2-7-2024

Behind the curve: technology challenges facing the homeland intelligence and counterterrorism workforce

Michelle Black

Lana Obradovic

Deanna House

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2024, tyae002
https://doi.org/10.1093/cybsec/tyae002

Research paper

Behind the curve: technology challenges facing the homeland intelligence and counterterrorism workforce

Michelle Black [1,*], **Lana Obradovic** [1], **Deanna House** [2]

[1] Department of Political Science, University of Nebraska at Omaha, Omaha, NE 68182, United States
[2] Information Systems and Quantitative Analysis, University of Nebraska at Omaha, Omaha, NE 68182, United States

[*] Corresponding author. University of Nebraska at Omaha, 6001 Dodge St., ASH 275, Omaha, NE 68182, United States.
E-mail: michellblack@unomaha.edu

Received 8 May 2023; revised 21 December 2023; accepted 9 January 2024

Abstract

Those charged with protecting the homeland through intelligence analysis, particularly in counterterrorism, must be capable of rapidly adopting innovative technologies to detect and prevent exploitation and disruption of vulnerable critical infrastructures. However, implementing these responses requires a highly skilled technical workforce that is continually provided with timely educational and training programs. Yet, questions remain regarding the technical aptitude necessary to respond to today's terrorism threats and the Department of Homeland Security's ability to provide consistent and rigorous standards for technology training and education. By surveying analysts, we examine what, if any, educational and training programs have been provided to adapt and remain technologically competitive and effectively utilize emerging technologies. We find a distinct need to focus on improvements that involve clarifying terms, building a technology and cybersecurity roadmap for analysts, allocating additional training time for employees, and building partnerships with private industry.

Keywords: intelligence analysis; counterterrorism; training and education; technology; cybersecurity; Department of Homeland Security

Introduction

Recent technological advances, such as deepfakes and artificial intelligence (AI), have clarified that homeland defense and security organizations face an ever-evolving security landscape with new threats, technological advances, and educational and training requirements with new demands. This raises the question of how these security agencies should prepare for and respond to high-tech and sophisticated technological threats through education and training. This question was asked by the Department of Homeland Security (DHS), specifically through the *Strategic Framework for Countering Terrorism and Targeted Violence*, which acknowledges the need to "prevent terrorists and other hostile actors" through the advancement of their workforce to be innovative, flexible, and capable of rapidly adopting technologies wherever they may arise [1].

This research, which is part of a multiyear study, conducted a thorough examination of DHS intelligence, counterterrorism training, and counterterrorism education to answer this question. The first year of this project began by evaluating the current trends in intelligence training and education for workforce development community-wide, in an effort to provide consistent and rigorous standards for DHS intelligence training and education [2]. As a result of that project, basic technology competency was identified as one of the six core competencies that every DHS intelligence analyst should possess to be effective in countering terrorism [2]. However, a greater understanding of which technologies contribute to DHS-focused intelligence analysis remains largely unexplored and understudied. Therefore, we sought to build on previous findings and recommendations by examining the impact of emerging technologies on DHS workforce needs, with a particular focus on counterterrorism and intelligence analysts. This research seeks to answer the following: How can DHS receive consistent, updated, and relevant technology workforce training for their intelligence and counterterrorism professionals?

This research first focuses on collecting current training and educational technology trends across the Intelligence Community (IC) and also tech-savvy companies within the private sector to identify, compare, and contrast the key technologies and technological competencies. We wanted to understand exactly what DHS may be missing in their technology and training needs to be current and effective to counter technology threats. This led us toward reviewing and comparing the academic literature and government documents in which technological competency is conceptualized. It examines the current talent shortage and highlights some of the key themes regarding existing efforts and challenges within academic and private sector training and education programs.

Furthermore, we review current efforts with technology introductions into the intelligence community, identifying challenges and successes with these efforts. Of particular note, there is an intense debate on if and how DHS is connected to the intelligence community. We have heard many perspectives connected to the Department of Defense (DOD) and the Central Intelligence Agency (CIA), where they consider DHS separate from the larger intelligence community. However, DHS maintains both Title 50 and Title 18 authorities, which gives them a unique position in the intelligence community [2]. For example, Title 50 sets the roles and responsibilities of the intelligence community, which governs its legal authorities abroad, to include covert action. Title 18, on the other hand, is the US Code that deals with federal crimes and criminal procedures, internal and within the jurisdiction of the USA, giving DHS both authority and jurisdiction to conduct domestic and international operations and activities.

Therefore, during our research, we queried and consulted both the larger intelligence community and DHS analysts specifically to gain both perspectives and provide a comparison. Our analysis and recommendations, however, focus specifically on DHS due to the scope of the research and the research question posed.

Second, we introduce and describe our methodology. We used interdisciplinary approaches to thoroughly assess, examine, and understand training and education in technological competency, which has allowed government security institutions and private industry to improve and transform the collection, analysis, and delivery of intelligence products.

Third, we present and discuss the findings from the analysis and data from multiple sources, including surveys created for both the government and private sectors; past and current interviews with experts working within DHS elements, as well as private sector technology companies; current reports capturing intelligence inefficiencies and gaps; congressional testimonies on the subject of training and equipping the intelligence workforce; and reports and recommendations on technological competency assessments and needs. We also reflect on the challenges related to technology training and education for DHS with intelligence and counterterrorism, including a lack of standardized definitions of technological competency differences in technology utilization in the private and government sectors, and increased digitization of training and education programs. Finally, these recommendations can be evaluated across other intelligence communities to improve the implementation of technology, cybersecurity training, and education.

