to their portfolios. The Air Force has the Adaptive Basing concept, the Marine Corps has the Expeditionary Advanced Basing Operations (EABO) concept, and the Navy has joined the Marine Corps in authoring the Littoral Operations in Contested Environments (LOCE) concept.[42] These concepts contain

[40] Colleen McCue, "Data Mining and Predictive Analytics: Battlespace Awareness for the War on Terrorism," *Defense Intelligence Journal* 13, no.1/2 (2005): 48.
[41] Michael E. Hutchens, et al., "Joint Concept for Access and Maneuver in the Global Commons," *Joint Force Quarterly* 84, no. 1 (January 2017): 137, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-84/jfq-84.pdf.
[42] William Dries, "Some New, Some Old, All Necessary: The Multi-Domain Imperative," *War on the Rocks*, March 27, 2017, https://warontherocks.com/2017/03/some-new-some-old-all-necessary-the-multi-domain-imperative.

expectations of what future conflict will look like and how the US military will array its forces in a contested environment.

An expeditionary military base in the future will not look like the well-established bases that one commonly recognizes today in Qatar or Afghanistan. Two of the most important features required of the future joint force are being distributable, "the ability to disperse, reposition, and use a variety of bases and operating locations, while retaining the ability to maneuver and concentrate combat power," and resilient, "the ability to recover rapidly from adversity and setbacks."[43] At first read, these two features might seem at odds with one another; however, resiliency can be more than a single, well-defended base. EABO seeks to eliminate the effect of adversary A2/AD targeting by fluidly operating between dispersed temporary bases, which require less infrastructure and present a reduced footprint.[44] This makes them harder to detect, but if they are, it also means quickly disassembling or abandoning them is an acceptable course of action. Second, the concept provides resiliency "by avoiding easily targeted deep water ports, long runways and large capital ships."[45] Distributing forces across multiple bases makes it much harder for the adversary to impose overwhelming costs on the joint force, and instead increases its own cost of achieving success. Instead of massing its combat power against a single base or ship, the adversary must determine how much capability it has to attack multiple assets simultaneously. Examining how the military currently defends its bases and protects its personnel and equipment will help to conceptualize the role big data and predictive analytics can play in protecting an expeditionary force engaged in conflict against a near-peer competitor.

[43] Hutchens, et al., "Joint Concept for Access and Maneuver," 137.
[44] Marine Corps Warfighting Laboratory, *Industry Panel Discussion* (Naval S&T Expo, April 20, 2017), PowerPoint presentation, Slide 8, https://www.mcwl.marines.mil/portals/34/ST_ExpoBRIEF_ApprovedPublicRelease.pdf.
[45] Ibid.

Doctrine provides the basis for how military forces plan, execute, and assess the force protection mission in an expeditionary environment. Joint Publication (JP) 3-0, Joint Operations, defines force protection as "preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information."[46] Of note, force protection is inherently defensive; offensive activities would generally fall outside of its scope. Intelligence is an essential component of force protection, particularly in the hope of deterring or preventing an attack, because it provides the details about an adversary's capability, intent, and disposition, which then allows a commander to establish appropriate security measures.[47] JP 3-10, Joint Security Operations in Theater, lists the fundamental actions required to ensure security in an expeditionary environment and describes the necessity of intelligence in understanding the adversary and the operational environment.[48] At the next level, intelligence helps commanders comprehend the relationship between the adversary and its environment, which then reveals the challenges to mitigate and opportunities to exploit the threat. Additionally, the host nation's intelligence organizations can add an indigenous context and cultural perspective to intelligence products and data.[49] Having local knowledge is valuable because force protection is a multi-dimensional mission that may require different actions based on the adversary threat, friendly capability, and risk acceptance in a particular location.

[46] US Department of Defense, *Joint Operations*, JP 3-0 (Washington, DC: US Department of Defense, January 17, 2017 Incorporating Change 1, October 22, 2018), III-41.
[47] Ibid., III-41.
[48] US Department of Defense, *Joint Security Operations in Theater*, JP 3-10 (Washington, DC: US Department of Defense, November 13, 2014), III-2.
[49] US Department of Defense, *Joint Security Operations in Theater*, JP 3-10 (Washington, DC: US Department of Defense, November 13, 2014), III-23.

