Cybersecurity Support of Insider Threat Operations: DoD Regulation and Constitutional Compliance

*Capt. Salahudin Ali**†

Introduction

Insider threats are a common foe to many organizations.[1] The United States (U.S.) government is no exception.[2] The Department of Defense (DoD) defines an insider threat as "[a] *person*, known or suspected, who uses their authorized access to DoD facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise DoD information, or commit espionage on behalf of an FIE [Foreign Intelligence Entity]."[3] Although the common belief is that insider threats occur for espionage purposes, insider threats commit actions for a variety of reasons; psychological beliefs and other personal motivations have been found to be core elements.[4] Indeed, the DoD has suffered a string of visible insider threat incidents, including Edward Snowden's leak of classified information and Harold Thomas Martin III's theft of highly classified pro-

* Judge Advocate, United States Marine Corps. LL.M., 2018, Antonin Scalia Law School at George Mason University; J.D., 2011, Lewis & Clark Law School. The comments, thoughts, and opinions in this article are those of the author and are not associated with the Department of Defense or any other government agency.

† The author recognizes that the existence of classified sources may significantly impact this article's analysis. All errors are my own.

1 Zehra Ali, *Insider Threat Statistics,* U.S. Cybersecurity Magazine (2018), https://www.uscybersecurity.net/insider-threats-2018-statistics/; *see also* Harriet Taylor, *Insider threats may be the biggest cyberthreats an organization faces,* CNBC (Oct. 5, 2016), https://www.cnbc.com/2016/10/05/insider-threats-may-be-the-biggest-cyberthreat-an-organization-faces.html.

2 *Science and Technology: Insider Threat*, U.S. Dep't of Homeland Sec., https://www.dhs.gov/insider-threat-cyber (last visited Sept. 27, 2019).

3 U.S. Dep't of Def., Instr. 5240.26, Countering Espionage, International Terrorism, and the Counterintelligence Insider Threat 12-13 (Apr. 30, 2018) (emphasis and brackets added).

4 *See* David L. Charney & John A. Irvin, *The Psychology of Espionage*, 22 The Intelligencer J. of U.S. Intelligence Studies 71 (2016); *see also* David L. Charney, *True Psychology of the Insider Spy* 2 (2014) (explaining that money, ideology, and ego are factors that motivate insider spies).

gram information, both for separate reasons.[5] As a result, the DoD continues to maintain an expansive interdisciplinary insider threat detection program that blends elements of intelligence and cybersecurity authorities and advanced technologies as part of its efforts to detect, deter, and deny those who pose a danger to DoD agencies from within.[6] This program ensures such incidents do not result in encore performances and serves as an example of operationalizing sound insider threat prevention programing.[7]

The DoD utilizes cybersecurity technology to support the DoD's insider threat program by using artificial intelligence (AI) and machine learning methodologies for continuous monitoring, assessment, and analysis of user activity.[8] Cybersecurity is generally considered a service that uses a "process of protecting information and information systems by preventing, detecting, and responding to unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability."[9] Constant monitoring and analysis is done by the DoD on a pervasive and warrantless basis to allow this service the most effective use of

---

[5] *See* Christopher Woolley, Mark D. Troutman, & Paul B. Losieiwicz, *Insider Threat: Policy Impact and Overview* 4 (2014) ("The recent case of Edward Snowden brought insider threat to the forefront of the public and corporate mind."); Christian Davenport, *NSA case highlights growing concerns over insider threats*, WASH. POST (Oct. 6, 2016), https://www.washingtonpost.com/business/economy/nsa-case-highlights-growing-concerns-over-insider-threats/2016/10/06/61b90a5e-8bc7-11e6-bf8a-3d26847eeed4_story.html?utm_term=.6a02a7c8bda9; *see also* Josh Gerstein, *Feds' case against alleged NSA hoarder hits turbulence*, POLITICO (Feb. 26, 2018) (explaining that Martin III was motivated by mental illness), https://www.politico.com/blogs/under-the-radar/2018/02/26/nsa-classified-information-home-424293.

[6] *See* National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 922, 125 Stat. 1298, 1537-39 (2011) (authorizing the establishment of the Insider Threat Detection Program); Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 76 Fed. Reg. 65811 (Oct. 7, 2011) (instructing all executive agencies to establish insider threat programs to protect classified national security information); PRESIDENTIAL MEMORANDUM: NATIONAL INSIDER THREAT POLICY AND MINIMUM STANDARDS FOR EXECUTIVE BRANCH INSIDER THREAT PROGRAMS (2012); U.S. DEP'T OF DEF., DIR. 5205.16, THE DOD INSIDER THREAT PROGRAM (2017); U.S. DEP'T OF DEF., INSTR. 8500.01, CYBERSECURITY (2014); U.S. DEP'T OF DEF., INSTR. 8530.01, CYBERSECURITY ACTIVITIES SUPPORT TO DOD INFORMATION NETWORK OPERATIONS (2017).

[7] U.S. DEP'T OF DEF., DIR. 5205.16, THE DOD INSIDER THREAT PROGRAM (2017).

[8] *See* U.S. DEP'T OF DEF., INSTR. 8500.01, CYBERSECURITY (2014); U.S. DEP'T OF DEF., INSTR. 8530.01, CYBERSECURITY ACTIVITIES SUPPORT TO DOD INFORMATION NETWORK OPERATIONS (2017).

[9] CHRIS JAIKARAN, CONG. RES. SERV., R45127, CYBERSECURITY: SELECTED ISSUES FOR THE 115TH CONGRESS 2 (2018).

these advanced technologies.[10] The intersection between the DoD's use of cybersecurity on its own networks to support its insider threat program and the individual constitutional rights of employees and authorized users of DoD networks who may be potential threats is a key issue for the DoD.

Thus far, government and academic commentary has attempted to address the matter of warrantless and pervasive monitoring of government networks.[11] This commentary primarily focuses on one cybersecurity program: *Einstein*.[12] Commentators ultimately concluded that the use of these cybersecurity programs is constitutionally sufficient and only minimally impacts privacy so long as certain processes and procedures of monitoring are followed.[13]

Although correct in its analysis, previous commentary may not be fully capable of addressing the DoD insider threat program. First, the commentary dealt with technology used in *Einstein* that was not truly an AI tool nor a tool that used machine learning methodologies. Instead, it dealt with technology that performed as an automated system.[14] Second, the commentary addressed *Einstein* tools, which the DoD does not use.[15] Third, previous commentary addressed the limited context of cyberspace threats involving malicious and harmful codes based upon signatures.[16] Although the DoD insider threat program includes aspects of cybersecurity threats, like malicious code and signatures, the program remains focused on the *human actor*—and indicators that drive her behavior—and her ability to extend harm beyond a cyberspace network.[17] Lastly, the previous commentary was written in the absence of the strong regulatory and programmatic regimes that govern intelligence and counterintelligence activities

---

[10] *Cf.* NAT'L INST. OF STANDARDS AND TECH., RISK MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEMS AND ORGANIZATIONS: A SYSTEM LIFE CYCLE APPROACH FOR SECURITY AND PRIVACY, NO. 800-37, at 2 (2018).

[11] *See* 18 U.S.C. § 2511 (2018); *see also* Federal Information Security Modernization Act of 2014, Pub. Law. No. 113-283, § 3551(4) ("[P]rovide a mechanism for oversight of Federal agency information security programs, including through automated security tools to continuously diagnose and improve security[.]").

[12] *E.g.*, U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE INITIATIVE THREE EXERCISE 3 (2018).

[13] *See* 18 U.S.C. § 2511 (2018) (outlining the legal ways to intercept electronic communications).

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] U.S. DEP'T OF DEF., DIR. 5205.16, THE DOD INSIDER THREAT PROGRAM (2017).

within the DoD.[18] This indicates a point of legal departure between the technology used, its framework, and authorities allowing the DoD to conduct insider threat detection and prevention operations on a legally sufficient basis using advanced AI and machine learning technologies as support. These points of legal departure have yet to be examined.

Quickly merging innovative and advanced technologies into existing programs poses legal issues when there is little understanding of how the technologies operate and impact existing constitutional and statutory rights of network users. Today's AI and machine learning technologies use advanced hidden algorithms for statistical and pattern recognition, psychological behavioral profiling, and deep neural networks.[19] This allows AI agents to mimic human critical thinking, operate autonomously, act rationally, and learn continuously to detect, prevent, and deter insider threats in cyberspace.[20] Public confidence and understanding are vital for the longevity of these programs to avoid the perception that large and powerful government organizations, like the DoD, operate against the constitutional and privacy rights of citizens. Without public confidence and understanding, these programs may remind the public of domestic intelligence surveillance abuses of the past.[21]

This Article seeks to address the legal issues created under the DoD's regulatory regime regarding the use of AI and machine learning methodologies to detect and prevent insider threats on its cyberspace network. It also provides an example for other organizations to show how strong legal authority and an understanding of constitutional compliance through internal regulation and procedures can serve as a force-multiplier for preventative insider threat operations.

This Article's analysis uses three main internal DoD regulations: (1) *Department of Defense Directive 5205.16*, which authorizes the insider threat program; (2) *Department of Defense Instructions 8500.01* and *8530.01*, which provide for cybersecurity support of insider threat operations; and (3) *Department of Defense Manual 5240.01* (the Manual), which implements constitutional privacy and

---

[18] *Id.*

[19] Cliff Kuang, *Can A.I. Be Taught to Explain Itself?*, N.Y. TIMES MAG. (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html.

[20] *Id.*

[21] *See* S. REP. NO. 94-755 (1976) (revealing decades of constitutional violations by intelligence agencies during the Cold War).

civil liberties protections during intelligence and counterintelligence gathering actions. This final regulation also establishes processes and procedures for organizations seeking to enforce constitutional compliance during insider threat operations. These regulations give the DoD authority to conduct insider threat detection and prevention using cybersecurity assistance. The regulations are based on strong executive intelligence collection authorities and compliance with protections for privacy and civil liberties.[22] This Article concludes by illustrating the DoD's implementation of its regulatory system for preventing and detecting insider threats is complex but constitutionally adequate to protect privacy and civil liberties.

Part I of this Article will illuminate the nature of cyberspace, detail previous government and academic commentary, explain issues in typology for the different technologies involved, and explore problems with the frameworks of applying these technologies. Part II references the legal framework that may impact DoD's use of AI and machine learning in support of its insider threat context. Part III introduces a hypothetical that analyzes the legal landscape and technology involved. Part IV provides normative arguments about current uses of AI and machine learning. Finally, this Article concludes by reemphasizing how the DoD utilizes AI within the legal parameters set by both the United States Consitution and relevant jurisprudence.

I. ISSUES

A. *Cyberspace*

The issue of insider threats in cyberspace is murky, partly due to the very nature of the problem.[23] The DoD defines cyberspace as a "global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and control-

22 *See* U.S. DEP'T OF DEF., DIR. 5205.16, THE DOD INSIDER THREAT PROGRAM 1 (2017) (describing that the directive is authorized by the National Defense Authorization Act and Executive Orders related to intelligence collection).

23 *See* Peter Pascucci, *Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution*, 26 MINN. J. INT'L L. 419, 426 (2017).

lers."[24] The interdependence, interconnectedness, and complexity of cyberspace exists in the DoD's network. This network is vast and transacts many facets of national security information of various classifications that are strategic assets.[25] Cyberspace was originally created by the DoD for communication, storage, and access of information in case of nuclear war.[26] However, cyberspace quickly emerged as an academic and consumer enterprise focused on the ease and efficiency of communicating information, in direct contrast to the security of information.[27] The current model for creating programs and applications that later fix vulnerabilities—"patching," a software update that temporarily fixes an existing vulnerability before the full release of entirely new software—is ill-suited for national defense.[28] The lack of focus on security from the outset by enterprising and innovative companies is a problem for the DoD in managing the security of its cyberspace network.[29] This issue is a consequence of cyberspace's natural tendencies, like its interconnectedness to the larger outside cyberspace environment.[30]

The interconnectedness of interdependent networks that rely on certain protocols to communicate with each other became the advent of the ubiquitous internet of cyberspace—the connection of many networks to form a larger holistic one.[31] This holistic network includes a number of connected devices, called the "internet of things" (IoT), referring to devices that are interconnected or connected to the internet.[32] IoT devices range from government computers to con-

---

24 JOINT CHIEFS OF STAFF, JOINT PUB. 3-12 GL-4, CYBERSPACE OPERATIONS (2018).

25 U.S. DEP'T OF DEF., DIR. 8000.01, MANAGEMENT OF THE DEPARTMENT OF DEFENSE INFORMATION ENTERPRISE 2 (2017). For example, one study indicates that the DoD experienced 360 million attempts to penetrate its networks in 2008 alone, and explains that the DoD is a global "network of networks," making it hard to configure and control; ERIC LANDREE, ET AL., IMPLICATIONS OF AGGREGATED DOD INFORMATION SYSTEMS FOR INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION 1 (2010).

26 JOHN P. CARLIN, DAWN OF THE CODE WAR, 39-40 (2018).

27 *Id.; see also* Barry M. Leiner, et al., *A Brief History of the Internet*, 39 ACM SIGCOMM COMPUTER COMM. REV. 22, 25 (2009) (explaining that the other concerns with the emergence of cyberspace also included efficiency and internetwork performance, but not security).

28 CARLIN, *supra* note 26, at 40-41; *see also* Andra Zaharia, *15 + Experts Explain Why Software Patching is Key for Your Online Security,* HEIMDAL SEC. (April, 6, 2016), https://heimdalsecurity.com/blog/expert-roundup-software-patching/.

29 *Id.* at 40-47.

30 *Id.*

31 Pascucci, *supra* note 23, at 422-425.

32 Matt Burgess, *What is the Internet of Things? WIRED explains*, WIRED U.K. (Feb. 16, 2018), https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot.

sumer goods. These devices, in theory, are connected to the DoD's network through the larger internet.[33] These devices communicate and share information with one another, which theoretically includes sensitive and classified information located in cyberspace.[34] The vulnerability for each device is also a vulnerability to a DoD network, making it easier for someone outside the DoD to find a way in.[35] If it is easy for someone to find his way into a network and exploit information, then it is clearly even easier for someone on the inside of the DoD's cyberspace network to do the same.

B. *Previous Commentary*

1. Government Commentary

The U.S. government proactively develops automated systems to detect and prevent harm to its many cyberspace networks.[36] This includes constant government surveillance and warrantless monitoring of its systems' users, particularly U.S. citizens, which creates an immediately apparent constitutionality question.[37] Consequently, commentary produced by the Department of Justice (DoJ) Office of Legal Counsel (OLC) and the Department of Homeland Security (DHS) Office of Cybersecurity & Communications sought to analyze the constitutionality and privacy impact of these programs.[38]

---

33 *Id.*

34 *See* BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD 5-8 (2018).

35 CARLIN, *supra* note 26, at 42-47.

36 *See* Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, § 3551(4) ("[P]rovide a mechanism for oversight of Federal agency information security programs, including through automated security tools to continuously diagnose and improve security[.]").

37 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 7-8 (2009).

38 *See id.*; Legality of Intrusion-Detection Sys. to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 2-3 (2009); U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR EINSTEIN-3 ACCELERATED, NPPD E^3 A 4 (2013); DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR EINSTEIN-3 ACCELERATED, NPPD-027(a) E^3 A 4 (2016).

Both commentaries dealt with the *Einstein* program.[39] The program evolved from performing intrusion-detection system (IDS) tasks to also performing intrusion-prevention system (IPS) tasks.[40] At its core, *Einstein* is an automated system that observes information about an electronic message that assists in getting the message to its destination (packet information), and information that assists in converting the message's software code into readable content.[41] The system detects malicious and harmful codes based on associated signatures and threat indicators—clues, known by industry and cybersecurity professionals, that the information represented by a message's software code poses a threat to the network.[42] Signatures and indicators are identified through several classified and unclassified sources from interagency and private sectors.[43] Once a signature or indicator is identified, it is added to a database for sensors to detect during future network infiltration attempts.[44] If a threat is detected, the system alerts an analyst who views the communication and prevents the threat from reaching its destination.[45] At all times during this process, the focus remains on the communication's digital code. Communications not associated with a malicious code are deleted.[46]

Because the system is automated, it conducts continual observation without a warrant.[47] The DoJ commentary, issued via various OLC opinions, analyzed this warrantless surveillance under the Fourth Amendment to the U.S. Constitution.[48] The DoJ concluded that certain third-party metadata information, such as subject lines

---

[39] *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR EINSTEIN-3 ACCELERATED, NPPD E^3 A 4 (2013); U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR EINSTEIN-3 ACCELERATED, NPPD-027(a) E^3 A 4 (2016).