Technological competency: from conceptualization to technology-based counterterrorism solutions

Previous research has demonstrated that a basic understanding of technology is required for all intelligent analysts to perform their jobs [2]. Our research understands that the DHS seeks to improve and standardize training and education for their future workforce, but it is clear that DHS staff members struggle with system functionality and the integration of technology into their analysis. Even more, there are additional deficiencies, as technology was not previously identified, prioritized, and integrated as a specific core competency in the existing DHS training and education programs [2]. However, being able to seamlessly access data across multiple distinct DHS information systems and databases and bring the merged data into additional technology-based analytical tools and applications is necessary for every DHS analyst. In addition, counterterrorism analysts must be knowledgeable and aware of the new and emerging technologies that both nonstate and state adversaries might use against the homeland to recruit, plan, and perpetrate terrorist attacks. Our research attempts to close the gap by understanding how technology should be incorporated and taught into DHS intelligence and counterterrorism sectors of the department. As presented above, there is an extensive concern in regard to the overall intelligence community to incorporate technology and cybersecurity competency into workforce needs, but we notice that DHS is largely absent from this conversation and effort. This could be due to numerous accounts, either due to their constant debate of being connected to the larger IC community in general and their split association of Title 50 and Title 18, due to the fact that their intelligence community is still new and developing. Regardless, this research sought to understand why these gaps still exist. Therefore, we pushed forward and asked questions of the IC community, DHS analysts, and even the private sector to understand why it might still exist and how to incorporate more technology competency into DHS.

Defining technological competency

The DHS workforce faces new challenges, including the technologization of their daily tasks, utilization of increasingly automated systems, and overall digitization of their skills and occupations. These analysts and practitioners are now facing a new threat landscape that includes cyberattacks, biotechnology, nanotechnology, quantum computing, and AI, among others, and agencies are struggling to keep up with a rapid technological shift [3, 4]. Similarly, state and nonstate actors have adopted information technology and the Internet to reach and recruit supporters, acquire knowledge and funds, and perpetrate attacks against the USA.

Consequently, to meet its mission and operational goals, the DHS leadership must consider defining and adapting talent needs, including the technological competence of the individuals responsible for intelligence and counterterrorism. However, pinpointing what has been done specifically in terms of technology is a bit of a challenge, and this is due to how technology is framed, defined, and discussed among the defense community, especially DHS. Therefore, understanding how technology competency is defined is an essential first step.

We approach the competency discussion by building on the National Academies' (including the National Academy of Sciences, the National Academy of Engineering, the Institute of Medicine, and the National Research Council) 2002 *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. In their follow-up 2003 *Information Technology in Responding to Terrorism* report, experts have already highlighted the importance of developing "authoritative, current-knowledge expertise and support regarding information technology" [5]. Two decades later, as threats multiply and grow in scope, impact, complexity, and technological sophistication, the IC is still faced with the question of how to produce intelligent analysts with adequate and appropriate technology skills and knowledge to counter terrorist attacks against the homeland, its critical infrastructure, electronic information assets, security, confidentiality, integrity, and the availability of its information systems.

We begin by defining some of the key terms that help us understand the conceptualization of technological competency necessary for the 21st-century intelligence analysts to work smarter using digital platforms and improve the quality and efficiency of their work. Marc Giget is credited with coining the term *technological competency* in his seminal study of developments in R&D management practices in major Japanese industrial corporations and the consequent integration of technological competencies into the strategic process of a company [6].

Arballo, Nunez, and Tapia argue that given the diversity of definitions, "technological competency can be understood as specific performance applied to different professional fields" [7]. When their argument is applied to the intelligence field, it means that intelligence analysts should have two types of competencies operating symbiotically and with their own logic: the professional field's specific competencies (such as subject matter expertise, critical thinking, collaboration, writing, communication) and technological competencies to process information, knowledge, and communication pertaining to the field.

The federal government has supported the integration of technology into curricula and instruction, but the responsibility of this training has become blurred [8]. Training for intelligence and counterterrorism has largely been an agency responsibility with academic augmenting with specialized programs [8, 9]. However, when you add technology competency into the mix, education and training can come from all sorts of entities [10, 11]. The biggest focus of both academic and federal government programs seems to be on information technology and cybersecurity as the two primary technology competencies. Title 40, Section 11101 (6) defines information technology as "any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency" [12]. Other government agencies, such as the National Association of Regulatory Utility Commissioners, developed their definitions as part of their cybersecurity primers for policymakers in charge of the state's electric, gas, water, communications, and transportation systems. This document conceptualizes information technology as "a discrete set of electronic information resources organized for collecting, processing, maintaining, using, sharing, disseminating, and dispositioning information" [13]. In addition, the International Standards Organization (ISO) has also developed a definition that is used in the field of learning, education, and training (LET) to facilitate international communication. According to ISO, information technology is a "set of one or more computers, associated software, peripherals, terminals, human operations, physical processes, information transfer means, that form an autonomous whole, capable of performing information processing and/or information transfer" [14].

In short, the majority of descriptions of information technology competencies focus on the knowledge and ability to utilize electronic equipment and applications that allow for the collection, sharing, and storage of digital information.

Cybersecurity technological competence, on the other hand, is about the knowledge required to protect the electronic information stored within those information technology systems. According to the Cybersecurity and Infrastructure Security Agency (CISA), cybersecurity is "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" [15].

Additional studies have demonstrated that although the availability of technological hardware and software tools improves the speed of information flow and reduces uncertainty by allowing analysts to cross-verify data, these technological tools will not always be utilized for a variety of reasons, including personal preferences and the institutional and cultural values of different agencies that often disincentivize information sharing and collaboration to claim ownership over the subject matter and resources [16]. Understanding both cybersecurity and information technology competencies within a larger IC context and its environmental constraints is important, as they shape the way intelligence analysts engage with and utilize different technologies in their workplaces.

Defining competencies and ensuring that intelligent analysts possess them does not guarantee that they will be integrated correctly or efficiently into their daily activities if tools are not trusted, and the organizational culture is not aligned to support greater integration of technology. Moreover, there is still a lack of scholarly conversation on establishing baseline information technology and cybersecurity abilities and defining the different levels of proficiency required for success in the field of intelligence analysis. In other words, there is still a lot of work left to define different levels of user competence necessary to adequately use and manage information technology and maximize its benefits in the workplace. As evaluated in a study by Arkin and O'Brien, information technology and technology-related concentrations are common concentrations by existing workers in the intelligence community [17]. However, security and intelligence-relevant curricula are not always adequately integrated in a manner that engages learners from nontechnical backgrounds [11]. In particular, when it comes to the evaluation of intelligence analysts' IT competence proficiency, it is not always clear what specific qualifications or levels of knowledge, skills, and abilities are required from job applicants. Previous research has defined basic technological competencies: the ability to use computerized data visualization and intelligence analysis tools; the ability to use a personal computer and its applications; the ability to use assistive software to interpret data and draw meaning from qualitative and quantitative data; and the ability to think critically about the use and integration of AI and machine learning into the processes and methods of scientific inquiry involving experimentation, observation, and quantitative analysis [2].