Big Data and Predictive Analytics Applied to Force Protection

The application of predictive policing does not translate directly into strategies the military could use for force protection, antiterrorism, or counterterrorism purposes. However, the concepts behind predictive policing, namely big data and predictive analytics, offer great potential. At present, these concepts have not significantly entered the expeditionary environment in a meaningful way.[50] Perhaps the most advanced program looking to leverage the benefits of this technology is a Defense Innovation Unit Experimental (DIUx)-sponsored project that has developed "algorithms to transition from time-based maintenance to advanced predictive maintenance" for military equipment.[51] The project will track the real-time performance of components in the Army's M2 Bradley infantry fighting vehicle and, through big data and analytics, predict when each part is most likely to fail.[52] With such technology, logistics units can ensure they have the right spare parts at the right time, thereby avoiding potentially deadly maintenance failures, costly shipping, and vehicle down time that will not be compatible with the speed of future conflict.

Exploring how the military might use big data and predictive analytics for force protection purposes through the same individual, time, and location-based methods is a convenient way to structure the comparison and determine if any meaningful similarities or differences exist. Instead of attempting to predict the probability of the next crime, the military would use the concepts to predict the next hostile incident against military forces. In a near-peer contested environment, this hostile incident could take the form of a conventional military threat,

---

[50] Kelley M. Sayler, *Artificial Intelligence and National Security*, CRS Report for Congress R45178 (Washington DC: Congressional Research Service, January 30, 2019), 32, https://fas.org/sgp/crs/natsec/R45178.pdf.
[51] Defense Innovation Unit Experimental (DIUx), *DIUx Annual Report 2017*, (Silicon Valley, CA, DIUx, 2017), https://diux.mil/download/datasets/1774/DIUx%20Annual%20Report%202017.pdf.
[52] Sydney J. Freedburg Jr., "AI Logistics Let Combat Units Move Faster: Uptake's DIUX Contract," *Breaking Defense*, June 27, 2018, https://breakingdefense.com/2018/06/ai-logistics-can-speed-up-army-tanks-uptakes-diux-contract.

a short-range missile launch, large-scale terrorism, or even a lone-wolf attack. Advanced knowledge of this type of information could not only protect friendly forces, but it could also serve as a psychological deterrent by discouraging potential adversaries from attacking. Examining the relevancy of the individual, time, and location-based prediction methods to the expeditionary environment will help determine their feasibility and practicality.

Applying the individual-based prediction method to a militarized expeditionary environment requires a slightly different perspective to turn the theory into worthwhile practice. The manner in which an agency handles a list of individuals identified as "high-risk" for future violent crime will vary greatly between law enforcement and the military. A police officer may be able to knock on the doors of at-risk individuals to explain the dangers of their behavior and associations, but the military does not have the same option. A knock on the door by the military is almost certainly to follow with a detention or lethal force. This does not reduce the utility of developing a high-risk list, but it is necessary to recognize the different purposes. Until the military receives confirmation of an individual as responsible for or preparing to engage in hostile activity against US forces, big data and predicative analytics will continue to build an intelligence picture.

In the future expeditionary environment, individual-based predictions can have a direct impact on the warfighter's effectiveness. One example is examining the social networks of a local population. This could involve the use of signals intelligence to determine if a particular individual has connections to a known hostile actor via a cellular telephone network or an examination of financial transactions to determine where and how money transfers are taking

place.[53] Even if predictive analytics is unable to produce a single individual's name, it can expose connections pertinent to a group's size and structure, its purpose, or its leadership element that would otherwise remain hidden underneath volumes of data.[54] The speed of this analysis will also pay great dividends in the expeditionary environment because of the dynamic nature of future basing. Commanders rely on intelligence to drive their force protection decisions, and in an already contested environment, they cannot afford to wait or make mistakes on where to send military forces. Predictions aimed at detecting and knowing the adversary will feed decisions such as whether or not to remain in place, how many and what type of weapons to carry, and how much risk a commander is willing to take. Ultimately, the side that is able to make decisions faster than its adversary is likely to emerge victorious in the future.