[40] Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 1, 17 (2009).

[41] *Id*. at 2.

[42] *Id.* at 3.

[43] *Id.* at 3-4.

[44] *Id.* at 4.

[45] *Id.* at 33; *see also* GUY BRUNEAU, DNS SINKHOLE 2 (2010) (explaining that the DNS sinkhole can be used to provide IDS and IPS of malicious and unwanted activity occurring within a network by redirecting malicious activity to non-routable IP addresses).

[46] Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 4 (2009).

[47] *Id.* at 17 (arguing that it would be impracticable for the government to obtain a warrant for this type of surveillance).

[48] *Id.* at 17-19.

and IP addresses, was not subject to constitutional protection under case law because it was voluntarily disclosed to the government or government officials.[49] Certain circumstances also provided legal justification for the system's observation under the Constitution, like a user's consent through voluntarily accepting the network's terms of use or administrative reasons outside the scope of criminal investigations.[50] The DoJ ultimately concluded that under a totality of the circumstances analysis, the government's interest in monitoring its network systems outweighed the privacy concerns of individual users, which allowed the warrantless surveillance to continue.[51]

In addition to its analysis on constitutional rights, the OLC also analyzed various statutes that established privacy rights, such as the Wiretap Act,[52] the Foreign Intelligence Surveillance Act (FISA),[53] the Pen Registers and Trap and Trace Devices Statute,[54] and the Stored Communications Act.[55] The OLC opinions combed through each statute and provided justification for each impacted legal rule. After an in-depth analysis, the OLC found these statutes were not violated due to the U.S. government's right to defend its own network, the consent of network users, and the lack of a legitimate privacy expectation during the use of the network.[56]

DHS provided its own commentary of *Einstein* in a privacy impact assessment on U.S. government network users under the Privacy Act of 1974[57] and its progeny.[58] A noted difference from the DoJ commentary was DHS's review of *Einstein*'s evolution from an IDS to

---

[49] *Id.* at 19 (citing Illinois v. McArthur, 531 U.S. 326, 330 (2001) ("[W]hen faced with . . . diminished expectations of privacy, minimal intrusions, or the like, certain general, or individual, circumstances may render a warrantless search or seizure reasonable.").

[50] *Id.* at 15.

[51] *Id.* at 20; Legality of Intrusion-Detection Sys. to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 4 (2009).

[52] Wiretap Act, 18 U.S.C. §§ 2510-2522 (2019).

[53] Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1885c (2019).

[54] Pen Registers and Trap and Trace Devices Statute, 18 U.S.C. §§ 3121-3127 (2019).

[55] Stored Communications Act, 18 U.S.C. §§ 2701-2713 (2019); *see* Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 1 (2009); Legality of Intrusion-Detection Sys. to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 1, 5 (2009).

[56] Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 35 (2009); Legality of Intrusion-Detection Sys. to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 5 (2009).

[57] Privacy Act of 1974, 5 U.S.C. § 552a (2019).

an IPS, which gave it advanced capability to not only detect threats but also prevent them in real-time.[59] The DHS assessment concluded that appropriate notice, retention, and use of *Einstein* as governed by internal regulations caused a minimal impact on user privacy.[60]

Although these government commentaries are relevant when analyzing any warrantless search scenario on a government cyberspace network, the issue remains that these commentaries were not based on an analysis of internal DoD regulations. Rather, they were conducted in a pure cybersecurity context and based on legal authorities like the Federal Information Security Modernization Act[61] and other corresponding cybersecurity regulations.[62] Moreover, these commentaries did not contain the same type of advanced technologies and methodologies that are used for DoD insider threat detection and prevention.[63] The focus on *human actors,* their motivation indicators, and their ability to extend the threat beyond the network is the difference between previous technologies and the technologies discussed in this Article, because of the dynamic nature humans bring to a cyberspace environment. To defeat this threat, we need systems that think and predict human behavior in cyberspace.

2. Commentary in Academia

Academia has also attempted to address the pervasive and warrantless monitoring of government network systems.[64] One such commentary, authored by noted scholar Professor Jack Goldsmith,

---

58 U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR EINSTEIN-3 ACCELERATED, NPPD-027(a) E^3 A 1 (2016).

59 *Id.*

60 *Id.* at 7-8.

61 Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551-3559 (2019).

62 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 1 (2009); Legality of Intrusion-Detection Sys. to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 1 (2009).

63 *See* U.S. DEP'T OF DEF., DIR. 5205.16, THE DOD INSIDER THREAT PROGRAM 2 (2017) (stating that the Department's programs needed to cooperate to successfully respond to threats).

64 *See* Jack Goldsmith, *The Cyberthreat, Government Network Operations, and the Fourth Amendment*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 47, 48 (2011); Steven M. Bellovin et al., *Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure,* 3 HARV. NAT'L SEC. L.J. 1 (2011); Gordon Lederman & Kate Martin, *The Threat from Within: What is the Scope of Homegrown Terrorism?*, A.B.A. J. (July 1, 2012, 10:00 AM), http://www.abajournal.com/magazine/article/the_threat_from_within_what_is_the_scope_of_homegrown_terrorism/.

analyzed the *Einstein* system and its constitutionality and quasi-constitutionality.[65] In his commentary, Goldsmith notes that the *Einstein* system "requires (among other things) real-time traffic analysis, real-time detection, and real-time response" to provide the optimal level of defense for the government.[66] He provides imaginative hypothetical solutions about how technology applications can assist in securing critical government infrastructure as well as commercial infrastructure.[67] However, these solutions raise the same issues as the government commentaries regarding the Fourth Amendment and privacy protections.

First, Goldsmith notes that there must be a significant effort to "alter the complex patchwork of mostly outdated restrictions on the government's ability to collect and analyze the content" of the communications domestically, or involving U.S. citizens.[68] This effort requires the DoD to take a more proactive role in domestic cyber defense.[69] This does not implicate that U.S. citizens are subject to military authority, because DoD components would not perform law enforcement functions such as arresting or prosecuting citizens, nor force citizens to abide by DoD regulations. Instead, the DoD would only gather intelligence, and its operations would be governed by creating a new statutory authority.[70]

Second, Goldsmith notes there would need to be an incentive for the private sector to assist in these intelligence gathering cybersecurity operations.[71] Because many firms have a global presence, they are subject to foreign adversary power.[72] Statutes, like the Cybersecurity Information Sharing Act of 2015 (CISA), which allowed private companies to conduct certain countermeasures against cyber-security threats and encouraged them to share this information with the U.S. government, attempted to address this issue.[73] However, CISA has

---

65 Goldsmith, *supra* note 64, at 47.

66 *Id.* at 52.

67 *See id.* at 52-53.

68 *Id.* at 55-56.

69 *See id.* at 56.

70 *Id.* (suggesting statutory frameworks for accountability and review).

71 Goldsmith, *supra* note 64, at 53.

72 *Id.* at 57 (describing pressures on AT&T and Verizon to help China with cybersecurity tasks).

73 Cybersecurity Information Act of 2015, 6 U.S.C. § 1502 (2015).

been criticized as being too weak to address this issue.[74] The argument still stands that more incentives could be provided to address private sector concerns, shepherding a holistic societal approach to cybersecurity.

Finally, Goldsmith notes that Fourth Amendment concerns surrounding pervasive monitoring "present the most significant constitutional hurdle to the cybersecurity regime."[75] He ultimately comes to the same conclusion as the government commentaries: the third-party doctrine, special needs (administrative searches), and the reasonableness of such data collection pass constitutional muster.[76]

Other scholars have explored the feasibility of implementing the *Einstein* program to the private sector.[77] These scholars have analyzed how *Einstein*'s inability to dictate the hardware and software choices of private parties, as well as different legal regimes that govern private sector and government actors, raise questions about the success of the program.[78] Unfortunately, the complexities in common technical software and information gathering, interoperability, and inconsistent legal regimes create a blockade to a holistic cybersecurity approach between the government and private sectors.[79] However, this conclusion is dated, as DHS has since implemented *Einstein* through service-level agreements with the private sector.[80]

Whatever the case, academics present the same issues as the government commentary. Academic commentary analyzed an automated system that focuses on detecting and preventing malicious code, signatures, and indicators, but did not address how cybersecurity could focus on human actors to predict and prevent malicious behavior.[81] Lastly, these commentaries did not consider consistent and codified

---

74 Jamil N. Jaffer, *Carrots And Sticks In Cyberspace: Addressing Key Issues In The Cybersecurity Information Sharing Act Of 2015,* 67 S.C. L. REV. 585, 586-87 (2016) (criticizing the Act for lacking incentives for public-private information sharing).

75 Goldsmith, *supra* note 64, at 57.

76 *Id.* at 47-60.

77 Steven M. Bellovin et al., *Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure,* 3 HARV. NAT'L SEC. L.J. 1 (2011).

78 *Id.*

79 *Id.* at 5.

80 *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR EINSTEIN-3 ACCELERATED, NPPD E^3 A 7 (2013) (describing the contract relationships used to implement *Einstein*).

81 *See* Goldsmith, *supra* note 64, at 50; *see also* Manuel Egele et al., *A Survey on Automated Dynamic Malware Analysis Techniques and Tools*, 5 ACM COMPUTING SURVS. 1, 2 (2012) (analyzing automated dynamic analysis).

regulations for cybersecurity support of insider threat operations that exist within the DoD.

C. *Typology: Automation vs. Artificial Intelligence and Machine Learning Methodologies*

Commentary on the pervasive and warrantless monitoring of government cyberspace networks is relevant to the analysis of the legal protections provided by the U.S. Constitution and federal statutes. Different technological methodologies, however, demand separate analyses. The *Department of Defense Instruction 8530.01* and *Department of Defense Directive 8500.01*, requires the DoD to implement technologies in its insider threat program that not only monitor malicious code and signatures, but also monitor user activity.[82] Monitoring user activity is vital to predicting behavioral indicators of insider threats.[83] For this to occur, a monitoring system cannot be purely automated since it must address concerns based on human behavior and human thinking. Although used interchangeably, automation is not the same as AI and machine learning.[84] Automation carries out dictated pre-programed tasks, while AI and machine learning execute complex processes that mimic human thinking through producing and using algorithms to achieve assigned goals in a given environment.[85]

1. Automation

Automation in the context of cyberspace software means software following pre-programmed rules.[86] A platform using an automated program completes tasks by analyzing information under

---

[82] U.S. DEP'T OF DEF., INSTR. 8530.01, CYBERSECURITY ACTIVITIES SUPPORT TO DOD INFORMATION NETWORK OPERATIONS 2-3 (2017); U.S. DEP'T OF DEF., INSTR. 8500.01, CYBERSECURITY 14 (2014); U.S. DEP'T OF DEF., DIR. 5205.16, THE DOD INSIDER THREAT PROGRAM 2 (2014).

[83] *See* Frank L. Greitzer & Ryan E. Hohimer, *Modeling Human Behavior to Anticipate Insider Attacks*, 4 J. STRATEGIC SEC. 25, 43 (2011).

[84] Dave Evans, *So What's the Real Difference Between AI and Automation*, MEDIUM (Sept. 26, 2017), https://medium.com/@daveevansap/so-whats-the-real-difference-between-ai-and-automation-3c8bbf6b8f4b.

[85] *Id.*

[86] *Id.*; Irish Trazaona, *The Difference Between Artificial Intelligence and Automation*, IDEYATECH (May 12, 2017), https://www.ideyatech.com/difference-artificial-intelligence-automation/.

strict rules and providing dictated solutions.[87] It does not innovate, learn, or adjust behavior for new solutions based on its observation and memory.[88] Primary examples of automation include fillable forms or questionnaires used by businesses or employers.[89] These forms automatically prompt a user to type information into a new section depending on previous information provided, but the forms do not learn new information or innovate based on previous responses.[90] Another example of automation software can be found in manufacturing factories where robotics software allows machines to perform tasks like sealing doors or driving nails into an object.[91] These programs only respond with pre-programmed solutions; they do not possess the capability to create new solutions.[92]

The *Einstein* program performs similar basic tasks—it detects and prevents the delivery of certain "signatures" and code "indicators" that are flagged as threats to pre-programmed networks, queues an analyst, or throws the flagged threats into a digital trashcan.[93] Therefore, the legal analyses on predictive, automated programs such as *Einstein* are ill-suited for a program focusing on human behavior and interacting in a dynamic digital environment.

2. Artificial Intelligence

AI is designed to simulate independent human critical-thinking when solving complex tasks in a variety of environments.[94] Multiple official definitions of AI exist, but each definition depends on the approach within a given environment.[95] It is best to think of AI in terms of both the elements that make humans intelligent as well as a

---

87 Evans, *supra* note 84.

88 *Id*.

89 *See* Adam C. Uzialko, *Workplace Automation is Everywhere, and It's Not Just About Robots*, BUS. NEWS DAILY (Feb. 22, 2019, 5:55 PM), https://www.businessnewsdaily.com/9835-automation-tech-workforce.html.

90 *Id*.

91 Evans, *supra* note 84.

92 *Id.*

93 93 U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR EINSTEIN-3 ACCELERATED, NPPD E^3 A 3 (2013).

94 KELLEY M. SAYLER, CONG. RES. SERV., R45178, ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY 3-4 (2019).

95 *Id.* at 2 ("[AI] has a number of unique characteristics that may be important to consider as these technologies enter the national security arena.").

human's achievable goals.[96] AI perceives an environment through inputs, thinks logically about the environment through data storage, acts rationally to achieve goals within the environment through outputs, and learns from those experiences to continually improve performance by using predictive algorithms.[97] This is not to say AI could have perfect intelligence, or that it must reach a level of perfect performance to be an effective platform—indeed, both humans and machines are far from it.[98] However, what is required from AI is the ability to go through a process that mimics human critical thinking based on observations and decisions the agent makes to solve complex problems presented by observables.[99] This assists the agent in choosing the goals to be achieved and the best possible outcome for any given situation.[100] The difference between AI and automation is readily apparent.

It is not enough for AI to think; AI must also be able to use these thought processing elements autonomously. Therefore, for a majority of the time, an AI cannot depend on human supervision and inputs.[101] Although the AI will start with some level of knowledge inputted by

---

96 STUART RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 1-5 (3d ed. 2016) (discussing approaches to develop AI capabilities, ranging from liberal arts to modern scientific disciplines).

97 *See id.* at 1-59 (discussing elements AI must have).

98 *See* NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES 14-21, (2014). The author explores historical examples and predictions about the computational power and application of AI. *Id.* at 13. Until now, most of the focus on AI development has been on Narrow AI, that AI which is used to accomplish defined goals; playing chess, image recognition, online search engines, etc. *Id.* at 14. The next frontier may entail developing AI agents that exercise general intelligence, as General AI. *Id.* at 3-4. These agents contain a level of intelligence across multiple domains used in aggregate. *Id.* at 14.

99 *Id.* at 26; *see also* MAX TEGMARK, LIFE 3.0: BEING HUMAN IN THE AGE OF ARTIFICIAL INTELLIGENCE 49-51 (2017). This definition is limited to expected results from implementing AI and is not concerned with metaphysical concepts such as subjective consciousness of AI agents.

100 *See* RUSSELL & NORVIG, *supra* note 96, at 34-37 (explaining that percept sequences contain everything an agent has ever perceived, which influence its future choices of action). Percepts are perceptual inputs at any given time, and a Percept Sequence is the complete history of everything the agent has ever perceived. *Id.* at 34. I also realize that this sentence may fit within the current debate of humans being "in the loop" of AI decision-making processes, or "on the loop" of AI decision-making processes. The key difference being the level of supervision and veto power over an AI agent's final decision by human supervisors. Further discussion is beyond the scope of this essay. *See, e.g.*, Alan L. Schuller, *At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law*, 8 HARV. NAT'L SEC. L.J. 379, 402-04 (2017).