Black and Obradovic found that being proficient only in information systems or software, such as word processing or spreadsheets, as most US job descriptions suggest, is no longer adequate for intelligence or counterterrorism analysts [2]. As the recent Center for Strategic and International Studies (CSIS) brief argues, today, it is necessary to have "technical and tactical knowledge to understand foreign AI systems … capabilities and limitations of their own AI-enabled collection, targeting, and acquired data" as well as understand how adversaries might utilize other emerging technologies, such as biotechnology and quantum computing to achieve their strategic goals [18]. The same report also posits that we can achieve success only by tackling both analytic communities' preference for traditional tradecraft techniques and aversion to change, while simultaneously investing in greater integration of AI, OSINT, and TECHINT tools into analysis, and incentivizing technological competence training. This has been a challenge for all of the IC community and more than just a technology forefront, as expressed by research [9]. "Training has remained remarkably static amidst the big structural changes proposed by Presidential commissions and Congressional investigations over the last 20 years" [9], which holds true for technology education and training within the community.

Technological competency gap

For more than a decade, it has been clear that the federal government's mission and services cannot be achieved without investing in information technology and cybersecurity education to create a sustainable and robust workforce capable of engaging in both analysis and offensive and defensive operations. However, recent research has focused on understanding the new technologies necessary for different organizations, agencies, and components, rather than the skills that employees need to thrive in the new digital work environment [19]. DHS leadership must think about integrating these new technologies in a way that "can help *optimize* intelligence flows, *automate* mundane but vital processing tasks, *augment* analysts' sensemaking and critical thinking skills, and even *perform* certain types of analysis" [18]. Office of the Director of National Intelligence's (2019) *Augmenting Intelligence using Machines* (AIM) *Initiative Report* highlights the importance of AAA technologies (AI, process automation, and IC officer augmentation) as they transform missions and analysis. The report recognizes that to gain analytic superiority, there is a dramatic need to combine the private sector commercial AI applications "with IC-unique algorithms and data holdings to augment the reasoning capabilities of [our] analysts" [20]. Moreover, it underlines the increased competition for talent among agencies and against the private sector.

In fact, the report suggests making strategic workforce investments, such as training and retooling the existing workforce in skills necessary to work in an AI-augmented environment, restructuring its recruitment pipelines to include academic and private sector partnerships, developing more robust externship/internship programs, nongovernment-to-government rotations, sabbaticals, pregraduation hiring, and opening positions to foreign-born people and researchers to work on unclassified projects and domains, among others. The driving force behind this initiative was the notion that the IC, as a whole, must address its technologically competent talent pool to remain relevant and also keep pace with the information collected [21]. The DOD and specifically the Defense Advanced Research Projects Agency, has invested and sought to incorporate AI and advanced computing into their intelligence structure workforce, with this point further reasserted recently in the President's 2022 Budget, which strongly advocates a workforce that is "highly trained and equipped with modern-day technical skills in areas such as data science, cybersecurity, and artificial intelligence" [22, 23]. The White House has proposed adding $500 million to the federal Technology Modernization Fund, plus $9.8 billion for civilian cybersecurity programs. The challenges and concerns are echoed in Landon-Murray, which emphasizes the importance of developing today's IC workforce utilizing higher education institutions while also understanding the needs of the IC community [24]. To remain competitive, higher education institutions must consider the needs of the government, particularly for offensive curricula, such as research, surveillance, and tactical strategies [25].

What we find alarming, is the concern about the inability to keep up with technological innovation, and the demand for talent is not new [9, 21]. Ever since the *Comprehensive Cybersecurity National Initiative*, when President Barack Obama declared cyberthreats to be "one of the most serious economic and national security challenges we face as a nation," the federal government has been recommending strategic workforce development plans to address what technological competencies will be needed and how they will be obtained [26]. At the same time, a White Paper of the CSIS Commission on Cybersecurity for the 44th President titled "*A Human Capital Crisis in Cybersecurity*" raised alarm that "there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the Federal government" [27]. Further evidence of a talent shortage is the 2013 US Government Accountability Office report, which showed a vacancy rate of 22% within the DHS National Protection and Program Directorate's Office of Cybersecurity and Communications.

This report also suggests that some of the biggest reasons for such a high vacancy rate are the long period of time required to conduct security checks, low compensation compared to private sector openings, and a "lack of clearly defined skill sets or a unique occupational series for these positions" [27]. When the CSIS White Paper was written over a decade ago, the USA had only ∼1000 security specialists with the skills to fill between 10 000 and 30 000 positions. In 2021 (ISC)2, an international nonprofit organization that provides cybersecurity training and certification, reported in their annual "Cybersecurity Workforce Study" that despite a surge of 700 000 new cyber professionals, "the global demand for cybersecurity professionals continues to outpace supply—resulting in the cybersecurity workforce gap" [28]. At the time of that study, the country's total cybersecurity workforce was 716 000, but today, there are almost 600 000 vacant cybersecurity jobs, with ∼39 000 job openings in the public sector [29, 30]. Last year, as DHS reported >2000 cybersecurity vacancies, Secretary of Homeland Security Alejandro Mayorkas launched a "60-day Cybersecurity Workforce Sprint" that allowed the department to fill 200 of its vacancies, making it one of the largest cyber hiring efforts in its history [31].

The DHS was one of the first agencies that have taken steps to define skills, competencies, roles, and responsibilities for the federal cybersecurity workforce, along with the Chief Information Officers Council, National Institute of Standards and Technology (NIST), and Office of Personnel Management (OPM). However, even with hiring initiatives such as this, the public sector must compete with the private sector and its more generous compensation and benefits packages. As businesses expand their e-commerce services, the workforce seeks remote jobs, governments integrate cloud computing infrastructure, and the cyber skills gap becomes more apparent. The global cybersecurity market, in particular, is projected to reach $366.1 billion by 2028, making it one of the fastest-growing sectors in the world [32]. This forecast growth requires a highly skilled technical workforce to support innovation. Recent studies have found that as many as 82% of employers in eight countries reported a workforce shortage of cybersecurity professionals [33].