Time is of the essence in a near-peer conflict; thus, time-based prediction methods will be central to military success in the future. Fortunately, there is congruency between the law enforcement and military applications of these methods. With the help of big data, analysts can easily convert historical data reflecting the times when hostile incidents have occurred into maps depicting when future incidents are likely to occur. As a result, a commander could choose to prevent forces from driving off-base at particular times or might send patrols out to interdict potentially hostile behavior. For example, knowing that the cover of darkness makes it easier to conceal one's actions, a heat map could identify high-risk windows of time when attacks are most likely. Instead of paralyzing the movement of an entire base, the prediction windows allow a commander to visualize the risk and determine the best ways to counter or mitigate the threat. Unfortunately, there are also examples where data and time-based predictions can go badly. In

[53] Mark Jacobsohn and Scott Jachimski, *Predictive Analytics Handbook for National Defense*, Booz Allen Hamilton, (McLean, VA, Booz Allen Hamilton Inc., 2017), https://www.boozallen.com/d/insight/thought-leadership/predictive-analytics-handbook-for-national-defense.html, 25.
[54] McCue, "Data Mining and Predictive Analytics," 53.

November 2017, the popular fitness app Strava inadvertently revealed the outlines of military bases around the world by publishing a global heat map depicting locations and times of its users' fitness activities.[55] With that information, an adversary could predict when and where coalition forces might be exercising and plan an attack to maximize casualties. Thus, the time-based method is valuable for understanding the adversary threat, but it can also help commanders develop friendly force protection and operational security plans. An even more powerful time-based tool is the use of real-time surveillance.

Among the most in-demand technologies for the modern warfighter is that of intelligence, surveillance and reconnaissance (ISR), and it is among the most advanced with respect to integration with big data. In 2017, the Air Force received nearly 25,000 ISR taskings, collected 340,000 hours of full motion video, and produced 2.55 million intelligence products.[56] Those are striking figures, but they do not fully represent the ISR enterprise. Behind each hour of collected video and each written intelligence product, there are numerous analysts who must process and exploit the data into meaningful intelligence. This is where the DoD hopes the benefit of artificial intelligence and big data will help the most. Project Maven, a joint effort with Google, was a program designed to use artificial intelligence to help identify objects in the video footage collected by ISR platforms thereby freeing analysts to focus on the most pressing priorities and concerns.[57] The program stalled after Google withdrew its cooperation over ethical concerns, but it represents a future role in the expeditionary environment.

---

[55] Richard Perez-Pena and Matthew Rosenberg, "Strava Fitness App Can Reveal Military Sites, Analysts Say," *NYTimes.com*, January 29, 2018, https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html.
[56] *USAF Posture Statement Fiscal Year 2019: Department of the Air Force Presentation to the Committees and Subcommittees of the United States Senate and the House of Representatives*, 115th Cong., 2 (2018) (statement of The Honorable Dr. Heather Wilson, Secretary of the Air Force and General David L. Goldfein, Chief of Staff, United States Air Force), http://www.af.mil/portals/1/documents/1/fy19_AF_Posture_Statement_High_Res.pdf, 2.
[57] Zachary Fryer-Giggs, "Inside the Pentagon's Plan to Win Over Silicon Valley's AI Experts," *Wired*, December 2018, https://www.wired.com/story/inside-the-pentagons-plan-to-win-over-silicon-valleys-ai-experts/.

Force protection in the future will almost certainly rely on data and computer-assisted analytics to detect and identify threats and help predict when a hostile incident is likely to occur. At the same time, future threats will compel the deployment of smaller, more agile units in order to survive. Time-based prediction methods can assist with the reduction of a base's footprint by decreasing the number of security forces, the primary safety and security factor affecting a deployed force's size, required to defend a base.[58] A commander can better tailor security patrol schedules, reduce manning, or request additional support based on the predictions gleaned from data. ISR and liaison with the host nation, if trusted, in advance of the deployment can provide the initial data from which to make initial calculations on force requirements. Additionally, in a contested environment the number and duration of ISR sorties may be severely limited. Having methods in place to process and exploit data quickly and efficiently with a minimal footprint will be imperative to maintaining security while gathering necessary intelligence.