101 *See* RUSSELL & NORVIG, *supra* note 96, at 39 (explaining that a rational agent learns from what it perceives in addition to its prior programmed knowledge).

its programmer, it must ultimately gain independent knowledge to facilitate the use of outputs.[102]

3. Machine Learning

Autonomy is achieved through learning.[103] Machine learning provides this autonomy to AI when it is able to train itself by using massive data sets and create predictive algorithms that solve problems in complex environments.[104] The AI can then apply the learned data set values to its own experiences—without being explicitly programmed—by using various processes.[105] Such processes include backpropagation, the Hidden Markov Model, and Bayesian model algorithms. Backpropagation assigns value to data by calculating the gradients, the elements needed for to assign data weight, within each piece of the data.[106] Hidden Markov Model algorithms are complex Bayesian models that capture hidden patterns within data for sequential pattern recognition and probability assignment of data that is not directly visible to the AI.[107] Finally, simple Bayesian model algorithms recognize patterns and probability assignment of visible data.[108]

---

102 *See id.* at 39.

103 *Id.*

104 *See* Robert Bruneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 113-114 (2018) (explaining that the use and creation of predictive algorithms constructed through analysis of large datasets that may reveal correlations between various features and desired or objectionable outcomes.).

105 *Id.* at 113-14.

106 *See* BOSTROM, *supra* note 98, at 8. Backpropagation allows the modeling of a given function or task by modifying weights of inputs (information received by an AI for this article's purposes) for output use (observing and understanding an environment). *Id.* It trains multilayered ML neural networks that resemble the human brain. *Id.* These layers work in unison, feeding each other relevant weights to assist in their individual functions. *Id.* Combined with massive pre-programmed data sets and increased computational power, application of these algorithms assists in the creation of AI agents that act humanly in their decision-making capacity. *Id.*

107 *See* Zoubin Ghahramani, *An Introduction to Hidden Markov Models and Bayesian Networks*, 15 INT'L J. OF PATTERN RECOGNITION AND ARTIFICIAL INTELLIGENCE 9, 9-42 (2001). Hidden Markov Models algorithms are a subset of Bayesian models that are ubiquitous, and model ubiquitous patterns within time series data. *Id.* at 9. The model works by distributing probabilities over observations made in sequence, predicting future occurrences in a time sequence. *Id.* at 10. The requirements for this model are that an observed data's state be hidden within the environment, and such observed data's state occurs independently of other observed states of data. *Id.* at 10-11. Basically, "the state at some time encapsulates all we need to know about the history of the process" to make predictions about future occurrences. *Id.* at 11.

108 *Id.* at 12*; see also* BOSTROM, *supra* note 98, at 9. Bayesian models represent "conditional independencies between a set of random variables," implying relationships amongst each

Thus, new inputs attained by AI through using its own observations are included in an internal memory database, assigned values, and combined with existing values in a cyclical fashion (output).[109] This process assists the AI in the future application of such data because the agent continually improves its ability to achieve assigned goals within a given environment.[110] Machine learning minimizes the simplification and assumptions found in manual programming plagued by human bias.[111]

4. Machine Learning Methodologies and Training AI

Facilitating machine learning requires training.[112] A preferred method for facilitating machine learning—as applied to this discussion—involves unsupervised AI training using a system of sensors that process data.[113] This method enables the perceptual development of normal patterns and the identification of anomalies that deviate from those patterns.[114] This process of learning from data representations is the separating characteristic between basic machine learning and "deep" machine learning.[115] Deep machine learning involves layers of hidden and open neural networks that resemble a human brain, working in combination to solve a problem within an environment.[116] Unsupervised learning does not allow the AI to rely upon a supervi-

---

independent set. Ghahramani, *supra* note 107, at 12. The model factors joint distribution as shown in a graphical manner. *Id.* An optimal Bayesian agent would start with some level of prior inputted knowledge that includes bias from a programmer, allowing to set probabilities for future occurrences it observes. It would then update and reassign probabilities based upon new knowledge gained through its own inputs, shifting all data held into new sets of variables.

109 *See* RUSSELL & NORVIG, *supra* note 96, at 39.

110 *See id.*

111 SHAI SHALEV-SHWARTZ & SHAU BEN-DAVID, UNDERSTANDING MACHINE LEARNING: FROM THEORY TO ALGORITHMS 21 (2014) ("[T]he incorporation of prior knowledge, biasing the learning process, is inevitable for the success of learning algorithms. . .[h]owever, the stronger the prior assumptions are, the less flexible the learning is. . .").

112 *Id.* at 19.

113 *See id.* at 22-23.

114 *See id.*

115 *See* Michel Copeland, *What's the Difference Between Artificial Intelligence, Machine Learning, and Deep Learning?*, NVIDIA (July 29, 2016), https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/. Deep Machine Learning is a process of using neural networks which mimic the human brain by connecting discrete layers of neurons to direct data propagation. *Id.* A value or weight is assigned to the data and is used to achieve a goal for future tasks.

116 *Id.*

sor's experience and expertise.[117] Further, deep machine learning is the process of applying the many variants of learned tasks in an artificial intelligence agent's neural network that allow it to give shifting value to data and probabilities for use in complex pattern recognition and reuse in unknown dynamic environments.[118] By learning through its own experience with limited human intervention, the AI achieves autonomy.[119]

Concerning insider threats, machine learning methods allow an AI to develop natural language processing for threat detection. This is an important technique for analyzing content and syntax in a cyberspace network's correspondence.[120] Natural language processing includes an AI's ability to mine text and topics, recognize normative topic models, make inferences, and learn behavioral cues related to the use and context of written speech.[121] The natural language processing model is currently used in social media studies that weigh personality profiles for behavior and statistical analysis.[122]

The elements of AI and machine learning methods can be combined to develop a common baseline for threat detection of anomalous behavior through written text and word usage within a given environment. Allowing AI to learn independently and act autonomously using machine learning techniques best prepares the AI to act intelligently and rationally when identifying threats within a system. AI and machine learning do not merely rely on pre-programmed data like the *Einstein* program. Instead, they predict and learn what threats exist in an ever-changing environment. They also enable the AI to take appropriate measures to deal with such threats before they occur.

D. *Relevancy of Artificial and Machine Learning Methodology Use for Insider Threat Detection*

A blend of counterintelligence, cybersecurity, and behavioral science are used in the DoD insider threat program's interdisciplinary

---

117 *See* SHALEV-SHWARTZ & BEN-DAVID, *supra* note 111, at 22-23.

118 *See* Osonde A. Osoba & Paul K. Davis, *An Artificial Intelligence/Machine Learning Perspective on Social Simulation: New Data and New Challenges* 6-7 (Rand Corp., Working Paper No. WR1213-DARPA 2018).

119 *Id*. at 6.

120 *See id.* at 7.

121 *Id.* at 7 -8.

122 *Id.* at 8.

approach to cybersecurity issues.[123] As previously mentioned, this level of intrusiveness differs from the past because AI builds profiles to detect threats based on content, word choice, and user actions.[124] Unlike other programs, such as the *Einstein* system, AI and machine learning methods do not merely scan copies of e-mails for malicious code.[125] For an AI agent, its methods for detection are an extremely personal affair. The observables utilized by the AI through the machine learning methodologies are employed within the framework of an intelligence cycle to best detect, prevent, and deter insider threats.[126]

1. The Intelligence Cycle

Insider threat detection involves organized thinking, planning, and execution. An example of this process is found in the cyclical counterintelligence process. The phases of this process include: (1) the planning and direction for information collection; (2) the actual information collection; (3) processing and exploiting collected information; (4) analysis and production of products based upon the information collected; (5) dissemination of such products; and (6) the valuation of information to be collected in light of a product.[127] This cyclical process seeks to turn raw information—information not yet ready to use—into a comprehensible and usable format for its intended recipient.[128] At a minimum, this process helps organizations think clearly when attempting to detect and prevent insider threats.

The planning and direction phase of the cycle is a response to requests by a consumer of intelligence information for intelligence products or information from an agency.[129] The intelligence organization must then plan and execute the remaining steps of the process.[130]

---

123 U.S. DEP'T OF DEF., INST. 8500.01, CYBERSECURITY 33 (2014).

124 *Cf.* Osaba & Davis, *supra* note 118, at 6.

125 *See* Irish Trazona, *The Difference Between Artificial Intelligence and Automation*, IDEYATECH (May 12, 2017), https://www.ideyatech.com/difference-artificial-intelligence-automation/.

126 *See id.*

127 *See* DIR. OF NAT'L INTELLIGENCE, U. S. NAT'L INTELLIGENCE: AN OVERVIEW 11-12 (2011); JOINT CHIEFS OF STAFF, JOINT PUB. 2-0, JOINT INTELLIGENCE IV-1 (2013).

128 DIR. OF NAT'L INTELLIGENCE, U. S. NAT'L INTELLIGENCE: AN OVERVIEW 11 (2011).

129 *Id.*

130 Exec. Order No. 12333, 46 Fed. Reg. 59941, 59943 (1981).

The collection phase gathers raw data and information required by the consumer.[131] The organization uses several methods and techniques to collect intelligence data, including human, geospatial, and open-source intelligence, as well as measurement and signature intelligence and signals intelligence, which includes electronic surveillance and communications intelligence.[132] Each method contains its different techniques and methods differ depending on the choice the intelligence collector makes to achieve a specific collection mission objective.

The analysis and production phase of the cycle seeks to answer the questions and requests posed by the consumer by presenting the collected raw data.[133] This presentation enables an analyst to create a completed product.[134] The analyst may be satisfied with the raw data or develop more tailored requirements for a new collection phase to complete the project.[135] Depending upon certain classifications and analytical products, specific organizations or analysts are granted authority to work on a project.[136]

Dissemination includes the delivery of a final product to the consumer.[137] Products may vary depending on whether the analysis relates to long-term or short-term trends,[138] the type of data requested—such as scientific intelligence or estimations on enemy troop movements—and classification. These differences determine who can see and receive the final product.[139] After dissemination, the product is reviewed by the consumer.[140] If more information is needed, or the consumer makes another request based upon the product received, the cycle begins anew.

---

131 DIR. OF NAT'L INTELLIGENCE, U. S. NAT'L INTELLIGENCE: AN OVERVIEW 11 (2011).

132 *Id.*

133 *Id.* at 12.

134 *Id.*

135 *Id.*

136 JOINT CHIEFS OF STAFF, JOINT PUB. 2-0, JOINT INTELLIGENCE IV-24 (2013).

137 *Id*.

138 *See* DIR. OF NAT'L INTELLIGENCE, U. S. NAT'L INTELLIGENCE: AN OVERVIEW 61 (2011) (describing long-term assessment).

139 *Id*. at 62-63 (explaining that intelligence reports are usually classified due to the potential results of analysis).

140 *Id.* at 12.

2. Technical Aspects of Cybersecurity Support of Insider Threat Detection and Prevention

The intelligence cycle process detects and prevents insider threats by monitoring DoD networks for information and is supported by cyberspace defense operations and behavioral science.[141] This process of searching for threats and defending against them within the network is a blend of "Department of Defense Information Network Operations" (DODIN) and "Defensive Cyberspace Operations" (DCO)—otherwise known as "Defensive Cyber Operations-Internal Defense Measures" when conducted only within the DoD network—as a means to detect and prevent insider threats.[142] It is important to recall that the insider threat program is not a DCO or a DODIN operation, but focuses on human threats while using cybersecurity as support. These operations act to defend, secure, and sustain DoD cyberspace, as well as preserve the confidentiality and integrity of the networks, including the information maintained on the network through cybersecurity methodologies and profiling of human behavior.[143] Through continuous monitoring, the intelligence cycle process accomplishes these tasks by identifying, locating, and preventing insider threats from doing serious harm to cyberspace networks before they occur.

Many techniques are used to detect and prevent insider threats. For example, behavioral science techniques, which use psychological profiling and structural anomaly detection to observe behavior, semantic written text, and the syntax of a system's users are often utilized.[144] Using deep machine learning, an AI identifies malicious intent by analyzing the actions of a user, comparing the user to previously programmed profiles the AI built, observing, and ultimately

---

141 JOINT CHIEFS OF STAFF, JOINT PUB. 3-12 GL-4, CYBERSPACE OPERATIONS II-2-II-4 (2018).

142 *Id.* at II-2; JOINT CHIEFS OF STAFF, JOINT PUB. 6-0, JOINT COMMUNICATIONS SYSTEM II-2 (2015).

143 *See* JOINT CHIEFS OF STAFF, JOINT PUB. 3-12 GL-4, CYBERSPACE OPERATIONS II-2 (2018).

144 Oliver Brdiczka et al., *Proactive Insider Threat Detection through Graph Learning and Psychological Context*, 2012 IEEC SYMP. ON SEC. & PRIVACY 142 (2012). These studies are not new, linguistic inquiry and behavioral profile analysis has occurred since the early 20th Century. *See* Yla R. Tausczik & James W. Pennebaker, *The Psychological Meaning of Words: LIWC and Computerized Text Analysis Methods,* 29 J. OF LANGUAGE & SOC. PSYCHOL. 24, 25 (2010) (detailing the history of computerized text psychological analysis).

classifying threat indicators.[145] This method seeks to detect threats before they come to fruition and cause severe damage to a network, or physically extend beyond the cyberspace network.[146]

In this context, AI uses machine learning to analyze large-scale data over an extended period of time.[147] This allows the AI to discern what normative behavior within the network looks like by defining patterns between groups and classes of users, as well as individual users.[148] The AI then extracts this information and compares the suspicious actions against daily network use while looking for anomalies deviating from normal individual and group patterns of behavior.[149] The AI then ranks anomalies based upon psychological profiles—using text content, semantic, and syntax analysis—and then queues an analyst for further examination.[150] Because the of the AI's ability to learn using machine learning methodology, it can modify its analysis of normative and anomalous behavior as the environment continually shifts.[151]

Other methods use techniques like decoy documents, "watering holes,"—planted malware on frequently visited webpages that lure an individual based on her behavior—and beacons to monitor specific users once they have begun acting maliciously against a network.[152] This adds another defensive layer against insider threats once a user's behavior has deviated from norms established by the AI's precepts. By the time the user has chosen to take malicious action against the network or organization, the AI has built a profile and provided the user with a tailored decoy to attack, which helps the queued analysis

---

145 Brdiczka et al., *supra* note 144, at 144.

146 *Id.* at 142.

147 *Id.* at 144.

148 *See id.* at 145 (using data from online gaming because it is the most analogous to behaviors of malicious insiders).

149 *Id.*

150 *Id*. at 147-48.

151 Oliver Brdiczka et al., *Proactive Insider Threat Detection through Graph Learning and Psychological Context,* 2012 IEEC SYMP. ON SEC. & PRIVACY 142, 144-45 (2012).

152 Brian M. Bowen et al., *Designing Host and Network Sensors to Mitigate the Insider Threat*, 7 IEEE SEC. & PRIVACY 22, 23-28 (2009); Sumayah Alrwais et al., *Catching Predators at Watering Holes: Finding and Understanding Strategically Comprised Websites,* 2016 ANN. COMPUTER SEC. APPLICATIONS CONF. 153, 154 (2016) (explaining that watering holes are a strategically and carefully planned targeting of individual(s) for a cyber-attack that uses malware planted in frequently visited websites, menus, pages, etc.). Attacks are based on behaviors of victim and seek to attack while they are conducting their normal-course-of-business activities. *Id.* at 153. The attack mimics the familiar scene in the animal kingdom, a 'watering hole,' where animal predators attack prey as they drink from a watering hole unsuspectingly.

have better situational awareness.[153] Although these methods add an attractive opportunity for an insider threat, the original analysis of what constitutes the threat still relies on the structural anomaly detection and psychological profiles built by the AI's precepts.[154]

II. LEGAL LANDSCAPE

The differences in authorities and technology used to monitor a cyberspace network raise questions concerning previous commentary and its applicability to the DoD. The overarching themes of the Fourth Amendment and its progeny are relevant, but the DoD's internal regulations must also be applied to the analysis. First, the *Einstein* program's legal authority was founded on federal cybersecurity initiatives with a focus on combating intrusions of malicious code and threat indicators to government systems.[155] The insider threat program, however, focuses on human actors relying on the Executive Branch power under Article II of the U.S. Constitution and delegated to the DoD to promulgate internal regulation.[156] Cybersecurity is used to support the insider threat program whereas the independent cybersecurity operations of this program are based on separate authorities.[157] Primarily, *Department of Defense Instructions 8500.01* and *8530.01* provide the legal basis for the DoD to conduct these operations, allowing support from advanced technologies such as AI and machine learning methodologies.[158] This authority sets it apart from previous commentary by truly addressing the balance between legitimate government interest and individual privacy rights.

---

153 *See* Bowen et al., *supra* note 152, at 24-25 (describing qualities of good decoys).