Other studies, including the Information Systems Security Association (ISSA) and the Enterprise Strategy Group (ESG), conducted a cooperative research project that found that "28% of cybersecurity professionals say that the cybersecurity skills shortage has had a significant impact on their organization, while 42% claim that their organizations have been impacted somewhat by the global security skills shortage" [34]. The respondents identified cybersecurity training as one of the key contributors to the workforce gap as "36% of respondents reported that they thought that their organizations should provide a bit more cybersecurity training, while 29% believe their organizations should provide significantly more training" [35].

Similarly, in terms of information technology skills, the US Bureau for Labor Statistics (BLS) predicts that the demand for talent will grow by 12.1% from 2019 to 2029, or 48 941 new jobs every year (2020) [36]. The most recent statistics demonstrate that ∼5 jobs exist for every software developer in the USA alone [37]. These numbers have been exacerbated due to the COVID-19 pandemic. Information technology talent shortage is now cited as the main barrier to the adoption of 64% of emerging technologies, compared to only 4% in 2020 [38]. Specifically, the same report demonstrated that companies are reluctant to adopt IT automation tools (75%) and digital workplace technologies (41%) because of talent availability. These dramatic talent challenges disrupt both private sector businesses and

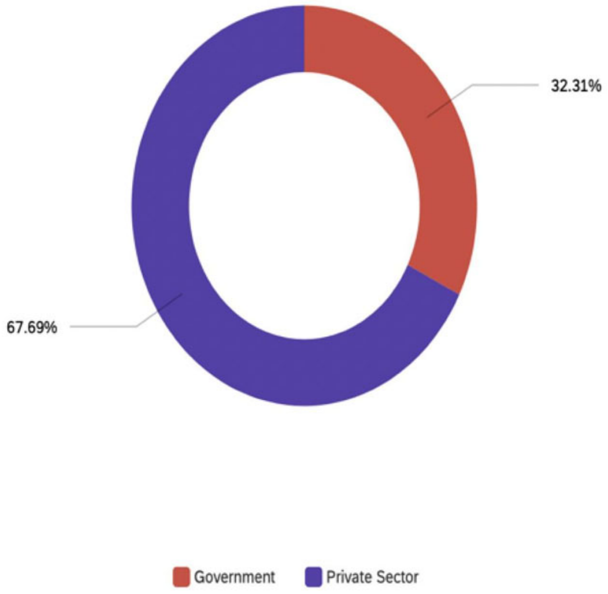

Figure 1: Survey response.

the way IC agencies prioritize and operate. More importantly, they pose a serious threat to national security [39].

A further challenge in keeping a DHS technology and cyber-ready workforce is the number of agencies that are turning to utilize technology to fill the gap in collection, exploration, and processing. Especially when many analysts in the security and intelligence sectors lack a technology background, but need to work with big data software tools and the outputs of algorithms [11]. "Performing this cognitive task has become a more daunting one for intelligent analysts. It has become more challenging due to an unprecedented increase in the sheer volume and velocity of unstructured and structured data generated by and correspondingly collected with open source and multiple classified platforms" [40]. Regen argues that leveraging high-performance computing and AI will help enhance the processing needed by intelligence agencies [40]. "January 2019, ODNI released a new strategy on the use of artificial intelligence technologies in US Intelligence" [41]. The ODNI report requested additional help from AI and automation to help the IC with data interpretation and decision-making. However, the problem still exists in using this technology when the human element is not being trained, educated, or even socialized to understand this technology. Our review of the literature confirmed that DHS was still struggling with just what and how to train their analysts on technology. In addition, the above review also provided us with a theoretical framework to understand the problem itself and review the accumulated knowledge, methods, and approaches to solve it.

Materials and methods

Our research combines both quantitative and qualitative data from surveys, quantitative analytics, past interviews, and comparative analyses. We opted to use surveys because they are an important data collection method for research and organizational quality improvement. We utilized both quantitative (using questions with numerically rated items) and qualitative (using open-ended questions) research strategies. Due to this being a multiyear study, we were also able to utilize our past 2021–2022 interviews, which included 17 intelligence professionals from multiple agencies (DHS, DOD, and Defense Intelligence Agency), DHS program analysts, and DHS leadership on technology to help direct data collection and comparative analysis. Most of our government participants that were contacted for the survey were professionally connected to the DHS due to the grant being funded by a DHS Center of Excellence, the National Counterterrorism Innovation, Technology, and Education (NCITE). Private industry, on the other hand, was contacted through personal contacts through LinkedIn and the snowball effect. We included a comparative analysis to broaden the research results, ensure triangulation because of the lack of survey responses, and help to truly understand the findings.

Survey construction

We utilized Qualtrics to ask questions from both the government and the private sector. The survey tool was used to specifically collect the experiences, behaviors, meanings, and interpretations of technology competency, technology use, and training and education of those in intelligence and counterterrorism functions at DHS, government positions, and private sector positions. We designed a survey consisting of 77 questions divided into seven categories.

Survey distribution and response rates

We distributed the survey to government and private sector contacts. Since our research is connected to NCITE, we utilized suggested government contacts from DHS key stakeholders in intelligence and counterterrorism, along with the names of our professional private sector technology network contacts. We included participants from both sectors to determine and examine the differences in technology preferences, required competencies, overall education, training quality, and satisfaction between the two. Private sector contacts were identified through professional networks and prior engagement with the lead investigator, co-lead investigator, and graduate students.

Survey requests were personally sent to 114 individuals from our complied list of public and private sector with 70 responses received. After controlling for incomplete responses, the final survey count was 61. The survey link was live from 20 January 2022 to 15 April 2022 and it allowed one response per email. Once opened, the survey had to be completed within 2 weeks, or responses would be voided. All survey responses were stored on a secure cloud site and assigned numbers to maintain the interviewees' anonymity throughout the analysis.

The respondents varied by industry, with the majority of the government sector respondents in the military and government and public service sectors and the majority of the private sector respondents in the finance and insurance and information services and data processing sectors. The average experience for respondents in the government sector was 14.9 years and 9.5 years for the private sector. Figure 1 shows a visual representation of our survey response rate, separating government respondents from private sector respondents.