The final prediction method, location-based, has already successfully transitioned from the civilian sector into the current deployed environment. Improvised Explosive Devices (IEDs) presented a major force protection challenge for coalition forces operating throughout Iraq during Operation Iraqi Freedom. Fortunately, the RAND Corporation developed the Actionable HotSpot (AHS) program to detect patterns from past IED incident data to predict where, and eventually when, the next incident was likely to occur.[59] The several test units who received daily nominations from RAND used the information to supplement other intelligence, sometimes just for increased situational awareness, and other times to actually adjust patrols or sniper

[58] Patrick Mills et al., *Estimating Air Force Deployment Requirements for Lean Force Packages: A Methodology and Decision Support Tool Prototype*, RAND Project AIR FORCE (Santa Monica, CA, RAND Corporation, 2017), https://www.rand.org/pubs/research_reports/RR1855.html, 51.
[59] Perry, et al., *Predictive Policing*, 73.

teams.[60] The program identified future IED incidents with an average success rate of 30%, with success defined as an IED incident taking place in a predicated area within the 24 or 48 hours following its placement on the list.[61] The program's success supports, and expands, the fundamental finding in Weisburd's study that criminal activity is highly concentrated, even in a military combat environment. Additional research further supports the "spatio-temporal pattern" of IED attacks, presenting significant implications for how the military might utilize a location-based prediction method in the future.[62]

Flexibility is one of the largest benefits the location-based prediction methods offer. In a manner similar to that of the time-based method, predicting where a hostile incident might occur allows a commander to tailor resources and responses to more specific threats. Additionally, because of the dispersed nature of future expeditionary operations, accurate predictions can create opportunities to enlist the help of host nation police and security forces without having to utilize scarce joint force resources. A host nation does not want hostile incidents endangering its own people, so there is an incentive for cooperation and intelligence sharing. Depending on the speed and pace of the conflict, location-based methods can help commanders decide where to land their forces. If a particular island or swath of land is likely to experience hostile activity, analytics could recommend alternative aerial or sea ports of debarkation with less risk. Additionally, accurate predictions could serve as the basis for deception operations. The joint force could make it appear they are still planning to arrive at or depart from a targeted location when in actuality they are moving to a less threatened area. In sum, location-based prediction

[60] Ibid., 74.
[61] Ibid., 74.
[62] Michael Townsley, Shane D. Johnson, and Jerry H. Ratcliffe, "Space Time Dynamics of Insurgent Activity in Iraq," *Security Journal* 21, no. 3 (July 2008): 144-145, https://doi.org/10.1057/palgrave.sj.8350090.

methods grant commanders greater awareness of potential threats and flexibility in how to mitigate them.

Big Data and Predictive Analytics Limitations

In addition to the positive benefits big data and predictive analytics offer in an expeditionary environment, there are also limitations that one must recognize and be prepared to overcome. Future conflict is likely to exist across all domains: air, land, sea, space, and cyber. Unlike today's conflicts where air supremacy is so common one can easily take it for granted and satellites can relay information with minimal concern for interception, future conflicts will not be as manageable. The joint force's reliance on data to generate intelligence and situational awareness makes it a desirable target for an adversary.

In fact, data protection will be more important and challenging than ever to implementing a data-driven strategy in an expeditionary environment. Recent research suggests it is possible to make changes to an image that are imperceptible to the human eye, yet cause neural networks to misinterpret the image despite believing it to be recognizable with 99.99% certainty.[63] This could pose major concerns for data collected from ISR platforms and analyzed with artificial intelligence. If an adversary hacks the data, it could lead to the misidentification of an adversary threat or, worse, the identification of a friendly force as hostile. Further, big data sets are vulnerable to data poisoning, which occurs by introducing compromised initial training data into a system that will cause it to make errors.[64] As mentioned previously, quality data in equals

[63] Anh Nguyen, Jason Yosinski, Jeff Clune, "Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images," In Computer Vision and Pattern Recognition (CVPR '15), IEEE (April 2015), 1, https://arxiv.org/pdf/1412.1897.pdf.