154 *Id*. at 28. This practice may present an issue of entrapment if the AI crosses a threshold of inducing an employee or user who would not otherwise had committed an insider threat act. *See* U.S. DEP'T OF JUSTICE, JUSTICE MANUAL: CRIMINAL RESOURCE MANUAL, 645 (2018).

155 MILTON MUELLER & ANDREAS KUHN, EINSTEIN ON THE BREACH: SURVEILLANCE TECHNOLOGY, CYBERSECURITY, AND ORGANIZATIONAL CHANGE 8 (2013).

156 U.S. DEP'T OF DEF., DIR. 5205.16, THE DOD INSIDER THREAT PROGRAM 1 (2017).

157 *Cf. id.*

158 *See* U.S. DEP'T OF DEF., DIR. 8500.01, CYBERSECURITY 1 (2014); U.S. DEP'T OF DEF., DIR. 8530.01 CYBERSECURITY ACTIVITIES SUPPORT TO DOD INFORMATION NETWORK OPERATIONS 1 (2017).

A. *Authority to Conduct Insider Threat Operations*

The President maintains the authority under his Article II powers to collect foreign and domestic intelligence to protect the nation.[159] This rationale, consistently applied by the Judicial Branch, provides that the President's power as Chief Executive and Commander-in-Chief of the military mandates that he ensures the laws are faithfully executed, preserves and protects the Constitution, and expressly and impliedly defends the nation against attacks.[160] These Article II powers are impacted by the domestic and foreign intelligence collection legal regimes enacted by Congress, which play upon the separation of powers and tripartite governance concepts.[161] Although such legislation serves to limit Executive Branch intelligence collection, the President maintains authority under the Constitution to ensure national security and can utilize foreign intelligence collection to do so. He further delegates this power of intelligence collection down a chain-of-command established by statutes, specific orders, and regulations, to which Congress has acquiesced in practice.[162]

Domestic insider threat detection authority is delegated from the President to his principal advisors for the defense of the nation and intelligence operations—the Secretary of Defense and the Under Secretary of Defense for Intelligence.[163] The Secretary of Defense and his Under Secretary of Defense for Intelligence implement Executive Branch priorities through internal regulations that carry the force of statutory law for DoD employees.[164] The insider threat program is

---

159 *See* Deborah Pearlstein, *Before Privacy, Power: The Structural Constitution and the Challenge of Mass Surveillance*, 9 J. NAT'L SEC. L. & POL'Y 159, 176-79 (2017) (describing the legal support of the President's power to gather intelligence).

160 *Id.* at 175-176 (citing to several cases concerning the President's power as Commander-in-Chief).

161 *See id.* at 179 ("Indeed, as OLC later put it, the President's Power thus included 'all the discretion traditionally available to any sovereign in its external relations, except insofar as the Constitution places that discretion in another branch of government.'").

162 *See* 10 U.S.C. § 113(b) (2018) (establishing the Secretary of Defense as the President's principal assistant in all matters related to defense); 10 U.S.C § 137(b) (establishing the Under Secretary of Defense's role in national security); Dames & Moore v. Regan, 453 U.S. 654, 670 (1981) (describing the classifications of presidential executive actions as discussed in Justice Jackson's concurrence in Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring)).

163 Exec. Order 12333, 46 Fed. Reg. 59941, 59943 (1981).

164 *See* Chrysler Corp. v. Brown, 441 U.S. 281, 295-296 (1979) ("It has been established in a variety of contexts that properly promulgated, substantive agency regulations have the 'force and effect of law.'").

authorized by *Department of Defense Directive 5205.16*.[165] This directive allows DoD agencies to conduct a variety of activities within their networks to identify and prevent insider threats.[166] The directive provides:

> Through an integrated capability to monitor and audit information for insider threat detection and mitigation, the DoD . . . will gather, integrate, review, assess, and respond to information derived from [CI], security, *cybersecurity* . . . monitoring of user's activity on [DoD] information networks . . . to identify, mitigate, and counter insider threats.[167]

This directive allows DoD intelligence agencies to utilize a multidisciplinary approach by conducting insider threat prevention operations through a variety of techniques, tools, and methods.[168] Although this multidisciplinary approach is subject to several caveats, *Department of Defense Instructions 8500.01* and *8530.01* still allow cybersecurity support for insider threat operations focused on human actors.[169] The insider threat directive notes a number of references governing information collection and monitoring, many of which overlap. Notably, there are distinctions between what are considered permissible collections on U.S. persons, foreign persons, and employees and non-employees within the cyberspace network, as well as directives dictating the storage of such personal identifiable information and the dissemination of such information.[170] Because of these differences, the DoD must adhere to these practice methods and requirements on collection, storage, and dissemination during insider threat monitoring operations.[171]

---

165 U.S. DEP'T OF DEF., DIR. 5205.16, THE DOD INSIDER THREAT PROGRAM 1-3 (2017).

166 *Id.* at 1-2.

167 *Id.* at 2 (emphasis added).

168 *See* U.S. DEP'T OF DEF., DIR. 8500.01, CYBERSECURITY 33 (2014).

169 *Id.* at 34 ("Cybersecurity will be used *in support of* countering espionage, international terrorism, and the *[CI] insider threat*[.]") (emphasis added).

170 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 8-9 (2016); U.S. DEP'T OF DEF., DIR. 8500.01, CYBERSECURITY 3 (2014).

171 *See* U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 18, 20-23 (2016); U.S. DEP'T OF DEF., INSTR. 5240.26, COUNTERING ESPIONAGE, INTERNATIONAL TERRORISM, AND THE COUNTERINTELLIGENCE (CI) INSIDER THREAT 6-8 (2018).

B. *Department of Defense Intelligence Collection Manual Provides Guidance for Insider Threat Operations*

Two key sources for these varying standards and collection limitations are the *Department of Defense Instruction 5240.26* and the previously referenced Intelligence Collection Manual.[172] These two public regulations establish the responsibilities and procedures enabling the insider threat monitoring of people by purely cyberspace actors.[173] The former requires programs to detect anomalies and insider threat indicators within the network and share information on these anomalies with other DoD intelligence components.[174] The latter requires procedures for monitoring and information collection on cyberspace system users because of insider threat program intelligence gathering aspects.[175] Although required for intelligence agencies, DoD non-intelligence agencies follow both procedures to ensure constitutional and statutory compliance for insider threat detection and prevention.

1. Information Collection of U.S. Persons

Most DoD employees and users monitored on a DoD cyberspace network are U.S. persons[176] for the purposes of analysis under the Manual.[177] Consequently, insider threat collection is mainly concerned with the interplay of government interests and privacy rights associated with this class of individuals. Procedural collections on U.S. persons are found in Section 3 of the Manual, which provides for the intentional and incidental collection of information concerning U.S. persons, as well as its limitations and exceptions.[178] This section also notes a classified annex applicable in specific circumstances where normal authorities may not apply.[179]

---

172 *See* U.S. DEP'T OF DEF., INSTR. 5240.26, COUNTERING ESPIONAGE, INTERNATIONAL TERRORISM, AND THE COUNTERINTELLIGENCE (CI) INSIDER THREAT 10-11 (2018).

173 *Id.*

174 *Id.* at 10.

175 *See* U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 10-20 (2016).

176 *Id*. at 54.

177 *See* Citizenship 5 C.F.R. § 7.3 (2018) (defining who can take the civil service exam); Exec. Order 11935 (1976), as amended.

178 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 10-15 (2016).

179 *Id.*

Intentional collection of U.S. person information (USPI) occurs when an intelligence agency deliberately seeks to collect information concerning such persons.[180] Intentional collection on U.S. persons is permissible *only if* the information sought is reasonably believed to be necessary for the performance of an authorized intelligence mission or function assigned to the agency, *and* if the U.S. person information falls within one of the thirteen categories defined in the Manual.[181] This two-prong test is essential to determine if it is permissible to intentionally seek information concerning U.S. persons. Information is reasonably believed to be necessary for the performance of an authorized intelligence mission or function if "the facts and circumstances are such that a reasonable person would hold the belief."[182] The Manual provides that the facts and circumstances involved must rest on the ability to be articulated, and that "hunches or intuitions are not sufficient" for collection.[183] However, "a reasonable belief can be based on experience, training, and knowledge of foreign intelligence or [counterintelligence] activities as applied to particular facts and circumstances," even when it is apparent that someone unfamiliar with such activities may not hold the same belief based on the facts and circumstances.[184] This ensures collection efforts are not conducted on a purely subjective basis, but are instead based on an objectively reasonable standard. Any hypothetical offered in this Article assumes that the referenced organization is an intelligence agency acting pursuant to its mission.

Thirteen categories exist for intentional collection of USPI. However, the following are the most relevant here: (1) consent of the U.S. person; (2) counterintelligence activities against a U.S. person; and (3) incidental collection on USPI.[185] Consent occurs when there is an agreement by a person to permit the agency to take particular

---

180 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 50 (2016).

181 *Id.* at 11 (emphasis added).

182 *Id.* at 53.

183 *Id.*

184 *Id.*

185 *Id.* at 11-13. The other eleven categories are: publicly available information; foreign intelligence information; threats to safety information; protection of intelligence sources, methods, and activities; current, former, or potential sources of assistance to intelligence activities information; persons in contact with sources or potential sources' information; personnel security; physical security; communications security investigation information; overhead and airborne reconnaissance information; and administrative purposes.

actions affecting such person.[186] Consent can be given in written, electronic, or oral form unless a specific form of consent is legally required.[187] The consent may be explicit or, alternatively, implied if adequate information is provided that the U.S. person carried a presumption of consent accompanying his actions, or if an adequate policy was published or otherwise articulated.[188] As insurance for the agency, the agency's general counsel or legal advisor determines whether adequate consent was given under this standard.[189]

Counterintelligence activities constitute those actions taken as part of the DoD insider threat program, even though the "threat" so happens to be a U.S. person.[190] Counterintelligence includes information gathering activities conducted to "identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or their agents, or terrorist organizations or activities."[191] Intelligence information gathering activities are those conducted by DoD organizations pursuant to *Executive Order 12333*, which includes the National Security Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and military service component intelligence agencies.[192] If there is a nexus between the insider threat and foreign powers or terrorist organizations, AI may be employed against a U.S. person to collect USPI under the justification that it is a counterintelligence operation.[193] This is important because some insider threats operate on behalf of a foreign adversary, its interest, and its goals.[194]

---

186 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 46 (2016).

187 *Id.*

188 *Id.*

189 *Id.*

190 *See* U.S. DEP'T OF DEF., DIR. 5250.16, THE DOD INSIDER THREAT PROGRAM 16 (2016); U.S. DEP'T OF DEF., DIR. 5240.02, COUNTERINTELLIGENCE 1-2 (2015); U.S. DEP'T OF DEF., DIR. 5240.02, COUNTERINTELLIGENCE 11-12 (2015) (defining "counterintelligence" to include any information gathered on any activities against the United States without an exception for U.S. citizens).

191 U.S. DEP'T OF DEF., DIR. 5240.02, COUNTERINTELLIGENCE 11-12 (2015).

192 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 5 (2016).

193 *Id.* at 11.

194 *Id.* (allowing intentional collection of USPI when the information sought is reasonably believed to constitute foreign intelligence from a U.S. person believed to be working on behalf of a foreign power).

Incidental collection is also allowed.[195] Incidental collection involves USPI not deliberately sought by an agency but nonetheless collected.[196] Such circumstances can easily occur in the context of the DoD's insider threat detection and prevention program. For example, an AI detects an anomaly from a network user it is monitoring. Upon discovering further information relating to the location and identification of the anomaly, the user is now known as a U.S. person. The AI would not have intentionally targeted the U.S. person for collection; however, because the situation involves a U.S. person, it is ancillary to the purpose of the detection.[197]

Thus, if both prongs of the test are met regarding the necessity to an agency's mission, performance, or function, and it falls within one of the thirteen categories intentional collection of information concerning U.S. persons may be permissible.[198] Although no specific targeting of individuals occurs for insider threat detection until behavior is queued, algorithmic monitoring could collect information on U.S. persons. These actions subject insider threat monitoring by AI to this regulation's provisions.[199]

2. Electronic Surveillance and Collection

Insider threat operations using AI and machine learning methods within a cyberspace network under DCO and DODIN operations are categorized as "electronic surveillance" operations procedures.[200] These operations are not cybersecurity operations per se, but rather operations using cybersecurity as a means to prevent insider threats.[201] This is because insider threats require a specific type of surveillance and collection operation focused on the underlying human activity, as opposed to surveillance that seeks to defeat malicious cyber access and payloads in a cybersecurity context.[202]

---

195 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 13-14 (2016).

196 *Id.* at 15-16.

197 *Id.*

198 *Id.* at 11-13.

199 U.S. DEP'T OF DEF., DIR. 5205.16, THE INSIDER THREAT PROGRAM 2 (2014).

200 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 48 (2016).

201 U.S. DEP'T OF DEF., INST. 8500.01, CYBERSECURITY 34 (2014).

202 *Compare id.* at 55 (defining "cybersecurity"), *with* U.S. DEP'T OF DEF., INST. 5240.26, COUNTERING ESPIONAGE, INTERNATIONAL TERRORISM, AND THE COUNTERINTELLIGENCE INSIDER THREAT 12 (2018) (defining "insider threat").

In the Manual, electronic surveillance hinges on whether non-public information is surveilled and collected using electronic means. AI operates using algorithms and collects information within a network that relies on electronic representations and architecture.[203] Furthermore, collection occurs when information is received by a defense intelligence component.[204] In practice, it is not difficult to meet this definition. If an exception exists, however, the surveillance would not be subject to the definition of collection.[205] The difficulty lies in the specifics of the method used and the person surveilled during an insider threat operation.

Electronic surveillance must have an authorized, restricted purpose and use the least intrusive means available.[206] This method must also adhere to the limitations on collection of foreign intelligence within the U.S.[207] Under the Manual, a "restriction on purpose" means that the information may not be collected *solely* for purposes of monitoring protected speech under the First Amendment of the Constitution, or the lawful exercise of other rights provided in the Constitution and laws of the U.S.[208] Thus, an agency may not collect information that AI or machine learning mistakes as anomalous if the behavior merely involves the exercise of a permissible constitutional right. This could include, for example, a military member or DoD civilian employee viewing a political candidate's campaign website or an information page about a particular religion.[209] However, such an action could still be included as part of a larger holistic detection and surveillance method.[210]

Collection using "the least intrusive means" first looks to publicly available information or information a person has consented to share.[211] The agency then looks to cooperating sources, which include

---

203 Burgess, *supra* note 32.

204 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 45 (2016).

205 *Id.*

206 *Id.* at 14.

207 *Id.*

208 *Id.*

209 *See* 5 U.S.C. § 7323 (1993) (authorizing a federal employee to take part in political campaigns).

210 U.S. DEP'T OF DEF., NO. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 9 (2016) (explaining that intelligence collection will not be used to affect the United States' political process).

211 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 14 (2016).

"government agencies, law enforcement authorities, credit agencies, commercial entities, academic institutions, employers, and foreign governments."[212] Next, the agency uses techniques that do not require a judicial warrant or the approval of the U.S. Attorney General.[213] This provision is especially aimed at the processes required by FISA[214] and for criminal investigations.[215] Furthermore, the General Counsel of the DoD may approve collection techniques requiring a judicial warrant or approval from the U.S. Attorney General.[216] Lastly, in collecting non-publicly available USPI, an agency should collect no more than is reasonably necessary to complete its mission.[217]

A final limitation of USPI collection involves foreign intelligence collection within the U.S.[218] An agency may collect foreign intelligence concerning U.S. persons in the U.S. if the information is publicly available.[219] Furthermore, collection may occur if: (1) the DoD intelligence component seeks information where the foreign intelligence aspect is significant and collection is not undertaken for the purpose of acquiring information about any U.S. person's domestic activities; (2) the information cannot be reasonably obtained from publicly available information or from sources who are advised or otherwise aware that they are providing information to a DoD intelligence component; or (3) the head of the DoD intelligence component has approved a technique not fitting into the aforementioned categories.[220] This limitation is strictly applicable to the FISA legal regime on foreign intelligence collections.[221]

Although not the focus of this Article, retention and dissemination of USPI collected under these DoD regulations are provided for in relevant regulatory provisions.[222] The salient point of these provi-

---

212 *Id.* at 46.

213 *Id.*

214 *Id.* at 10.

215 *Id.* at 23.