The figure shows a significant difference in the participation rates as the private sector participants responded at a much higher rate than their government counterparts. We noticed this early in the study; therefore, we extended the survey deadline to allow additional time for government employees to participate. The research team interacted throughout the project with a DHS-focused working group, with its many high-level stakeholders who offered to disseminate the survey through their own contacts, further adding to our snowball effect. After this round, we noticed an increase in the number of government responses, but the distribution of responses stayed the same.

We conclude that there are several reasons why government employees did not participate in higher numbers, including survey fatigue, lack of trust in anonymity, and lack of incentives. In terms of "survey fatigue," it is well known that the government sector gives their employees surveys often, which discourages them from participating in optional surveys [42]. Second, according to the OPM, government employees might find such surveys untrustworthy, have concerns regarding the confidentiality of the information provided, and may expect retribution if they are critical of their employer. Finally, when a survey is voluntary, the ones who respond tend to be more interested in the topic and those who think that the survey will bring changes to their workplace [43, 44]. Other studies found that if there is no incentive, either cash or in-kind, some respondents may choose not to complete or participate in the survey [45]. They simply ignore the request, as they do not see the benefit either to themselves or to the participating organization.

While the survey received a response rate of 57% from both public and private sectors, we understood that most government employees were simply unwilling to discuss the main subject of this study: government-provided technology training. We did notice that those who responded held different positions and had varying degrees of expertise. As technology becomes more intricate, complex, interconnected, and ubiquitous, the lines between those who need some and a lot of experience or knowledge of emerging technologies become increasingly blurred. Therefore, we analyzed the survey results carefully and thoroughly. Instead of taking the results at face value and looking at the number of respondents, we compared the participants, their positions, sectors, and organizational affiliations. These data allowed us to focus more on the context of the answers than on the number of respondents.

Results

When initiating this research, we specifically wanted to answer "how can DHS receive consistent, updated, and relevant technology workforce training for intelligence and counterterrorism analysts?" What we discovered were four key findings that outline the challenges DHS faces preventing them from success, and why they are essentially "behind the curve" in this area. The section below presents a chart summarizing each of those key findings, followed by an extended discussion of the supporting evidence collected during the research.

Differing terminology and standardizations

We found through our governmental guidance documents and literature data collection that technological competency, training, and education were not necessarily the same across all government agencies and private sector companies. This lack of standardized definitions and approaches complicates the writing and advertising of job postings, the development and implementation of government and academic curricula, and the cross-referencing required DHS analyst qualifications. It is clear that DHS staff continue to struggle with system functionality and the integration of technology into their analysis. There are deficiencies, as there are no mechanisms for the identification, prioritization, and integration of this competency into training and education. More specifically, DHS analysts communicated that being able to collect, analyze, and interpret data from up to 27 distinct DHS information systems and databases was a requirement for core competencies [2]. Furthermore, we discovered that many academic intelligence study programs have already integrated STEM-related courses into their offerings based on intelligence requirements and ODNI needs assessments. Therefore, adding "technology" as a core competency was identified as a reasonable contribution to the list of skills an analyst needs to have to perform their job effectively. However, subsequent research has found that different guidance documents lack a comprehensive definition of "basic technological competency" and the corresponding proficiency levels. While this emphasized the need to provide "specialized" technology training for analysts to gain more complex skills that were growing in demand for counterterrorism and targeted violence analysis, our analysis here revealed an additional dimension that is a need to problematize the difference between "basic technology training and education" and "specialized technology training and education" as the gap between the two was initially understood to be much wider than it actually is. Although Finding Two suggests that more training and education in technology is available and growing for agencies such as DHS, it is not clear how to separate courses into basic and advanced training and identify the training courses required for core competency in the intelligence and counterterrorism professions.

To address this issue, we reviewed current technology education and training efforts across government agencies and academic institutions. We found differences between terminologies and how they are used within courses, such as cybersecurity, cyber defense, technology, and data analysis. Furthermore, government agencies have created organizations to build educational curricula and courses specifically for technology. The two most prominent organizations in cybersecurity education are the National Initiative for Cybersecurity Education and National Cybersecurity Workforce Framework. Through the NIST, the National Initiative for Cybersecurity Education (NICE) is a partnership between multiple sectors to better educate cybersecurity professionals and foster innovation among governments, academia, and industry partners. However, there is no mapping for these courses to the agencies or career fields, leaving analyst confused on what they need to do to fulfill their technology competencies.

Training is available, but which one?

During our research collection section, we found that the DHS provides both technological and cybersecurity training and education through in-house courses or their operational components: CISA. This agency, which was established in 2018, succeeded the DHS's National Protection and Programs Directorate (NPPD). CISA was specifically designed to coordinate collaborative partnerships to "lead[s] the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure," in order to "…connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people" [46].

CISA created the National Initiative for Cybersecurity Careers and Studies (NICCS) to advance the nation's cybersecurity workforce through information partnerships, collaborative education, and studies. NICCS was created to "promote[s] cybersecurity awareness, training, education, and career advancement with the added goal of broadening the Nation's volume of cybersecurity professionals in the workforce," and "to provide the nation with the tools and resources necessary to ensure the Nation's workforce has the appropriate training and education in the cybersecurity field" [47].

Outside the NICCS, the DHS and government partners could utilize a vast array of online course content from private sector providers and e-learning outlets. Companies such as Udemy, Coursera, and edX provide thousands of free or low-cost courses on various subjects, including quantum computing and machine learning. NIST maintains an extensive list of free, low-cost cybersecurity courses. Tech leaders such as IBM, Microsoft, and LinkedIn provide low-cost

Table 1: Key findings for technology training and education.

Finding One	Technological competency training and education terminology is defined differently among government agencies and the private sector, making standardization of training requirements, curriculum, and qualification, as well as private–public partnerships complicated and prevent DHS from building a comprehensive training plan on this technology for their employees.
Finding Two	Technological competency training and education are available and widely provided by government entities for DHS, but there is a lack of understanding regarding which training is the best to develop workforce in counterterrorism and targeted violence, and how to track this training within the career field. This overwhelming amount of training with a lack of direction prevents DHS employees and leadership to understand which training would be best for their career and job position needs.
Finding Three	There is a distinct lag in maintaining up-to-date content related to the latest technological developments and emerging technologies as compared to the private sector. The private sector places a greater emphasis on modernized training and education due to higher financial stakes and risks. The lag prevents DHS from staying above the curve in technology training like their private counterparts.
Finding Four	The technology competency training and education, both within government and private sectors, are moving toward online delivery to include self-paced training, online courses, and webinars by academia, contractors, or technology vendors. This has helped DHS train their employees due to time and budget constraints but also impacts the ability to share or discuss classified information.

learning content that similarly covers a wide range of topics, although they mostly focus on the products and services, which the specific company provides. CISA provides an array of cybersecurity and critical infrastructure courses and training programs that would be useful in filling the gaps in these respective fields. The final training resource is the National Science Foundation's Advanced Technological Education (NSF-ATE) program. This program selects 2-year educational institutions across the country to develop innovative approaches to educate skilled technicians in industries such as advanced manufacturing, biotechnology, and autonomous technology. Each ATE center develops training programs, curriculum resources, and learning modules, most of which are readily downloadable or offered at a low cost.