[64] Miles Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Migration," *arXiv preprint* (2018), 17, https://arxiv.org/pdf/1802.07228.pdf.

quality data out. If the training data is corrupt from the start, it ruins the value of any identified trends and predictions.

Additionally, there are concerns about how facial recognition algorithms could contain biases based on the content of the training data. These algorithms develop their ability to determine the similarity of facial features in photographs by practicing on training data sets containing pre-loaded faces.[65] However, a 2011 study suggested that "the conditions in which an algorithm is created—particularly the racial makeup of its development team and test photo databases—can influence the accuracy of its results."[66] The findings of this study should serve as a cautionary warning. Databases designed to help identify individuals in an expeditionary environment, but created in the United States, may inherently contain biases that decrease their effectiveness and generate false positives. The consequences of a false positive identification in a near-peer conflict are likely to be strategic in nature and could be catastrophic.

Another challenge is determining the type of data needed to support predictive analytics and how best to acquire it. Military forces may only be at an expeditionary location for small periods of time, thus making it difficult to collect the amounts of data needed to make accurate predictions. Gathering data on past hostile incidents is an obvious starting point, but that could prove more difficult than expected. Certain host nations may be reluctant or flatly refuse to release criminal and terrorism information. An alternative option is to rely on news reports and social media to provide some perspective, but then accuracy and bias concerns may arise. The most reliable method is for the United States to gather the data itself through a variety of intelligence collection disciplines. A risk with this approach is that any historical data could

[65] Clare Garvie and Jonathan Frankle, "Facial Recognition Software Might Have a Racial Bias Problem," *The Atlantic*, April 7, 2016, https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991.
[66] Ibid.

become irrelevant once military forces arrive at an expeditionary base. Local public opinion might view a foreign military presence as overbearing or imperialist, and thus the focus of historical criminal activity could start to shift towards an anti-U.S. sentiment and alter any predications. Accurate predictions require time to build reliable data; unfortunately, time will be a critical element in future conflict. The speed of war has changed, and the side that makes decisions faster than an adversary and outpaces its thinking is likely to be victorious.[67] As a result, the applicability of big data and predictive analytics in a future expeditionary environment is directly related to the speed of data collection.

Recommendations

Big data and predictive analytics will undoubtedly serve a prominent role in securing future expeditionary bases and protecting the forces who fight from them. Below are several recommendations that will help transition the concepts from civilian police departments to a combat military force:

- **Strategy Integration** - Integrating these concepts into a base defense strategy will provide commanders better situational awareness and improve their ability to make force protection decisions in an increasingly competitive and uncertain security environment. The 2018 DoD Artificial Intelligence Strategy relates this type of integration requires "iterative, interdisciplinary development of technology…and will demand early study of the cognitive and physical work that can be improved."[68] The technology associated with big data and predictive analytics is proving itself in the

[67] Joseph F. Dunford, Jr., "From the Chairman: The Character of War and Strategic Landscape Have Changed," *Joint Forces Quarterly* 89, no. 2 (April 2018): 2-3, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-89/jfq-89.pdf?ver=2018-04-19-153711-177.

[68] US Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*, Washington, DC, 2018, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/summary-of-dod-ai-strategy.pdf, 11.

field of law enforcement, but it must continue to evolve to meet the unique requirements of the military and its mission to defend the nation. This is not an easy endeavor, but it is imperative to continue addressing the challenge as quickly as possible. A comprehensive effort that brings together experts from industry, academia, law enforcement, and other federal government agencies to explore the technological requirements is a necessary first step.

- **Wargaming and Simulation** - Once established, testing of existing technologies when applied to the individual, time and location-based predictive methods should continue through the use of wargaming and simulation. The newly-established DoD Joint Artificial Intelligence Center in coordination with organizations such as the Defense Advanced Research Projects Agency, DIUx, and DoD laboratories must work to adapt algorithms and collect the diverse data needed to rigorously test the accuracy and reliability of predictive technologies in a military context. In this setting, the joint force can examine potential big data and predictive capabilities across a range of military situations, from peacetime to near-peer conflict, to determine when and how to best employ them.
- **Talent Management** – The DoD must look to attract and retain talented individuals. Existing recruitment approaches attempting to inspire a dedication to a higher cause may not resonate with the young engineering students at the nation's top universities, so the DoD could utilize industry exchange programs to generate and maintain interest in the defense enterprise.[69] Bringing new talent into the artificial intelligence