216 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 14 (2016).

217 *Id*. at 14.

218 *Id.*

219 *Id.*

220 *Id.* at 15.

221 *Id.* ("Only paragraphs 3.2.f. and 3.2.g. apply to the acquisition of information in accordance with Chapter 36 of Title 50, U.S.C., also known and referred to in this issuance as the "Foreign Intelligence Surveillance Act [FISA)]).").

222 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 15 (2016).

sions depends upon the information collected and queries conducted to find information in a retention system, as well as the enhanced safeguards, time-frames, and methods that must be used to avoid infringing on constitutional protections.[223]

Even when collection is permissible, analysis must be done within existing DoD authorities to ensure collection of USPI adheres to its purpose concerning a DoD intelligence agency's mission. Here, intelligence practices use AI to detect insider threats. The procedures and limitations imposed on the collection of USPI exist to minimize the impact on constitutional protections and individual privacy rights in light of the DoD's need to execute its mission of detecting, deterring, and preventing insider threats.[224]

3. Electronic Surveillance Collection of U.S. Person Information

Because of the nature of a network's cyberspace environment, electronic surveillance methods are preferred for monitoring, detecting, and preventing insider threats within a cyber network. Electronic surveillance is permissible for insider threat purposes targeting USPI within specific legal frameworks dependent upon an intelligence component's mission, the location of the U.S. person, the methods used to conduct the electronic surveillance, and the type of communication sought.[225] These considerations are complex and subject to change when dealing with AI and machine learning methodologies.

The limitations posed on information collection consist of the legal regimes in the Manual, as well as some authorities not provided by the Manual, such as *Executive Order 12333* and FISA.[226] The Manual also contains provisions for retaining foreign surveillance information, such as those under the Wiretap Act, as well as general Fourth Amendment principles.[227] Although collection depends on a variety of considerations, limitations grounded in specific, legal regimes must be consulted before monitoring begins. Given the unique nature of

---

223 *See id.* at 15-16.

224 *See id.* at 14 ("A Defense Intelligence Component may not collect USPI solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States.").

225 *Id.* at 23.

226 *Id.* (explaining the legal authorities governing electronic surveillance).

227 *Id.*

insider threat detection operations, a crucial focal point is the application of legal regimes to USPI within a DoD network that are holistically monitored.

III. ANALYSIS

What happens when a U.S. citizen-employee of the DoD begins to show signs of being an insider threat to her organization? She begins to visit questionable websites, writes extremely angry emails to her colleagues, and repeatedly attempts to access files she does not have permission to access. There is concern she may resort to violence or use some form of cyber manipulation to achieve a malicious purpose. The organization's AI platform, using machine learning, picks-up on this behavior and cues a supervisor to alert authorities. She is later found attempting to plug a USB drive into a colleague's computer. Furthermore, consider that she is a U.S. citizen, she was using a government computer on a government network, and she was at her organization's place of business.

A. *Hypothetical: DoD Employee Asserts Her Fourth Amendment Rights Were Violated by the AI When It Identified Her Behavior Using Machine Learning Methodologies*

Insider threat detection operations conducted by the DoD must adhere to the Fourth Amendment when conducting electronic surveillance of U.S. persons.[228] Thus, a traditional Fourth Amendment analysis is required. The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."[229] The general framework for a Fourth Amendment analysis poses a series of questions that consider a variety of factors including whether a "search" has occurred, whether a government agent was involved in a search activity, the existence of a warrant based upon probable cause and issued by a neutral magistrate, the reasonableness of the search, the applicability of any exception to the general requirements, and

---

228 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 23 (2016) ("All electronic surveillance must comply with the Fourth Amendment to the Constitution.").

229 U.S. CONST. amend. IV.

whether the search may be nonetheless reasonable based upon the totality of the circumstances.[230] A determination may rise or fall on any one of these factors. In this hypothetical, the DoD did not violate the employee's Fourth Amendment rights by using AI and machine learning methodology, because its monitoring was reasonable and it complied with the Manual.

1. Search

The factor of whether a government agent is involved in the search is met here, because AI is an instrument of the U.S. government. A search occurs when the DoD's AI infringes upon the property interest of an employee and that employee has an objectively recognizable subjective expectation of privacy. Such objectively recognizable expectations of privacy generally have "a source outside the Fourth Amendment, either by reference to concepts of real property or personal property law or to understandings that are recognized and permitted by society."[231] This framework was modified in *United States v. Jones*, where the Supreme Court resurrected the originalist approach of property interest as a foundation of Fourth Amendment analysis.[232] Under this traditional approach, if the government invades a person's property without a warrant, it violates that person's constitutional rights.[233] If the person does not have a property interest, then under the *Jones* approach courts must look at the person's expectation of privacy and whether society recognizes it as reasonable.[234] Reasonableness is judged on a case-by-case basis and courts ensure fairness by weighing the individual's expectation of privacy and

---

230 JEFF KOSSEFF, CYBERSECURITY LAW 261 (2017).

231 Minnesota v. Carter, 525 U.S. 83, 88 (1998) (quoting Rakas v. Illinois, 439 U.S. 128, 143-44 (1978).

232 United States v. Jones, 565 U.S. 400, 405 (2012).

233 *Id.* at 409-12; *see also* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that the Fourth Amendment is not violated unless there was an official search and seizure of a person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house or curtilage for the purpose of making a seizure).

234 Carpenter v. United States, 138 S. Ct. 2206, 2213 (quoting Soldal v. Cook Cty., 506 U.S. 56, 64 (1992) ("[T]he Court has recognized that 'property rights are not the sole measure of Fourth Amendment violations.'); *Jones*, 565 U.S. at 406-412; Katz v. United States, 389 U.S. 347, 588 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual [subjective] expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

the search's level of intrusiveness.[235] The principle that the Constitution protects both people and their property includes over fifty years of jurisprudential precedent.[236] The multi-prong test the *Jones* court created helps ensure that an individual's constitutional privacy rights are reasonably safeguarded.

The first prong of the *Jones* test is not met in this case, because employees do not have property interest in government resources or assets and the employee used a government-owned computer and network. The employee was aware of this through the employer's policy.[237] Additionally, employees do not maintain an expectation of privacy concerning metadata. Employees share metadata with the government under the third-party doctrine. The third-party doctrine states that if an individual voluntarily shares information with a third party, then the individual does not have a reasonable expectation of privacy concerning the shared information. This includes any information shared by government employees via their acknowledgement and acceptance of government monitoring on work computers before they log-in.[238] Although there have been recent developments that challenge this notion of "third-party metadata" due to its questionable application to modern technology, such challenges have been limited

---

235 Sarah Fowler, *Circumventing the Constitution for National Security: An Analysis of the Evolution of the Foreign Intelligence Exception to the Fourth Amendment's Warrant Requirement*, 4 U. MIAMI NAT'L SEC. & ARMED CONFLICT L. REV. 208, 213 (2014) (quoting Harris v. United States, 331 U.S. 145, 150 (1947)) ("[E]ach case is decided on its own facts and circumstances").

236 *See* ANTHONY GREGORY, AMERICAN SURVEILLANCE: INTELLIGENCE, PRIVACY, AND THE FOURTH AMENDMENT 124-47 (2016) (surveying the history of Fourth Amendment jurisprudence from the founding of the Constitution to the present).

237 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 5 (2009).

238 *Carpenter*, 138 S. Ct. at 2216 ("[T]he Government is typically free to obtain [information given to a third party] from the recipient without triggering Fourth Amendment protections"); *see also* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing information. . . . [E]-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers" (citing Smith v. Maryland, 442 U.S. 735, 742-44 (1979)); Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 7 (2009).

to narrow circumstances.[239] Under current principles, an employee has no reasonable expectation of privacy in metadata. The employee acquiesced to its reception and use by another party, exemplified here by the DoD.

Employees do maintain a level of privacy expectation, however, in the content of their correspondence.[240] This expectation may be challenged and overcome, especially in workplace environments where the operational culture and policies indicate that employees and users will be monitored, or where assets and networks do not belong to the employee.[241] The test turns upon whether the employee has an objectively reasonable expectation of privacy in her email content as determined by operational reality, actual practices, procedures, and legitimate regulation of the office.[242] No unconstitutional search occurs if the employee is put on notice by the employer's policies and practices regarding monitoring programs and the general lack of privacy she has in the government's assets and networks.[243]

There is no reasonable expectation of privacy under the Fourth Amendment for DoD employees due to the specifics of the insider threat program, which involves annual training and daily consent by employees to be monitored on a government network, as well as the initial alert in the terms of employment.[244] By consenting to use the network, attending classes and trainings about insider threat detection and prevention, and voluntarily disclosing information to other government officials in the workplace—work related or otherwise—the employee disclaimed protection concerning information for which she

---

239 *Carpenter*, 138 S. Ct. 2206, 2219 (2018) (holding that the government's acquisition of a person's cell-site records without a warrant was a violation of the Fourth Amendment).

240 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. ___, 8 (2009).

241 *Id.* at 9 (quoting United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000)) ("[O]ffice practices, procedures, or regulations may reduce legitimate privacy expectations.").

242 *Id.* (quoting O'Conner v. Ortega, 480 U.S. 709, 717 (1987)) ("[W]hether, in a particular circumstance, a government employee has a legitimate expectation of privacy in his use of governmental property at work is determined by 'the operational realities of the workplace and by virtue of actual office practices and procedures, or by legitimate regulation.'").

243 *Id. cf.*, Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 904-905 (9th Cir. 2008) (explaining that public employer intrusions for non-investigatory, work-related purposes are evaluated under the reasonableness of all the circumstances), *rev'd on other grounds*, 529 F.3d 892 (9th Cir. 2008).

244 *See* U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 12 (2016) (stating that Department of Defense employees are subject to intentional collection of information).

may have otherwise had an expectation of privacy. Under the current legal regime, her voluntary disclosure of information and her consent to be monitored allows the DoD to collect this information without violating the employee's Fourth Amendment rights.[245]

This same approach also applies to monitoring non-employees who send correspondence to employees using a DoD network. Non-employees also voluntarily give their metadata and content to a third-party—the employee—who has consented to monitoring, leaving no reasonable expectation that the correspondence will remain private.[246] The analysis ends at this point, because under the third-party doctrine and Section 3 of the Manual, the Fourth Amendment has not been violated.[247]

2. Voluntary Consent and Administrative Investigations as Special Needs

a. *Consent*

Consider now that the employee asserts she never understood the terms of consent and did not attend the yearly training. She states her supervisor told her not to worry about the training, as her organization's operational tempo means she is too busy to attend.

The DoD's monitoring and collection would still be reasonable under these circumstances. The employee still consented per the Manual, and the insider threat program constitutes a special need of the government outside of a non-criminal investigatory purpose.[248] Although courts usually consider searches without a warrant unrea-

---

245 *See* U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 13 (2016) (discussing voluntary disclosure).

246 *See* Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 12 (2009) ("We believe [the third-party doctrine] applies to a person e-mailing an Executive Branch employee at the employee's personal e-mail account, where the employee has agreed to permit the Government to monitor, intercept, and search all of his Internet communications and data transiting Government-owned information systems.").

247 *See* U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 8-44 (2016).

248 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 16-17 (2009) (concluding that Einstein 2.0 is reasonable because it serves a special governmental need beyond the normal need for law enforcement).

sonable, a warrant is not always necessary.[249] Rather, the level of reasonableness of a search is the crucial point.[250] If governmental actions through AI monitoring and collection qualify under the exception standards, then the actions are reasonable.[251] Thus, there is no Fourth Amendment violation.

Consent is a settled exception to the warrant requirement under Supreme Court precedent.[252] Section 3 of the Manual also allows for monitoring based on consent.[253] However, consent alone is not enough—it must be voluntary and not based on duress or coercion.[254] DoD employees and users of a DoD network agree to the network's terms and conditions before logging-in.[255] The terms and conditions include a notification about monitoring.[256] Additionally, under DoD policy, consent can be implied through adequate notice.[257] In the context of this hypothetical, consent may be tricky. If the employee does not understand the terms of use and does not attend annual training for the insider threat program, she may suffer employment consequences because of an inability to perform her official duties.[258] These consequences create a situation where consent given by the employee is unreasonably coercive or made under duress and could be considered questionable concerning its legal sufficiency.[259]

---

249 U.S. CONST. amend. IV; Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) ("Although the 'ultimate measure of the constitutionality of a governmental search is 'reasonableness,' our cases establish that warrantless searches are typically unreasonable where 'a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing.'").

250 Maryland v. King, 569 U.S. 435, 447 (2013) ("As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is reasonableness.").

251 *Carpenter*, 138 S. Ct. at 2221 ("[A] search is reasonable only if it falls within a specific exception to the warrant requirement.") (internal citations omitted).

252 Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

253 *See* U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 8-44 (2016).

254 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch, 33 Op. O.L.C. __, 15 (2009).

255 *Id.* at 5.

256 *Id.*

257 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 46 (2016).

258 U.S. DEP'T OF DEF., DIR. 5205.16, THE DOD INSIDER THREAT PROGRAM (2016) (requiring annual mandatory insider threat training and consent for network login).

259 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 15 (2009).

First, under the insider threat program, the employee consented to AI monitoring her activity and behaviors to detect threats on the network and to the organization. However, the AI does not specifically target any individual employee.[260] Any specific monitoring or investigation that results from monitoring is ancillary to the employee's original consent to gain access to the network. Therefore, the AI only focuses on the employee's actions once those actions deviate dangerously from normative behavioral patterns and profiles, and are screened via machine learning algorithms.[261] By building insider threat detection and prevention on this basis into the DoD's regulatory regime, the employee's consent is reasonable.[262]

Second, consent may be implied by logging into the network and accepting the DoD's established terms and conditions. The Manual provides that "[c]onsent may be implied if adequate notice is provided that a particular action carries with it the presumption of consent to an accompanying action," or "where adequate policy has been published or otherwise articulated."[263] The notice provided before the employee logs into the network allows the employee to accept the terms and conditions of use.[264] When the employee accepts, the organization can actively monitor the employee's use of the network. The general awareness of the program via published order and annual training are adequate to infer the employee is aware of the program and its requirements. In this scenario, the employee's admission that she knew she must attend the training also infers the employee is aware of the program. Objectively, the employee understood that monitoring could occur.

b. *Administrative Exception and Special Needs of the Government*

Using AI and machine learning methodologies to monitor employee behavior on a network to screen for insider threats also

---

260 *Id.*

261 *See* Cliff Kuang, *Can A.I. Be Taught to Explain Itself?*, N.Y. TIMES MAG. (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html.

262 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 11 (2016).

263 *Id.* at 46.

264 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 14-15 (2009).

qualifies as an administrative-programmatic exception to the Fourth Amendment. This administrative exception focuses on the "special needs" of the government beyond law enforcement and allows the government to monitor legitimate work-related intrusions when otherwise the Fourth Amendment would normally apply.[265] This non-investigatory purpose is judged on a reasonable basis standard for both the absence of a warrant and the "reasonableness of the search."[266]

A warrantless administrative search may be reasonable if the public interest is such that neither a warrant nor probable cause is required, or if an individual is *already on notice* because of their employment where some level of intrusion is expected.[267] This is especially true when a warrant would not limit the discretion of the government or the user being monitored on the network.[268] Scrutiny of the reasonableness of a search is determined by balancing the legitimate governmental interests against the degree the search intrudes upon an individual's privacy.[269] This balance is related to the circumstances that caused the search in the first place.[270]

First, *Department of Defense Directive 5205.16* and the Manual establish and implement this administrative exception through its insider threat program. The program is not used for purposes of criminal investigation, but as a counterintelligence action to protect its networks, information concerning the networks, and people within its organization.[271] This program's core objective is to "prevent, deter, detect, and mitigate the threats insiders may pose to . . . installations, facilities, personnel, missions, and resources."[272] This official policy and authorization is outside the scope of ordinary criminal law

---

265 Maryland v. King, 569 U.S. 435, 447 (2013); *see also In re* Directives Pursuant to § 105(b) of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008) (holding that there is a special needs exception to the warrant requirement for certain types of surveillance-related searches).

266 *King*, 569 U.S. at 447-48 ("[T]he ultimate measure of the constitutionality of a governmental search is 'reasonableness.'"); *In re* Directives Pursuant to § 105(b) of the Foreign Intelligence Surveillance Act, 551 F.3d at 1011.

267 *King*, 569 U.S. at 447.