Our survey found that, even with all these government-sponsored, paid, and available resources, 73% of government respondents had never received any CISA training and 55% of government respondents were not aware of the opportunity to take CISA training. Essentially, DHS employees generally do not know about or pursue CISA training to enhance their technological training.

Even through data collection of all the courses offered, the research found that some government respondents commented that they "were on their own to seek training" or that they simply needed training in the basic technological functions that they perform everyday for their job. For example, respondents commented that they could greatly benefit from training in Microsoft Word, Excel, and Teams, which contributed to their day-to-day functioning. Furthermore, training is not always equitable, meaning that leaders may receive specialized education and analysts must fend for themselves, and there is a lack of money to train on software and equipment.

Furthermore, when government participants were asked if they would benefit from additional training in emerging technologies, there was consensus that they would benefit from more training on any of the topics listed in the question set (AI, cloud computing, etc.). Only a few indicated that they had received any training or education in this technology.

One result from the survey that is puzzling is the number of government employees who agree that their employer does utilize an educational management system to advertise and track their training and education, but does not specifically track technology training and education. Some respondents requested that technology training should be mandated to address this awareness problem. Our respondents confirmed that there is a plethora of opportunities for DHS employees to take technological and cybersecurity training to enhance their skills and specialization for counterterrorism and targeted violence. What remains the issue is "which training is best for DHS intelligence and counterterrorism professionals at the core competency level and next level up?" Meaning, of the training offered and presented by CISA, government agencies, and private functions, which training should an agent focus on for intelligence and counterterrorism?

Private industry above the curve

Our analysis from survey results and data collection revealed that there is a clear understanding that the government and private sectors have distinct roles in technology and cybersecurity. According to General Michael Hayden, former director of the National Security Agency (NSA) and CIA:

> The main effort for American cyber defense is the private sector. And the role of government is to do those things that only the government can do, and then for the other 98 percent of the problems, we have is to be an enabler for the private sector to be the best that we can be [48].

Unfortunately, the government is not always ready to provide a strong response and can sometimes be caught behind the curve in terms of technology. However, the private sector can, on its own accord, have different approval processes, policies, and functions that allow for more freedom than government organizations. It is beneficial for the government to allow the private sector more freedom to respond to cyberattacks. The private sector has infrastructure and expertise that allow it to maneuver in cyberspace and defend and respond at a faster pace. More recently, public and private sectors have been able to collaborate and identify best practices for partnerships. This collaboration moves away from the government-led approach and fosters partnership, and encourages partners to share leadership, appreciate each other's perspectives, and develop goals and objectives together.

The main purpose of a public–private partnerships is to foster synergy and collaboration between the government and the private sector [49]. A combination of collaboration and mutual responsibility is believed to create successful partnerships. However, entities in this partnership face challenges. Challenges include defining and working along identified and clear roles and trust among partners. Regardless of technological training and educational needs, both the government and private sectors challenge each other to fill obvious gaps and seek to benefit each other. One of the clear gaps identified through the survey and comparative analysis was the government's failure to keep up with the latest developments and emerging technologies. We found that 90% of private respondents claimed that their employer provides opportunities to attend webinars and/or

Table 2: Recommendations for key findings.

	Finding	Recommendation
One	Technological competency training and education terminology is defined differently among government agencies and the private sector, making standardization of training requirements, curriculum, and qualification, as well as private–public partnerships complicated and prevent DHS from building a comprehensive training plan on this technology for their employees.	We recommend developing a roadmap for basic and specialized technological competency training for DHS intelligence and counterterrorism analysts to ease the confusion about which competencies are required for DHS analysts. A draft roadmap has been produced as part of this study and is currently under review.
Two	Technological competency training and education are available and widely provided by government entities for DHS, but there is a lack of understanding regarding which training is the best to develop workforce in counterterrorism and targeted violence, and how to track this training within the career field. This overwhelming amount of training with a lack of direction prevents DHS employees and leadership to understand which training would be best for their career and job position needs.	We recommend that DHS and its components should increase their annual required training and education time allocation to include a focused approach for areas aligned with basic and specialized technology and cybersecurity education above their already allotted time for training.
Three	There is a distinct lag in maintaining up-to-date content related to the latest technological developments and emerging technologies as compared to the private sector. The private sector places a greater emphasis on modernized training and education due to higher financial stakes and risks. The lag prevents DHS from staying above the curve in technology training like their private counterparts.	We recommend that DHS promote private sector engagement and training, with a concentrated effort on government–private industry engagement programs or job shadowing.
Four	The technology competency training and education, both within government and private sectors, are moving toward online delivery to include self-paced training, online courses, and webinars by academia, contractors, or technology vendors. This has helped DHS train their employees due to time and budget constraints but also impacts the ability to share or discuss classified information.	We recommend that DHS centers of excellence (COEs) produce the required training and education modules that can be adopted, modified, and distributed online by the requesting agencies where specific gaps exist.

conferences to keep up-to-date on the latest industry developments, compared to 62% of government survey respondents. Furthermore, 62% of private respondents say they receive consistent and updated education on emerging technology, compared to 55% of government respondents stating they do not receive consistent and updated education on emerging technology.

Additionally, 51% of private respondents believe their technology is updated periodically throughout the year, while 43% of government respondents believe their technology is updated only every few years. This signals that private respondents are fully aware that they and their company need to be up-to-date on technology.