[69] Amy Zegart and Kevin Childs, "The Divide Between Silicon Valley and Washington is a National Security Threat," *The Atlantic*, December 13, 2018, https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963/.

field will facilitate a program that is at the leading edge of research thought and design. Equally important is ensuring those with years of talent and expertise remain motivated to their work with the military. In cooperation with civilian institutions as noted above, this will stimulate new and innovative ways to solve the big data and predictive analytics challenges.

- **Culture** – The DoD's willingness to embrace the transition from a descriptive to predictive analytical organization is a difficult task that will be crucial to force protection in the future. Dawn Meyerriecks, the Deputy Director of the Science and Technology Directorate at the Central Intelligence Agency, notes the greatest challenge in applying technology such as big data and predictive analytics is convincing senior leaders to trust intelligence that comes from a robot.[70] Developing a culture that is willing to accept this type of risk will not happen overnight, but building incremental confidence in the systems by testing them alongside traditional methods will help foster an accepting mindset.
- **Cyber Applicability** - Further research should also focus on the multi-domain nature of future conflict. This paper concentrated on the applicability of data and analytics for physical security and force protection purposes, but the possibility of a digital cyber threat that could destroy an expeditionary base from the inside out is very real. Just as in the physical domains, predictive analytics can provide better situational awareness of networks which, in turn, assist in prioritizing and tailoring incident response.[71] However, there are distinctive challenges in cyberspace, such as

[70] Patrick Tucker, "What the CIA Tech Director Wants From AI," *Defense One*, September 6, 2017, https://www.defenseone.com/technology/2017/09/cia-technology-director-artificial-intelligence/140801.
[71] Jon Ostik, "The Big Data Security Analytics Era is Here," (White Paper, Enterprise Security Group, January 2013), 3, https://www.emc.com/collateral/analyst-reports/security-analytics-esg-ar.pdf.

deception, attribution, and inadvertent escalation, that could limit the effectiveness of predictive analytics for cyber security and protection. These challenges warrant further examination by cyber experts to determine the significance of their influence on force protection in the expeditionary environment.

Conclusion

The future expeditionary environment will require the United States military to reconsider how it secures and protects its personnel, equipment, and facilities from the challenges posed by a near-peer competitor. Additionally, maintaining freedom of action in a battlespace contested with advanced A2/AD platforms means the joint force must employ a strategy that ensures maximum dispersion and resiliency without compromising capability and capacity to project power. Police departments have proven there is great potential in predicative analytics and an increasingly digitized world makes the combination of individual, time, and location-based predictive methods more important than ever to ensuring security in both civilian and military environments. Ultimately, a data and predictive analytics-based approach to security and force protection operations in an expeditionary environment will provide military commanders the situational awareness and flexibility necessary to make decisions more quickly and with better confidence.

Bibliography

American Civil Liberties Union. "Predictive Policing Today: A Shared Statement of Civil Rights Concerns." August 31, 2016, https://www.aclu.org/other/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice.

Andrejevic, Andre. *Infoglut: How Too Much Information is Changing the Way We Think and Know*. New York: Routledge, 2013.

Bachner, Jennifer. "Predictive Policing: Preventing Crime with Data and Analytics." IBM Center for the Business of Government, Improving Performance Series, John Hopkins University, 2013, http://www.businessofgovernment.org/report/predictive-policing-preventing-crime-data-and-analytics.

Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, et al. "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation." *arXiv preprint* (2018), https://arxiv.org/pdf/1802.07228.pdf.

Caplan, Joel M., Leslie W. Kennedy, and Joel Miller. "Risk Terrain Modeling: Brokering Criminological Theory and GIS Methods for Crime Forecasting." *Justice Quarterly* 28, no. 2 (April 2011): 360-381, https://doi.org/10.1080/07418825.2010.486037.

Chainey, Spencer, Lisa Thompson, and Sebastian Uhlig. "The Utility of Hotspot Mapping for Predicting Spatial Patterns of Crime." *Security Journal* 21 (February 2008): 4-28, https://doi.org/10.1057/palgrave.sj.8350066.