268 *Id.*

269 *Id.*

270 *Id.* at 448.

271 U.S. DEP'T OF DEF., DIR. 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 11 (2016); U.S. DEP'T OF DEF., DIR. 5205.16, THE DOD INSIDER THREAT PROGRAM 1 (2016).

272 U.S. DEP'T OF DEF., DIR. 5205.16, THE DOD INSIDER THREAT PROGRAM 1 (2016).

enforcement and is a part of the larger "national security" structure stemming from the Executive Branch's Article II power, which occasionally provides flexibility for government compliance beyond normal warrant requirements.[273] Any law enforcement involvement occurs after a threat is prevented, deterred, detected, or mitigated—assuming an individual is identified. This is secondary to the core purpose of threat detection and information collection on DoD network users.[274]

Moreover, each employee and network user is on notice regarding monitoring and information collection during network use before logging into the network.[275] Upon logging in, employees are confronted with a banner-page displaying specific terms of use, a monitoring agreement, and a notice of the DoD's intent. The employee or user can read and accept these conditions by selecting a live button.[276] A warrant would not limit the discretion of the search, because the AI is focused on identifying behaviors that stray from the normative baseline. Likewise, a warrant has no bearing concerning what the DoD considers a "threat" to its network vis-à-vis its insider threat program. The legitimate government interest exists outside of a law enforcement capacity, and the network user maintains adequate notice of the DoD's monitoring and collection.

Second, requiring a warrant for every instance when the AI detects a network threat is impracticable and inconsistent with the central purpose of warrants.[277] The DoD network is vast, processes many facets of national security information of various classifications, and is a strategic asset to the DoD.[278] There is a substantial need for the DoD to stop these threats efficiently and quickly since the alterna-

---

273 *In re* Directives Pursuant to § 105(b) of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008); Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. ___, 17 (2009).

274 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 17 (2009).

275 *Id.* at 6.

276 *Id.*

277 *Id.* at 17 ("The need for coordinated situational awareness regarding all intrusions and exploitations against Federal Systems is inconsistent with the requirement to obtain a warrant based upon probable cause.").

278 U.S. DEP'T OF DEF., DIR. 8000.01, MANAGEMENT OF THE DEPARTMENT OF DEFENSE ENTERPRISE 2 (2016). *See also* ERIC LANDREE ET AL., IMPLICATIONS OF AGGREGATED DOD INFORMATION SYSTEMS FOR INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION 1

tive could have damaging results. These reasons are removed from the primarily criminal investigatory purposes of the warrant requirement for the government's searches of individuals.[279] The speed and frequency of the monitoring needed to detect cyberspace threats, as well as the nature of machine learning methodologies needed to establish observed normative baseline behavior, would require constant court supervision through the warrant requirement, which courts are ill-equipped to handle. The result would be a frustration of efforts while attempting to protect the DoD network from insider threats.[280]

Through the administrative exception to the warrant requirement, using machine learning methodologies and AI monitoring of the DoD networks to conduct warrantless searches as part of the DoD's insider threats program is not presumptively unreasonable.[281]

c. *Reasonableness Based on Totality of Circumstances*

Lastly, based upon a totality of the circumstances analysis, using AI and machine learning methods to conduct this method of search is reasonable. A totality of the circumstances analysis balances intrusions upon employees' and network users' legitimate expectations of privacy against the government's need to monitor and protect its network.[282] This search must be justified and conducted in a manner related in scope to such justification.[283] Given the volume of attacks on the DoD networks by insider threats, and the damage these attacks can cause, efficient and sophisticated monitoring systems by AI using machine learning methods are justified to detect and prevent insider

(2010) (explaining that the Department of Defense detected 360 million attempts to penetrate its networks in 2008 alone), https://www.rand.org/pubs/monographs/MG951.html.

279 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 16-17 (2009) (concluding that *Einstein* 2.0 is reasonable because it serves a special governmental need beyond the normal need for law enforcement).

280 *Id.* at 16.

281 *Id.*

282 *Id. See also* JEFF KOSSEFF, CYBERSECURITY LAW 274 (2017) ("To assess reasonableness of a search, courts conduct a totality of the circumstances analysis of the search, in which they evaluate on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interest.") (internal quotations and citation omitted).

283 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 16 (2009) (citing O'Connor v. Ortega, 480 U.S. 709, 726 (1987)).

threats.[284] Therefore, the purpose and use of these methods are justified.

These methods are reasonable for two reasons: (1) the impact on employees and users of the network is minimal; and (2) the DoD has implemented minimization procedures.[285] Although the AI conducts constant monitoring of a DoD network, the focus of the monitoring remains on those elements that pose a threat to the network and not on routine tasks or private employee correspondence.[286] If the AI identifies a potential deviation, it would still have the opportunity to queue an analyst to determine whether the deviation is a real and immediate threat.[287] Moreover, as previously discussed, employees and users do not have a legitimate expectation of privacy concerning metadata and are on adequate notice that their content will be monitored before they use the network.[288] Because the AI does not focus on any individual without the individual first deviating from normative baseline behaviors, intrusion upon an employee's expectation of privacy is minimal.

The impact on privacy expectations of employees is further reduced due to the minimization procedures mandated by Section 3 of the Manual.[289] *In re Sealed Case* and *In re Directives Pursuant to § 105(b) of the Foreign Intelligence Surveillance Act* are examples where the court noted the importance of such minimization efforts when analyzing whether pervasive intrusions, such as those discussed

---

284 *See e.g.,* Kevin McCaney, *The accidental hackers: Insider pose the top threat to DoD networks*, PUB. SECTOR MEDIA GROUP (Jan 29, 2015), https://defensesystems.com/articles/2015/01/29/dod-insider-threats-it-security-survey.aspx; *see also* ALEXANDER CROWTHER, NATIONAL DEFENSE AND THE CYBER DOMAIN, 2018 INDEX OF U.S. MILITARY STRENGTH 84-85 (2017); Kevin McCaney, *DoD implementing a system to monitor insider threats*, PUB. SECTOR MEDIA GROUP (May 27, 2016), https://defensesystems.com/articles/2016/05/27/dod-insider-threat-monitoring-system.aspx.

285 *See* U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 10-23 (2016).

286 *See* U.S. DEP'T OF DEF., INST. 8500.01, CYBERSECURITY 3 (2014).

287 *See* U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 10-23 (2016).

288 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 10 (2009).

289 *See* U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 8-43 (2016).

here, are reasonable.[290] The court in *In re Sealed Case* recognized that minimization efforts are "constitutionally *significant*."[291] The court in *In re Directives* noted that such minimization efforts must be adequate enough for a search to qualify as constitutionally reasonable.[292]

The DoD emphasizes that its minimization methods for electronic surveillance are consistent by not only mandating that information should be collected in the least intrusive manner, but also in its retention and dissemination of such information.[293] The DoD mandates that information should be collected in the least intrusive manner by looking at whether there was consent, publicly available information, or alternative authorities and exceptions in the legal regime, such as foreign intelligence collection.[294] The DoD also stresses minimization methods in the retention and dissemination of information by placing vertical approval authorities for certain types of operations and collections, adhering to retention deadlines and tailored information queries, and placing limitations on disseminated information.[295] This process further reinforces that the surveillance and collection concerns those behaviors that indicate threats to a system through the personal and work-related behaviors of individuals using the network.[296] Both courts cited above found this process reasonable, especially in regards to DoD regulation and FISA, respectively.[297]

---

290 *In re* Directives Pursuant to § 105(b) of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008); *In re* Sealed Case No. 02-001, 310 F.3d 717, 731-32 (FISA Ct. Rev. 2002).

291 *In re* Sealed Case No. 02-001, 310 F.3d at 740 ("There are other elements of Title III that at least some circuits have determined are constitutionally significant—that is, necessity, duration of surveillance, and minimization.") (emphasis added).

292 *In re* Directives Pursuant to § 105(b) of the Foreign Intelligence Surveillance Act, 551 F.3d at 1015 ("It is also significant that effective minimization procedures are in place. These procedures serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons.").

293 *See* U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 14 (2016).

294 *Id.*

295 *Id.* at 18-19.

296 *In re* Directives Pursuant to § 105(b) of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008); *In re* Sealed Case No. 02-001, 310 F.3d 717, 731-32 (FISA Ct. Rev. 2002).

297 *In re* Directives Pursuant to § 105(b) of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008); *In re* Sealed Case No. 02-001, 310 F.3d 717, 731-32 (FISA Ct. Rev. 2002).

Because of factors such as minimization methods and the minimal impact on employees' personal privacy, AI and machine learning methodologies as applied to insider threat detection and prevention do not violate Fourth Amendment protections of employees. Consequently, they are constitutionally reasonable.

B. *Statutory Supplements*

Building further upon this hypothetical, consider now that the employee asserts a government violation of privacy protections provided by statutes. The organization's follow-up actions refer the employee for criminal prosecution. There is also a suspicion she may be working on behalf of a foreign nation-state.

The Fourth Amendment is supplemented by several regulatory regimes.[298] These regimes provide stringent standards for government actions that constitute a "search."[299] These statutes were developed within the context of their historical backdrops to address specific issues concerning government abuses of domestic surveillance.[300] The specific legal regimes pertinent for discussion here are the Wiretap Act, FISA, the Stored Communications Act (SCA), and the Pen Registers and Trap and Trace Devices Statute. With the exception of the SCA, the DoD has implemented these regimes in its internal regulations.[301] Each instance of monitoring that constitutes a search under a statute must look to that statute's language during a monitoring operation.

---

298 Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 (2019); Wiretap Act, 18 U.S.C. § 2510 (2019); Stored Communications Act, 18 U.S.C. § 2701 (2019); Pen Registers and Trap and Trace Devices, 18 U.S.C. § 3121 (2019).

299 *See* 50 U.S.C. § 1802 (2019) (providing that electronic surveillance can only be conducted within the parameters of the Attorney General's certification); 18 U.S.C. § 2516 (2019) (describing the circumstances in which a federal judge may grant an application for a wiretap); 18 U.S.C. § 2701 (2019) (prohibiting accessing stored communications without authorization); 18 U.S.C. § 3121 (2019) (prohibiting pen registers except in specific circumstances and after obtaining a court order).

300 Salahudin Ali, *The Bloody Nose: 10 U.S.C. 395*, 6 NAT'L SEC. L.J. 127, 148-51 (2019) (explaining eras and phases of intelligence oversight regulation given government domestic surveillance abuses of the mid-20th century).

301 *See* U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 8-43 (2016).

1. The Wiretap Act

The Wiretap Act provides prohibitions on the unauthorized intentional interception of any electronic communication.[302] As applied to this Article, interception is defined as the "acquisition of the contents of . . . electronic . . . communication through the use of any electronic, mechanical, or other device."[303] Electronic communication refers to any "transfer of sign, signals, writing, images, data, sounds, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, [photo optical] system that affects interstate or foreign commerce."[304] AI includes software-based platforms that monitor and collect electronic information via machine learning algorithms, fitting neatly within this statutory language as an electronic device that can be used to intercept an electronic communication.[305] Section 3 of the DoD Manual implements and requires compliance with this statute when conducting electronic surveillance if collected information will be used for criminal investigatory purposes.[306] It inevitably will if the employee is prosecuted for her actions.[307]

AI also monitors and collects the content of electronic communication within the meaning of the statute. "Content" includes information concerning the substance, purpose, or meaning of a communication.[308] Content is collected by capturing e-mails, website visits, and other actions by an employee or network user.[309] The term "acquired" is not defined by the statute, but courts have interpreted it to mean situations where the contents of a communication have been recorded, viewed, or listened to in real-time or shortly thereafter.[310]

---

302 18 U.S.C. § 2511(1) (2018).

303 *Id.* at § 2510(4).

304 *Id.* at § 2510(12).

305 *Id.* at § 2510(5) ("'[E]lectronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire, oral, or electronic communication.").

306 U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 1 (2016).

307 *Id.* at 23 ("Sections 2510-2522 of [T]itle 18, [U.S.C.]. . .govern electronic surveillance conducted as part of a criminal investigation.").

308 18 U.S.C. § 2510(8) (2018).

309 *See* U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 23-24 (2016).

310 United States v. Bynum, 360 F. Supp. 400, 408 (S.D.N.Y. 1973), *aff'd.*, 485 F.2d 490 (2d. Cir. 1973), *rev'd on other grounds* 417 U.S. 903 (1974) ("[This] definition clearly equates 'interception' with the listening to, monitoring, or hearing of described communications, *either at the*

The involvement of a human analyst meets this standard. Notably, the Wiretap Act also prohibits the use and disclosure of information obtained from unlawful interception for certain service providers.[311] The DoD Manual implements this statute by prohibiting such disclosures and uses outside of the intelligence community, except in narrow circumstances.[312]

An AI analyzing the text, behavior patterns, and content of electronic correspondence on a DoD network by constant monitoring to detect and prevent threats is subject to this statute because of its potential use in a criminal trial.[313] E-mail correspondence and use of a network occur within an electronic system and are electronic communications.[314] The AI needs to study this electronic environment to establish a baseline of normative behavior.[315] It also needs to acquire and analyze the content transmitted via e-mail and the actions of users to produce output.[316] The AI does this in a number of ways, such as text and word usage analysis to determine a behavioral profile through input algorithms.[317] Through this process, an AI can analyze the content of those behaviors it cues as threats to the network.[318] Both this process and its conclusion are the same once content is forwarded to a human analyst for further examination and production of a final product vis-à-vis the intelligence collection cycle. The AI intercepts, uses, and then discloses such electronic communication content for purposes of carrying out its insider threat mission, which subjects it to the statute's language.[319]

---

time such communications occur or at a subsequent time through the use of electronic means.") (emphasis added).

311 18 U.S.C. §§ 2511(1)(b)-(1)(e) (2018).

312 *See* U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 8-43 (2016).

313 *See* 18 U.S.C. § 2511(1)(e)(i) (2018).

314 U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 48 (2016) ("[E]lectronic surveillance. [The] acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.").

315 *See* SIFMA, INSIDER THREAT BEST PRACTICES GUIDE 12 (2018) (advising law firms on how to handle insider threats).

316 *See id.* at 26.

317 *Id.*

318 *Id.*

319 *See* 18 U.S.C. § 2511(1)(e)(i) (2018).

The statute and DoD regulations provide several exceptions.[320] First, an agency-provider that owns the network may intercept, disclose, or use such information necessary for the protection of the network for its users.[321] The statute allows an agency to protect the network as its own property.[322] The DoD maintains this right not only as the owner and provider of the network, but also as the owner of the assets connected to the network for official duties and work-related communication.[323] The insider threat program was created for this very reason.[324] The purpose of using an AI with machine learning methodologies is to efficiently and quickly identify threats that come from within the network.[325] Thus, the insider threat program provides the justification for monitoring and collection within the DoD network as a protection of property within the intelligence gathering context.

For an agency to protect its network property, there are some limiting factors. In this case, network protection is an exception to the general prohibition of unlawful interception of electronic communication in that the interception must be "necessary."[326] An action necessary to protect network property is decided on a case-by-case basis, but has generally been construed to mean that protection efforts must be reasonable.[327] For example, one standard requires the interception only collects what is minimally needed to accomplish protection goals.[328] The DoD meets this standard by requiring minimization in its network protection as implemented in its collection limitation regime.[329] Collection minimization standards and precedents include

---

320 *See* U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 10 (2016)); 18 U.S.C. § 2511(1) (2018).

321 18 U.S.C. § 2511(2)(a)(i) (2018).

322 *Id*.; *see also* Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 24 (2009) (concluding that Einstein 2.0 is used solely to protect the government's property and rights).

323 *Id.*

324 *Id.* at 3.

325 *Id.* at 3-4.

326 18 U.S.C. § 2511(2)(a)(i) (2019).

327 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 4 (2009) (citing United States v. Harvey, 540 F.2d 1345, 1351, 1352 (8th Cir. 1976)).

328 *Id.* (citing *Harvey*, 540 F.2d at 1351).

329 U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 11 (2016).

protecting employees' and network users' speech rights, which are built into the DoD collection procedures.[330] This ensures only the minimal amount of information needed to identify a threat is collected and meets the statutory standard.[331]

Another exception under the Wiretap Act allows the interception of electronic communication correspondence when the user gave voluntary consent.[332] Either the recipient's or the sender's consent to the monitoring and collection is considered sufficient.[333] If one party consents to monitoring, not only will their activities and correspondence be monitored and collected, but the correspondence of others with the consenting party will be as well.[334] This is similar to the consent exception discussed earlier in this Article.