We found that the private sector places more emphasis on staying up-to-date on training and education due to the risk of monetary loss. Simply, the motivation between government and private sector tech companies is different because the mission is different. Government entities focus more on defending the homeland and its interests, rather than on loss or gain of revenue. This forces each entity to prioritize differently and focus their employees' efforts on that prioritization.

For example, many respondents in past interviews claimed that there was a lack of time and attention given to training and education because of mission requirements. The DHS wanted employees to focus more on completing mission requirements rather than on professional development and training. Based on our survey responses from the private sector, this seems to be the opposite; instead, private sector leadership prioritizes the creation, adoption, and tracking of employees' basic and specialized technology training to improve their organization.

We find that the private sector appears to be more efficient in terms of engaging its employees with training opportunities and/or requirements and modernizing its emerging technology training. Private respondents are more adept at updating their employee-used technology throughout the year, illustrating the private sector's willingness and ability to invest in improved technology and related training. Private sector respondents seem to have more investment strategies in terms of offering training opportunities in the form of webinars, conferences, and other educational opportunities than their public counterparts.

In sum, this research finds that even though the government uses the private sector to fulfill its lack of ability to stay updated on the latest developments and with emerging technology, there needs to be a balanced approach to government–private partnerships within the field of technology. If the government relies strictly on in-house training, then this can cause a serious deficit within training and education. Likewise, if the government continues to devalue technology training and education, essentially not promoting the use or advancement of their analysts and agents, this too will cause a significant deficit in the DHS intelligence and counterterrorism workforce.

Moving technology training and education online

The last 2 years have witnessed an unprecedented amount of training and education moving to online platforms and delivery owing to the impact of COVID. The past interviews and current survey results noted that COVID enhanced government responses to moving online and through distance learning [2]. However, intelligence agencies and government entities are not alone moving toward online learning or introducing innovative training to meet employee demands. According to a 2019 survey of employees of large US enterprises, 91% use video technology for learning [50]. The same survey found that interactive videos were more effective in maintaining learners' attention. On-demand video learning is preferred because it allows learners to learn at their own pace on their own time without relying on external human supervision. It may also be a cost-effective and scalable training format. According to Baer, microlearning training involves short online demonstrations or tutorials that use spaced repetition, a retention-boosting method for breaking down learning topics into more manageable pieces and repeating them with adequate spacing between lessons [51]. For example, Google launched a free application called Google Primer in 2014. The app has 5-minute interactive lessons designed to teach digital marketing and business skills to small-to-medium business owners or startups.

Furthermore, AI and virtual reality (VR, which includes extended reality, augmented reality, and immersive learning) can facilitate a more personalized learning experience, provide customized learning content, visualize a new environment, and use tailored or adaptive scenarios [52]. Common themes across these training trends are that the future of learning in the workplace is digital and personalized to maximize retention and efficacy. However, these forms of learning are more generalized than concrete examples of how the private sector ensures that its staff are adequately prepared/skilled to do their jobs.

Companies invest in innovative ways to lead and create new career pipelines to attract entry-level talent, delivered through online courses and academic degree partnerships. AT&T, Amazon, Microsoft, Raytheon Technologies, and Deloitte are a few of those companies that are moving toward providing their own online technological training or partnering with academic programs [53]. As technology training is increasingly moving online through companies, we found similarities in the survey results for both the government and private sectors. Many respondents stated that online training, courses, and webinars were common educational avenues. Only a few said that online training was required and one said that they had not received any training on the systems they worked on. We asked both the government and private sector "How is your training generally delivered?" First, in the private sector, most responses highlight the existence of some form of digital training. With private sector training, most are online or virtual, a variety of training methods were used including in-person, conferences, product demonstrations, and workshops. COVID had an impact on in-person training and several respondents mentioned remote learning over Zoom or Teams. While some noted that they often collaborate with federal or commercial training providers, others said that they would never do one or the other.

In sum, regardless if employees are requesting online training or not, both private and government entities are moving their technology training online or through some type of artificial-augmented training. If DHS or the government resists this type of training, results could limit their recruitment and retention within the field of technology.

Discussion

Based on these findings, we provide a few recommendations for the homeland security enterprises to advance their workforce development and educational components in the fields of technology and cybersecurity. These recommendations are matched to the previous Findings Table, to map and mitigate the gaps and help answer "how" DHS can receive consistent, updated, and relevant technology workforce training and education.

First, we recommend developing a roadmap for basic and specialized technological competency training for DHS intelligence and counterterrorism analysts. The current workforce faces challenges in understanding technology training pathways, and resources provided by NICCS and the Workforce Framework for Cybersecurity (NICE Framework) can provide a starting point for building and aligning knowledge, skills, and abilities for intelligence and counterterrorism professionals in DHS. We found roadmaps and recommendations from academic COEs on technology courses and curricula; however, a roadmap for specifically DHS intelligence and counterterrorism is lacking. As a result of this finding, our research produced a draft technology and cybersecurity curriculum roadmap that connected certain skills offered in existing courses. Utilizing active and current courses to meet training requirements would improve resources and meet analysts' demands. This technology and cybersecurity roadmap is currently being circulated within DHS as part of the larger research project but may be published shortly.

Second, DHS and its components should increase their annual required training and education time allocation to include a focused approach for areas aligned with basic and specialized technology and cybersecurity education. We found that the DHS workforce can receive consistent, updated, and relevant technology training as long as there is an increase in allocated time. Private companies specifically allocate time and resources to ensure that analysts advance their education and workforce development. Private companies have different educational philosophies from those of the government sector, and if their analysts are untrained or stagnant in their ability to compete with other companies or defend against their systems, the company will go out of business or experience a major revenue loss. The comparison and compatibility of these two sectors are key to understanding and developing the way forward and improving the DHS's technological capabilities, designing recruitment and training programs. The DHS will need to make a stronger effort to allocate additional training time for its employees to gain technological competency, in addition to already allotted core competencies.

Third, we found that technologies from the private and commercial sectors are vital in helping the DHS workforce understand the potential areas related to professional development. This is because of the speed and agility of the private sector and investments in technology R&D. Even if the government is never able to stay up with emerging technologies, ensuring that there is a viable and existing partnership with the private sector is more important and advantageous. A DHS can benefit from the private sector through its ability to incentivize and promote training, which is of vital importance within its organization. This means a concentrated effort on government–private industry engagement programs or job shadowing. The DOD and other agencies commonly practice engagement to train their program managers in the best practices used by the industry. Likewise, the DHS Office of Intelligence and Analysis has a private sector engagement program whose mission is to ensure that critical private sector infrastructure owners and operators are equipped with information to fulfill their mission, but these programs are focused on information exchange rather than professional development. If training and education time is increased, along with personnel development through engagement or job shadowing, this would significantly improve DHS's consumption of advanced training in technology.