Chi, Michael. "Big Data in National Security." *Australian Strategic Policy Institute,* August 2017. https://www.jstor.org/stable/resrep04118.

Dean, Benjamin C. "Big Data: The Latest Tool in Fighting Crime" in "BIG DATA: A Twenty-First Century Arms Race." Washington DC: Atlantic Council. www.jstor.org/stable/resrep03719.

Defense Innovation Unit Experimental (DIUx), *DIUx Annual Report 2017*, (Silicon Valley, CA, DIUx, 2017), https://diux.mil/download/datasets/1774/DIUx%20Annual%20Report%202017.pdf.

Dries, William. "Some New, Some Old, All Necessary: The Multi-Domain Imperative." *War on the Rocks*, March 27, 2017. https://warontherocks.com/2017/03/some-new-some-old-all-necessary-the-multi-domain-imperative.

Dunford, Jr., Joseph F. "From the Chairman: The Character of War and Strategic Landscape Have Changed." *Joint Forces Quarterly* 89, no. 2 (April 2018): 2-3, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-89/jfq-89.pdf.

Ferguson, Andrew Guthrie. "Big Data and Predictive Reasonable Suspicion." *University of Pennsylvania Law Review* 163, no. 2 (January 2015): 327-410, https://www.jstor.org/stable/24247848.

Ferguson, Andrew Guthrie. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press, 2017.

Finn, Rachel L. and David Wright. "Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications." *Computer Law & Security Review* 28 (2012): 184-194, https://www.dhi.ac.uk/san/waysofbeing/data/data-crone-finn-2012.pdf.

Fryer-Giggs, Zachary. "Inside the Pentagon's Plan to Win Over Silicon Valley's AI Experts." *Wired*, December 2018. https://www.wired.com/story/inside-the-pentagons-plan-to-win-over-silicon-valleys-ai-experts/.

Garvie, Clare and Jonathan Frankle. "Facial Recognition Software Might Have a Racial Bias Problem." *The Atlantic*, April 7, 2016, https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991.

Hutchens, Michael E., William D. Dries, Jason C. Perdew, Vincent D. Bryant, and Kerry E. Moores. "Joint Concept for Access and Maneuver in the Global Commons." *Joint Force Quarterly* 8, no.1 (January 2017): 134-139, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-84/jfq-84.pdf.

Intel. "A Guide to the Internet of Things." https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.

Jacobsohn, Mark and Scott Jachimski. *Predictive Analytics Handbook for National Defense*. Booz Allen Hamilton. McLean, VA, Booz Allen Hamilton Inc., 2017. https://www.boozallen.com/d/insight/thought-leadership/predictive-analytics-handbook-for-national-defense.html.

Klein, Lawrence A. *Sensor and Data Fusion: A Tool for Information Assessment and Decision Making.* Bellingham, WA, SPIE Press, 2004.

Levine, Ned. "Crime Mapping and the *CrimeStat* Program." *Geographical Analysis* 38, no. 1 (January 2006): 41-56, https://doi.org/10.1111/j.0016-7363.2005.00673.x.

Linning, Shannon J., Martin A. Andersen, and Paul J. Brantingham. "Crime Seasonality: Examining the Temporal Fluctuations of Property Crime in Cities with Varying Climates." *International Journal of Offender Therapy and Comparative Criminology* 61, no. 16 (March 2016): 1-26, https://doi.org/10.1177/0306624X16632259.

Marine Corps Warfighting Laboratory. *Industry Panel Discussion*. PowerPoint presentation, Naval S&T Expo, April 20, 2017, https://www.mcwl.marines.mil/portals/34/ST_ExpoBRIEF_ApprovedPublicRelease.pdf.

McCue, Colleen. "Data Mining and Predictive Analytics: Battlespace Awareness for the War on Terrorism." *Defense Intelligence Journal* 13, no.1/2 (2005): 47-63.

Mills Patrick, James A. Leftwich, Kristin Van Abel, Jason Mastbaum. *Estimating Air Force Deployment Requirements for Lean Force Packages: A Methodology and Decision Support Tool Prototype*. RAND Project AIR FORCE. Santa Monica, CA, RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1855.html.