The employee has consented daily to monitoring and collection for insider threat purposes during the performance of her official duties.[335] Moreover, the employee received adequate notice of this consent and its purposes by attending annual training. The training and daily notice factors imply that the employee agreed to be monitored because she manifested consenting behavior by continuing to use the network, knowing she was being monitored.[336] The employee's participation in and acceptance of agency monitoring to detect and prevent insider threats clearly indicates the DoD has obtained her voluntary consent. Consequently, the DoD did not violate the Wiretap Act, because it obtained the employee's voluntary consent in this hypothetical and maintains its right as the owner of the property to protect its network using AI.

2. Foreign Intelligence Surveillance Act

FISA is a hallmark legislative piece governing the domestic counterintelligence surveillance and collection regime applicable to

---

330 *Id.* at 14.

331 *Id.* at 13.

332 18 U.S.C. § 2511(2)(c) (2019).

333 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 24 (2009) (citing U.S. v. Barone, 913 F.2d 46, 49 (2d Cir. 1990)) ("one-party consent obviates the need to obtain a court order under the Wiretap Act.").

334 *Id.* at 23.

335 *Id.* at 5.

336 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 24 (2009) (citing Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990)).

DoD networks.[337] Its roots stem from historical intelligence collection abuses by the Executive Branch,[338] and it was implemented in the DoD regulatory regime through the Manual's Section 3.[339] FISA has been subject to multiple revisions focused on balancing legitimate foreign intelligence collection activities while protecting U.S. persons' privacy rights.[340] Additionally, FISA applies to insider threat programs where insider threats act on behalf of, are motivated by, or are in the furtherance of the goals of foreign agents and nations.[341]

FISA is the exclusive means for electronic surveillance of U.S. persons located in the U.S. for foreign intelligence purposes.[342] This means there must be a connection between a foreign power and the U.S. person.[343] Additionally, FISA prohibits intentional electronic surveillance without the express statutory authorization provided by it or other statutes like the Wiretap Act, the Pen Registers and Trap and Trace Devices Statute, and the SCA.[344] This express authorization occurs through statutory warrants or statutory exceptions.[345] Electronic surveillance under this statute excludes situations where a U.S. person is not subject to intentional targeting,[346] there is no radio communication and emails do not constitute "radio communication" under the statute,[347] consent has been provided,[348] and there is not a reasonable expectation of privacy.[349]

The DoD's use of AI in its insider threat programs is exempt from FISA for several reasons. First, the AI does not intentionally target an individual until it finds behavior that deviates from its known baseline.[350] Likewise, e-mails are not "radio communications"

---

337 Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1813 (2019).

338 S. REP. NO. 110-209, at 23 (2007).

339 U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 23 (2016).

340 *See* Fowler, *supra* note 235, at 227-33 (describing the several amendments to FISA).

341 U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 23-25 (2016).

342 50 U.S.C. § 1812 (2018).

343 *See id.* at § 1801(b)(2).

344 *Id.* at §§ 1809(a)-1810.

345 *See* 50 U.S.C. §§ 1802-1804, 1806-1813, 1842-1845 (2019).

346 50 U.S.C. § 1801(f)(1) (2019).

347 *Id.* at § 1801(f)(2).

348 *Id.*

349 *Id.* at § 1801(f)(3).

350 *See* Vegard Flovik, *How to Use Machine Learning for Anomaly Detection and Condition Monitoring*, MEDIUM (Dec. 31, 2018), https://towardsdatascience.com/how-to-use-machine-learning-for-anomaly-detection-and-condition-monitoring-6742f82900d7.

as explained by the statute because radio communication indicates communications that use transmitters and receivers through internet wires, cables, and micro-processing chips found in computers.[351] Therefore, radio communications are considered more akin to an "oral utterance."[352] Moreover, as previously discussed, the employee provides consent with adequate notice before she logs onto the cyberspace network.[353] Lastly, a reasonable expectation of privacy does not exist due to: (1) consent;[354] (2) the employee's sharing of information with third-parties, government, or other government employees;[355] and (3) lack of ownership in the communication system.[356] Thus, FISA's requirements are not met, and no surveillance that violates FISA has occurred.

It is important to note that because of the existence of a worldwide DoD system, FISA also applies to employees stationed outside of the continental U.S.[357] Intelligence community members, namely those authorized to collect intelligence within DoD networks,[358] may not intentionally target a U.S. person located outside the U.S. for purposes of foreign intelligence information.[359] This is the case if such U.S. person is reasonably believed to be outside the United States, *and* such person has a reasonable expectation of privacy where a warrant would be required if the targeting had happened within the U.S. for law enforcement purposes.[360] The targeting must constitute "electronic surveillance," or it must seek to acquire either stored electronic communications or data requiring an order under FISA if the acquisi-

---

351 50 U.S.C. § 1801(f)(2) (2019); *see also* 18 U.S.C. (1)(b) (2019).

352 Interception of Radio Communication, 3 Op. O.L.C. 240, 242 (1979).

353 50 U.S.C. § 1801(2) (2019); U.S. v. Missick, 875 F.2d 1294, 1299-1300 (7th Cir. 1989) ("[C]onsent [does] not fall within any of the. . .definitions of 'electronic surveillance'."). The DoJ Office of Legal Counsel opinion also provides that consent regarding FISA entails the same type of consent as that of the Wiretap Act, thus section in both statutes defining "consent" may be read *in pari materia.* Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 30 (2009).

354 *See* 50 U.S.C. § 1801(f)(2) (2019).

355 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 7 (2009).

356 *See* U.S. DEP'T OF DEF., REG. 5500.7-R, JOINT ETHICS REGULATION 21, 23 (2011).

357 50 U.S.C. § 1881b(a)(1) (2019).

358 50 U.S.C. § 3003(4)(G) (2019).

359 50 U.S.C. § 1881c(a)(2) (2019).

360 *Id.*

tion is conducted within the U.S.[361] The order must be issued from the Foreign Intelligence Surveillance Court for the targeted U.S. person or an authorization is granted by the U.S. Attorney General, or some other provision of FISA has been granted.[362] If there is a reasonable belief that the U.S. person is now located within the U.S., the surveillance must cease until it is reasonably believed that the person has moved outside the U.S.[363]

An AI monitoring a DoD network for insider threats would not be stopped by these sections of FISA since these sections prevent the *intentional targeting* of a U.S. person where the monitoring seeks to collect foreign intelligence information using electronic surveillance.[364] The AI only seeks to monitor anomalous behavior to prevent network threats, it does not initially intend to target any individual. While foreign intelligence information is one aspect of the insider threat program, it is not the only information collected.[365] It may become relevant once the AI determines the existence of a threat, but it is a secondary consideration. The focus remains on preventing a network threat, not solely for the collection of foreign intelligence information on the individual. Consequently, AI monitoring and collection using its machine learning methodology would be permissible under *FISA*.

3. Stored Communication Act

The ability to retain and disseminate information raises a compliance issue concerning the SCA. Although not implemented in the DoD Manual, this statute is worth noting. It is debatable whether a DoD cyberspace network is considered a public service under the

361 *Id.* at § 1881b(a)(1).

362 *Id.*

363 *Id.*, § 1881b(a)(2) ("If a United States person targeted under this subsection is reasonably believed to be located in the United States. . .an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States."). This section applies to targeting granted by an order located in section (c), which provides that a U.S. person is reasonably believed to be located outside of the United States. The salient point is that a person located *within* the United States has protections governed by § 1812.

364 *See* 50 U.S.C. § 1801(f)(1) (2019) (prohibiting intentional targeting of a U.S. person).

365 18 U.S.C. §§ 2710-2711 (2019). *Cf.* Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 32 (2009) (comparing Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042-43 (N.D. Ill. 1998) with Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) because they reach opposite conclusions on whether the federal government is a provider of electronic communication services to the public).

SCA, but even if it were, AI agents monitoring a network that collects and disseminates information to relevant authorities would not run afoul of the statute.[366] The SCA creates two prohibitions. First, it prohibits individuals from accessing electronic communications without authorization or exceeding their authorization.[367] The electronic communication must be accessed in a facility that provides or stores the communication.[368] Second, the SCA prohibits knowingly divulging the communication's contents.[369] Whether a DoD network is considered a public or private electronic service provider or remote computing service under this statute is irrelevant. A DoD network needs to store information as a service and divulge content without authorization, or by exceeding such authorization.[370]

Electronic storage means any temporary, intermediate storage incidental to a communication's transmission.[371] It also includes the backup storage to protect and retain the communication.[372] Electronic communications sent over a DoD network by members and users are subject to the SCA due to the network's ability to store e-mails.[373] An AI inputs the data from electronic communications before, during, and after sending.[374] For example, this storage includes a sent e-mail sitting in the outbox folder or an unopened e-mail in an inbox folder. Although employees and network users can voluntarily store e-mails for their own information management purposes, the DoD does not provide this storage as an independent service.[375]

Furthermore, assuming the DoD offers storage services under the SCA, exceptions exist. The SCA permits access and divulgence of content information if authorized by the entity providing the service, the service user, or as authorized by an authorized order.[376] If the DoD is considered a provider, it still maintains access to all communications to disclose to itself or other internal staff to protect its net-

366 18 U.S.C. §§ 2701(a)(1)-(2) (2019).
367 *Id.*
368 *Id.*
369 *Id.* at § 2702(a)(1).
370 *See id.*
371 18 U.S.C. § 2510(17)(A) (2018).
372 *Id.* at § 2510(17)(B).
373 *See* Theofel v. Farey-Jones, 341 F.3d 978, 984-85 (9th Cir. 2003).
374 *See id.* (describing how messages are stored during and after sending).
375 *See* 18 U.S.C § 2701(c) (2018).
376 *Id.*

work.[377] Moreover, employees or users consent to this potential disclosure when they accept the terms and conditions, which allows the DoD's AI to monitor their content for insider threat purposes.[378] Therefore, the DoD's access to and divulgence of stored information would also be permissible because of its consent for the same purposes.[379]

Another exception would allow the DoD to access and divulge communications and stored communications if it is necessary to the rendition of the service or the protection of the network.[380] Additionally, an AI may access and divulge information as prescribed by DoD regulations to protect against insider threats.[381] Therefore, employees' privacy rights protected by the SCA would not be violated.

4. Pen Registers and Trap and Trace Devices Statute

The Pen Registers and Trap and Trace Devices Statute prohibits the installation or use of a pen register or trap and trace device without first obtaining a court order.[382] This statute is implemented within the DoD regulatory regime.[383] Among other things, these devices can record or decode routing, addressing, or signaling information transmitted by hardware within a network.[384] This information does not include content, but is only meant to identify a source of information.[385] This type of information is relevant because an AI would require it to perform its data input function in establishing baseline behavior, such as website visits or normal e-mail addresses. To acquire this information, the DoD must comply with this statute's language.[386]

---

377 *Id.* at § 2702(b)(4).

378 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 30 (2009).

379 18 U.S.C. § 2702(b)(3) (2018).

380 *Id.* at § 2702(b)(5).

381 U.S. DEP'T OF DEF., INSTR. 5240.26, COUNTERING ESPIONAGE, INTERNATIONAL TERRORISM, AND THE COUNTERINTELLIGENCE INSIDER THREAT 12-13 (2018).

382 18 U.S.C. § 3121(a) (2018).

383 U.S. DEP'T OF DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES 23 (2016).

384 18 U.S.C. §§ 3127(3)-(4) (2018).

385 *Id.* at § 3127(4) ("[S]uch information shall not include the contents of any communication . . . ").

386 18 U.S.C. §§ 3121, 3123 (2018).

Consistent with the above discussion, valid consent serves as an exception to this general prohibition if the device is used by a network provider.[387] Assuming the DoD qualifies as a network provider in this context, it would provide network services to users of its cyberspace network.[388] Each user accepts the terms of monitoring and information collection with each login before using the network.[389] Before accepting the terms of use, each user receives notice of the DoD's intent to monitor and the reason for its insider threat program.[390] Therefore, an AI that records this information after employees accept the terms of use is lawful without a court order.

Another exception found within the Pen Registers and Trap and Trace Devices Statute's is the right to defend network property.[391] Protecting a network from insider threats satisfies this statutory exception. If the information surveilled and collected pertains to the insider threat program, an AI that records information under this act may do so lawfully without a court order.

4. First Amendment

Consider this final change to our hypothetical. The employee now asserts that the DoD has violated her First Amendment rights to free speech, because of some of the analytics the AI uses collect and assign value to her exercise of political speech. However, she was using a government computer while exercising this political speech.

Speech protections for DoD network users are protected in the Manual and in a variety of other related regulations such as *Department of Defense Instruction 1000.29*.[392] This is an underdeveloped, but pertinent, area of law concerning AI and counterintelligence regula-

---

387 *Id.* at § 3121(b)(c).

388 *See* Burgess, *supra* note 32.

389 Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. __, 30 (2009).

390 *Id.*

391 18 U.S.C. § 3121(b)(1) (2018). This right is the same as the Wiretap Act as the DoD is a service provider to users and its employees. 18 U.S.C. § 2511(1) (2018). This differs from the Stored Communications Act (SCA), in that the SCA applies to public service providers. 18 U.S.C. § 2701 (2018).

392 *See* Hatch Act of 1939, 5 U.S.C. § 7323(a) (2008); U.S. DEP'T OF. DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF INTELLIGENCE AGENCIES 5 (2016); U.S. DEP'T OF DEF., DIR. 5500.07, STANDARDS OF CONDUCT 1-2 (2007); U.S. DEP'T OF DEF., DIR. 1344.10, POLITICAL ACTIVITIES BY MEMBERS OF THE ARMED FORCES 2 (2008).

tion.[393] The nature of AI monitoring and its rationally-based decisions concern whether certain behaviors are a deviation from an established normative baseline. This presents a friction point as DoD network users enjoy First Amendment protections.[394]

The First Amendment to the Constitution guarantees that "[C]ongress shall make no law. . . abridging the freedom of speech."[395] Although DoD cyberspace network users keep their First Amendment rights, these rights are limited within the network to ensure that they do not impede the effectiveness of the organization's mission.[396] The right to free speech does not include speech that directly advocates for the imminent incitement or production of illegal activity or action.[397] For example, a network user could not claim a freedom of speech right to commit an act of espionage, conspiracy, or any other activity constituting an insider threat to the DoD network.[398] This is especially true if the speech communicated presents a clear and present danger.[399]

The insider threat program is aimed at preventing insider threats that will cause damage to a DoD network.[400] Although speech is included in an AI's analysis, it is not the sole consideration.[401] An analogy arises from *State v. Loomis,* where the Wisconsin Supreme Court held in favor of using AI analytics in a judicial sentencing process.[402] This case indicates the validity of using algorithmic analytics based on some forms of constitutional protections as long as the ana-

---

393 *See* Bowen et al. *supra* note 152, at 22.

394 *See* U.S. DEP'T OF. DEF., DIR. 5420.01, PROCEDURES GOVERNING THE CONDUCT OF INTELLIGENCE AGENCIES 1 (2016).

395 U.S. CONST. amend. I.

396 *See* Parker v. Levy, 417 U.S. 733, 758 (1974) ("[F]undamental necessity for obedience, and the consequent necessity for imposition of discipline, may render permissible within the military that which would be constitutionally impermissible outside it").

397 Brandenburg v. Ohio, 395 U.S. 444, 448-49 (1969).

398 *See* United States v. Afshari*,* 426 F.3d 1150, 11621 (9th Cir. 2005), *reh'g denied*, 446 F.3d 915 (9th Cir. 2006), *cert. denied*, 127 S. Ct. 930 (2007); *see* Dunne v. United States, 138 F.2d 137 (8th Cir. 1943); United States. v. Rosenburg,195 F.2d 583 (2d Cir. 1952); and United States v. Mason, 60 M.J. 15, 20 (C.A.A.F. 2004).

399 *See* Schenck v. United States, 249 U.S. 47, 52-53 (1919); Schaefer v. United States, 251 U.S. 466, 474-75 (1920); *see also* Thomas v. Collins, 323 U.S. 516, 529-30 (1945) (holding that any restriction on First Amendment rights must be justified by a clear and present danger).

400 U.S. DEP'T OF DEF., INSTR. 5240.26, COUNTERING ESPIONAGE, INTERNATIONAL TERRORISM, AND THE COUNTERINTELLIGENCE INSIDER THREAT 6 (2018).