Nguyen, Anh, Jason Yosinski, and Jeff Clune. "Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images." In Computer Vision and Pattern Recognition (CVPR '15), IEEE (April 2015), https://arxiv.org/pdf/1412.1897.pdf.

Ostik, Jon. "The Big Data Security Analytics Era is Here." White Paper. Enterprise Security Group. January 2013. https://www.emc.com/collateral/analyst-reports/security-analytics-esg-ar.pdf.

Perry, Walter L., Brian McInnis, Carter C. Prince, Susan C. Smith, and John S. Hollywood. *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND Safety and Justice Program. Washington DC, RAND Corporation, 2013. https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

Peterson, Ruth D. and Lauren J. Krivo. "Race, Residence, and Violent Crime: A Structure of Inequality." *Kansas Law Review* 57, no. 4 (April 2009): 903-933, https://kuscholarworks.ku.edu/bitstream/handle/1808/20100/7.0-Peterson_Final.pdf?sequence=1&isAllowed=y.

Rosser, Gabriel, Toby Davies, Kate J. Bowers, Shane D. Johnson, and Tao Cheng. "Predictive Crime Mapping: Arbitrary Grids or Street Networks." *Journal of Quantitative Criminology* 33, no. 3 (2017): 569-594, https://doi.org/10.1007/s10940-016-9321-x.

Sayler, Kelley M. *Artificial Intelligence and National Security*. CRS Report for Congress R45178. Washington DC: Congressional Research Service, January 30, 2019. https://fas.org/sgp/crs/natsec/R45178.pdf.

Siegel, Eric. *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die*. Hoboken, NJ: John Wiley & Sons, 2013.

Telep, Cody W. "Police Interventions to Reduce Violent Crime: A Review of Rigorous Research." Fairfax, VA: Center for Evidence-Based Crime Policy, George Mason University, http://cebcp.org/wp-content/onepagers/InterventionsToReduceCrimeReview_Telep.pdf.

Townsley, Michael, Shane D. Johnson, and Jerry H. Ratcliffe. "Space Time Dynamics of Insurgent Activity in Iraq." *Security Journal* 21, no. 3 (July 2008): 139-146, https://doi.org/10.1057/palgrave.sj.8350090.

Tucker, Patrick. "What the CIA Tech Director Wants From AI." *Defense One*, September 6, 2017. https://www.defenseone.com/technology/2017/09/cia-technology-director-artificial-intelligence/140801.

Ünver, H. Akin. *Politics of Digital Surveillance, National Security and Privacy*. Cyber Governance and Digital Deomcracy. Istanbul, Turkey: Centre for Economics and Foreign Policy Studies, April 2018. https://www.jstor.org/stable/resrep17009.

USAF Posture Statement Fiscal Year 2019: Department of the Air Force Presentation to the Committees and Subcommittees of the United States Senate and the House of Representatives, 115th Cong., 2 (2018) (statement of The Honorable Dr. Heather Wilson, Secretary of the Air Force and General David L. Goldfein, Chief of Staff, United States Air Force), http://www.af.mil/portals/1/documents/1/fy19_AF_Posture_Statement_High_Res.pdf

US Department of Defense. *Joint Operations*. Joint Publication 3-0. Washington, DC: US Department of Defense, January 17, 2017 Incorporating Change 1, October 22, 2018.

US Department of Defense. *Joint Security Operations in Theater*. Joint Publication 3-10. Washington, DC: US Department of Defense, November 13, 2014.

US Department of Defense. *National Defense Strategy of the United States of America*. Washington, DC, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

US Department of Defense. *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*. Washington, DC, 2018. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/summary-of-dod-ai-strategy.pdf.

Weisburd, David. "The Law of Crime Concentration and the Criminology of Place." *Criminology* 53, no. 2 (2015): 133-157, https://doi.org/10.1111/1745-9125.12070.

Zegart, Amy and Kevin Childs. "The Divide Between Silicon Valley and Washington is a National Security Threat." *The Atlantic*, December 13, 2018, https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963/.