401 *Id.* at 7, 9.

402 State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

lytics are not the *sole* reason for a result of a decision-making process.[403]

In our hypothetical, the same result would occur. The AI uses speech as an analytical data collection point, but it is not the *sole* indicia of a present threat. Moreover, speech that attempts to damage the network and undermine the DoD's mission is not protected.[404] Thus, the DoD may monitor and collect information based upon speech that deviates from normative baselines established by an AI for insider threat detection purposes.

An analysis of First Amendment rights within a DoD network also raises implications as to whether certain speech is limited by viewpoint or allowed generally, given that a network may qualify as a non-public forum.[405] Although traditionally applied to physical installations, a network more than likely meets this test because it is not designed by purpose or tradition to act as a forum for public communication.[406] Instead, it is designed for the specific purpose of facilitating DoD information for organizational mission accomplishment. Any limitation must be reasonable and rationally related to the objectives of network administration.[407] Limitations on certain speech, like speech that poses a danger—such as an insider threat—are reasonable to accomplishing the DoD's objective to protect information transacted across the network and the organization overall.

The employee in the hypothetical could not claim that her actions fall within the First Amendment protections, since they indicate a threat to the network. Her actions as observed and screened by the

---

403 State v. Loomis, 881 N.W.2d 749, 772 (Wis. 2016), *cert. denied*, 137 S. Ct. 2290 (2017). The case dealt with a defendant's access to algorithm methodologies that were used to predict recidivism assessments. *Id.* at 755. The algorithms were covered by, among other things, commercial trade secrets. *Id.* at 761. The defendant argued that this lack of access deprived him of due process to challenge whether the algorithm wrongfully considered his race, gender, etc. *Id.* at 753. The court ultimately upheld the use of the specific program's constitutionality, but placed limits on its use—independent rationale must accompany a sentencing decision, the algorithm cannot be used to determine if someone should be incarcerated, or used to calculate length of sentence. *Id.* at 769.

404 *See* Parker v. Levy, 417 U.S. 733, 758 (1974) (holding that speech that abrogated the military's mission was not protected by the First Amendment).

405 *See* Greer v. Spock, 424 U.S. 828 (1976); Hague v. Comm. for Indus. Org., 307 U.S. 496, 515-17 (1939).

406 *See* Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 44-45 (1983); Cornelius v. NAACP Legal Defense and Education Fund, 473 U.S. 788, 799-801 (1985).

407 *See Perry Educ. Ass'n*, 460 U.S. at 54 (applying the rational basis test to nonpublic forums).

AI did not seek to limit her speech. The AI only sought to analyze whether her actions objectively indicated a danger to the DoD.

IV. NORMATIVE ARGUMENTS

As society continues to increase its reliance on technology, the implementation of complex and sophisticated AI platforms may assist in the detection and prevention of insider threats.[408] However, this rapidly evolving technology is not without controversy. Some commentators voice concerns regarding the appropriateness of allowing AI to fulfill tasks traditionally performed by humans to collect and analyze information,[409] while others argue that it may spark innovative uses in new and existing platforms.[410] There are benefits and drawbacks to using AI. However, if legal regimes exist to responsibly implement this technology for the protection of networks and people who serve critical missions in organizations like the DoD, implementation of these advanced technologies should be advocated for in any organization using cybersecurity to support its larger mission.

A. *Current Uses of Artificial Intelligence and Machine Learning in the Department of Defense*

AI's impact on current conventional DoD operations is evident. For example, the U.S. Air Force adapted an over 60-year old U-2 spy

---

408 Brdiczka et. al., *supra* note 144, at 143-43; *see also* ANDREA LITTLE LIMBAGO, ENDGAME: INPUT TO THE COMMISSION ON ENHANCING NATIONAL CYBERSECURITY 2 (2016) ("Unsupervised machine learning approaches—such as those focused on user and entity behavior analytics—works at the intersection of human behavior and big data analytics. . .this does not imply automated strategic decision, but more so the automation and evolution of protection and detection. . .cybersecurity should be viewed as a learning system that evolves with additional data, reflecting a system-within-systems environment. . .").

409 SAYLER, *supra* note 94, at 8.

410 *See* Jamey Keaten, *Experts assemble for UN-hosted meeting on 'killer robots*,' ASSOC. PRESS (Aug. 27, 2018) ("Experts from scores of countries are meeting to discuss ways to defined and deal with 'killer robots'—futuristic weapons systems that could conduct war without human intervention."), https://www.apnews.com/90fc2325b8244e179ee5a9677fe1fc23; *see also* Kelsey Atherton, *Targeting the future of the DOD's controversial Project Maven initiative*, C4ISRNET, IT & NETWORKS (July 28, 2018), https://www.c4isrnet.com/it-networks/2018/07/27/targeting-the-future-of-the-dods-controversial-project-maven-initiative/; *see* Michael M. Phillips, *The U-2 Spy Plane Is Still Flying Combat Missions 60 Years After Its Debut,* WALL ST. J. (June 8, 2018) ("Six decades after the U-2 flew its first mission, the military is trying to harness artificial-intelligence technology to enhance the venerable spy plane's combat reconnaissance capabilities."), https://www.wsj.com/articles/the-u-2-spy-plane-still-flying-combat-missions-60-years-after-debut-1528382700.

plane to utilize the advanced computer programs developed by Stanford University that analyze film shot during operational missions.[411] Before this development, the U-2 plane had the capability to collect massive amounts of imagery, but was constantly plagued by "too much imagery, too few analysts, and too little time."[412] By implementing AI technology, the expectation is that the AI can scan massive amounts of data and notify an analyst when potential areas of concern arise.[413] This would solve both the time and efficiency gaps plaguing military intelligence analysts and allow them to concentrate their time on comprehending the collected material, as opposed to mechanically sifting through data.[414]

The Algorithmic Warfare Cross-Functional Team (Project Maven) provides another example.[415] Project Maven's original purpose was to integrate AI and machine learning more effectively across military operations to maintain superiority.[416] Thus far, Project Maven has used AI and machine learning methodology via computer vision—the ability to autonomously extract objects of interest from moving or still imagery—to provide prolonged intelligence collection by drones, allowing analysts to multiply their efforts in the fight against the Islamic State.[417]

The use of AI in cybersecurity and insider threat detection is also prominent. One program,"Sharkseer," has thus far been a successful, publicly-disclosed program that protects DoD networks.[418] Its success is attributed to its ability to inspect the DoD system traffic for unknown vulnerabilities, such as zero-day exploits[419] and other

411 Phillips, *supra* note 410. The Stanford School of Engineering and Business also provides the Air Force with students to assist in this program.

412 *Id.*

413 *Id.*

414 *Id.*

415 U.S. DEP'T OF DEF., MEMORANDUM: ESTABLISHMENT OF AN ALGORITHMIC WARFARE CROSS-FUNCTIONAL TEAM (PROJECT MAVEN) 1 (2016).

416 *Id.*; *see also* John N.T. Shanahan & Cortney Weinbaum, *Intelligence in a Data-Driven Age,* 90 JOINT FORCE Q. 4, 6 (2018).

417 Cheryl Pellerin, *Project Maven to Deploy Computer Algorithms to War Zone by Year's End*, U.S. DEP'T OF DEF. (July 21, 2017), https://www.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end//.

418 Justin Lynch, *The AI that protects DoD networks from zero-day exploits*, THE FIFTH DOMAIN (July 27, 2018), https://www.fifthdomain.com/dod/2018/07/27/the-ai-that-protects-dod-networks-from-zero-day-exploits/.

419 *See* Kim Zetter, *Hacker Lexicon: What is a Zero Day?*, WIRED (Nov. 11, 2014), https://www.wired.com/2014/11/what-is-a-zero-day/. "A Zero-day exploit refers to code that attackers

advanced threats by scanning e-mails and documents that attempt to infect DoD networks.[420] Furthermore, the program can identify the location and actor responsible for such attempts, and can be used to conduct behavior analysis of suspicious files and actors.[421] The advancement of such technologies will no doubt serve the purpose of detecting and mitigating insider threats of DoD networks.

AI will continue to emerge as a common tool within the national security and intelligence framework. Indeed, the National Defense Authorization Act of 2019 signifies the growing importance of AI technology to the government, as the government increases its investment in AI and increases its integration in every domain to combat peer and near-peer competitors from gaining an advantage over the U.S.[422] Additionally, serious language is found in a 2018 Senate Report recommendation that the Director of the Defense Intelligence Agency, in coordination with relevant partners, report U.S. capabilities concerning emerging technologies like quantum information science[423] and AI with that of U.S. competitors.[424]

---

use to take advantage of a zero-day vulnerability." *Id.* "Zero-day vulnerability refers to a security hole . . . that is yet unknown to the software maker or to antivirus vendors." *Id.*

420 Lynch, *supra* note 418.

421 *Id.*

422 SEN. REP. NO. 115-262, at 4 (2018) ("[T]he [NDAA] makes significant investments in research and development [(R&D)] to re-establish a credible combat advantage. The legislation increases [R&D] spending by $1.2 billion, the majority of which is for science and technology spending with an emphasis on high priority emerging technologies like. . .artificial intelligence, space, cyber, and directed energy.").

423 *Id.* Quantum Information science (QIS) is a scientific field implemented in technology. *See, e.g.*, NAT'L SCI. FOUND., QUANTUM INFORMATION SCIENCE: AN EMERGING FIELD OF INTERDISCIPLINARY RESEARCH AND EDUCATION IN SCIENCE AND ENGINEERING (1999). It is multidisciplinary, blending elements of physical science, mathematics, computer science, and engineering. *Id.* at 4. It attempts to understand how certain fundamental laws of physics discovered can be harnessed to dramatically improve the acquisition, transmission, and processing of information. *Id.* QIS's direct impact for national security purposes will be in the field of cryptology and encryption vis-à-vis cybersecurity and cyber operations. For example, today's digital computers process classical information encoded in bits, a quantum computer processes information encoded in quantum bits, or qubits. A qubit is a quantum system that can exist in a coherent superposition of two distinguishable states and can be entangled with other such systems (as opposed to existing in binary states). *Id.* at 5. This means that information can be read and copied without being disturbed. Primarily, extremely secretive and accelerated processing are possible; abstractly, a platform running a quantum computing application can process in seconds what would take billions of year due to the ability to process the root of classical computing time. *Id.* Clearly, the impact on AI, CI, cryptology, and cybersecurity is astounding.

424 SEN. REP. NO. 115-262, at 60-61 (2018).

B. *Benefits of AI Tools Within an Intelligence Gathering Context*

Using AI in an insider threat context provides a more efficient and accurate assessment of threats. By training an AI to identify behaviors indicating a network threat, false positives are minimized and subversive activity prevented. Former FBI Counsel, Jim Baker, wrote about this issue in a series of articles regarding counterintelligence and AI.[425] Baker notes that counterintelligence contains certain elements beneficial to national security. Among other potential benefits, counterintelligence is proactive, protective, and powerful.[426] He further explains that an AI's ability to cheaply and quickly evaluate large data sets, word documents, e-mails, and speech and face recognition tools fills a need because humans are not as efficient.[427]

From a proactive standpoint, AI assists in forward-focused efforts to collect intelligence and prevent threats, as opposed to a reactive approach as adversaries make use of advanced technologies. The clandestine nature of counterintelligence is that AI assists in not only conducting proactive counterintelligence actions, but also in "countering both clandestine intelligence gathering activities" and other "covert actions" against the U.S.[428] This is extremely important given how cheaply AI tools are available to the masses, including insider threats that exist within a DoD network.[429]

From the protective point-of-view, AI can be used to diagnose weak far-side objectives that other nations will seek to exploit within the DoD. AI may be able to indicate certain zero-day exploits that an insider could use to damage a DoD network or disclose sensitive information to a hostile-nation. This creates obstacles against insider threats by closing the gap between time and space that hostile advanced technology, operating at speeds and capabilities faster than human analyst may be able to protect against, can otherwise exploit.

---

425 Jim Baker, *Artificial Intelligence-A Counterintelligence Perspective-Part I,* LAWFARE (Sept. 28, 2018), https://www.lawfareblog.com/artificial-intelligence-counterintelligence-perspective-part-1.

426 *Id.*

427 *Id.* ("In many instances, AI can do these things faster, better and more cheaply than people can. . .").

428 *Id.*

429 *See* R.J. Reinhart, *Most Americans Already Using Artificial Intelligence Products*, GALLUP ECONOMY (March 6, 2018), https://news.gallup.com/poll/228497/americans-already-using-artificial-intelligence-products.aspx.

This additional layer of defense augments human capabilities instead of merely replacing them.

AI also makes counterintelligence efforts more powerful. As Baker notes, counterintelligence leverages all national security resources and authorities available to combat hostile nations seeking to damage the U.S.[430] Already, the capability exists to conduct highly intrusive electronic surveillance as well as the authority to act on such surveillance.[431] AI increases the potency of this unity-in-effort by leveraging these resources in combination with large aggregate data outside of the traditional counterintelligence network.[432] This means pulling data from larger data sets found in immigration databases, credit reports, commercial transactions, and foreign criminal records databases in compliance with applicable law. AI is not completely constrained to the information that exists within a DoD network to establish a baseline of normative behavior. It instead takes a holistic counterintelligence approach in making rational decisions about insider threats by considering interdisciplinary and cross-functioning data.

Clearly, AI agents serve as a force-multiplier in insider threat detection. Fears of an overreliance on imperfect AI agents may prove to be unfounded if they can be blended with beneficial counterintelligence elements that already exist.

C. *Negative Impacts*

There is also an argument that using these extremely intrusive AI agents may blunt insider threat efforts. Dr. James Allen provides an example in his doctoral thesis that insider threat programs may impact employee attitudes in the participation of detecting and preventing insider threats.[433] Allen's empirical study examined the fears, trust, and privacy invasion considerations of insider threat programs.[434] Two of his key points state that insider threat programs depend on detecting the "driving forces" of such threats, and the motivation of

---

430 Baker, *supra* note 425.

431 *Id.*

432 *Id.*

433 James Allen, Impact of Insider Threat Detection and Prevention Programs on Under Secretary of Defense for Intelligence (USDI) Organizations (May 2017) (unpublished Ph.D. dissertation, Capitol Technology University) (on file with author).

434 *Id.*

the organization's personnel in countering them.[435] Money, carelessness, ideology, compromise, and ego are all factors that create an insider threat to a network.[436] Intrusive AI agents may exacerbate some of these elements if employees and network users feel as though they are the adversary, as opposed to part of the larger insider threat detection team.

Ultimately, Allen concludes there are no significant, current indications of whether an insider threat program impacts employees' motivations to participate or their continued efforts to be aware of and report insider threats.[437] He cautions, however, that continued awareness of potential demotivational impacts within certain employee groups is warranted if such insider threat programs become too focused on groups susceptible to surveillance.[438] This is especially true if the AI is using a machine learning methodology that builds behavior profiles and establishes normative behavior within a system based upon explicit and implicit biases of a human programmer. The best approach is to ensure continued auditing and reevaluation of insider threat programs, especially when using intrusive AI and machine learning methodology to monitor employees and users within a DoD network.

CONCLUSION

AI's importance will continue to be stressed in cybersecurity, intelligence, and insider threat communities. The benefits of its uses are all too apparent. As AI becomes more autonomous, rational, and intelligent, past notions of legal compliance of these technologies will be challenged. This Article sheds light on how to address those concerns causing friction between the rights of U.S. person who uses a DoD network and the U.S. government.

The DoD maintains a complex set of regulations allowing the use of AI in its insider threat detection efforts on a basis that respects constitutional privacy rights as well as government interests. Although previous analysis may still be relevant and provides a foun-

---

435 *Id.*; *see* Charney & Irvin, *supra* note 4, at, 72-74. Charney and Irvin explain that money, ideology (true believers), compromise/coercion, ego, disgruntlement, ingratiation, and thrills are all factors of the human psychological behavior that facilitate insider espionage.

436 Allen, *supra* note 433.

437 *Id.*

438 *Id.*

dation for continued evaluation and application of current legal regimes to these advanced technologies, prudent evaluation at every occasion when applying this technology is a best practice to ensure insider threat programs are conducted on a legally sufficient basis.

Finally, the normative implications of AI use in insider threat detection and prevention is still up for debate. Its uses will not only require prudency and real, achievable goals to maximize efficiency and timeliness, but also moderation to prevent the negative implications on employee morale and the complexity of threat activity.