Finally, DHS should collaborate with COEs to produce core competency training and education modules, especially in technologies that can be adopted, modified, and distributed online according to their training requirements. We found that technology training and education delivery formats, in both the government and private sectors, are moving toward online platforms, self-paced training, online courses, and webinars by academia, contractors, and technology vendors. Many participants expressed mixed opinions on this trend but agreed that this development was due to a lack of funding or time allocated to training and education. Training conducted through an online medium can significantly ease or eliminate the constraints faced by government and private sector employees. However, the same participants expressed the continued need to conduct training in person, either due to security classifications or due to the need to work more with students in person.

We discussed this finding with the participants, with the intent of gaining further feedback on their needs as a training department and how they might be impacted by this trend. Through these conversations, we learned that a recommendation should be made for COEs to produce the required training and education modules that can be adopted, modified, and distributed online by the requesting agencies. This collaboration should focus on integrating intelligence core competency subjects and training modules provided by specialized COEs. This curriculum development resource could also assist DHS in obtaining continuously updated training materials in technology and cybersecurity disciplines that can be tailored to their individual departments and personnel. Furthermore, these modules could provide a training and education baseline for other government training and education departments, particularly as they pertain to core competencies. The training modules can also be taught in person by a training manager to address the classification issues experienced by different components and agencies.

In summary, our findings indicate a distinct need to focus on improvements, specifically in the technological escort of intelligence and counterterrorism. These findings and recommendations may apply across other sectors of defense or agencies focused on intelligence and counterterrorism.

Acknowledgements

We are deeply grateful to the undergraduate and graduate students who assisted us in this research project, which was the result of a larger research project for the National Counterterrorism, Technology, and Education (NCITE) Center of Excellence, generously funded by the Department of Homeland Security.

Author contributions

Michelle Black (Conceptualization [lead], Formal analysis [equal], Funding acquisition [lead], Methodology [lead], Supervision [lead], Writing – original draft [equal], Writing – review & editing [equal]), Lana Obradovic (Data curation [lead], Investigation [lead], Validation [equal], Writing – original draft [equal], Writing – review & editing [equal]), and Deanna House (Data curation [equal], Formal analysis [lead], Investigation [equal], Visualization [lead], Writing – original draft [equal], Writing – review & editing [equal])

Supplementary data

Supplementary data is available at the *Journal of Cybersecurity* online version of the manuscript.

Conflict of interest: The authors report that there are no conflict of interests to declare.

Funding

The material in this article is based on the work supported by the US Department of Homeland Security under grant award number, 20STTPC00001 02-01. The views and conclusions included here are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the US Department of Homeland Security.

References

1. Department of Homeland Security (DHS). *Strategic framework for countering terrorism and targeting violence*. 2019;2. https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf (19 December 2023, date last accessed).
2. Black M, Obradovic L. Strengthening DHS intelligence analysis education: core competencies, gaps and challenges. *J Polic Intell Count Terror* 2022;**17**:1. https://doi.org/10.1080/18335330.2022.2069475.
3. Zegart A, Morell M. Spies, lies, and algorithms: why U.S. intelligence agencies must adapt or fail. *Foreign Aff* 2019. https://www.foreignaffairs.com/united-states/spies-lies-and-algorithms (20 December 2023, date last accessed).
4. Zegart AB. Threats never sleep: we still haven't done enough to prevent another 9/11. *Hoover Digest* 2022;**1**:138–44.
5. National Academies of Sciences, Engineering, and Medicine. *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*. Washington, DC: The National Academies Press, 2003, 3. https://doi.org/10.17226/10640.
6. Giget M. Technology, innovation and strategy: recent developments. *Int J Technol Manag* 1997;**14**:613–34.
7. Arballo NC, Nunez MEC, Tapia BR. Technological competencies: as systematic review of the literature in 22 years of study. *Int J Emerg Technol Learn* 2019;**14**:4.
8. Marrin S. Training and educating U.S. intelligence analysts. *Int J Intell Counterintell* 2009;**22**:131–46.
9. Chang W, Tetlock P. Rethinking the training of intelligence analysts. *Intell Natl Secur* 2016;**31**:903–20.
10. Ramsay J, Macpherson A. The integration of statistical learning in intelligence education: is the academy equipping tomorrow's intelligence professionals to analyze data-centric threats? *J Polic Intell Count Terror* 2022;1–19.
11. Coulthart S, Hossain MS, Sumrall J. *et al*. Data-science literacy for future security and intelligence professionals. *J Polic Intell Count Terror* 2023. https://doi.org/10.1080/18335330.2023.2187705.
12. Federal Property and Administrative Services. Title 40 United States Code (U.S.C.), 11101- Definitions, Information Technology Management. https://www.law.cornell.edu/uscode/text/40/11101 (19 December 2023, date last accessed).
13. Keogh M, Thomas S. *Cybersecurity: a primer for state utility regulators, version 3.0*. National Association of Regulatory Utility Commissioners, 2017, p. 33. https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F (19 December 2023, date last accessed).
14. International Organization for Standardization (ISO). *ISO/IEO 2382-36. Information technology for learning, education and training*. International Electrotechnical Commission (IEO), 2019. https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html (20 December 2023, date last accessed).
15. Cybersecurity and Infrastructure Security Agency (CISA). *Cybersecurity career paths and progression*. 2019a. https://niccs.cisa.gov/sites/default/files/documents/pdf/cybersecurity%20career%20paths%20and%20progressionv2.pdf?trackDocs=cybersecurity%20career%20paths%20and%20progressionv2.pdf (1 January 2024, date last accessed).
16. McNamara LA, Turnley JG. *An Ethnographic Study of Culture and Collaborative Technology in the Intelligence Community*. AlbuquerqueNM:Sandia National Lab, 2007.
17. Arkin WM, O'Brien A. The most militarized universities in America: a VICE News investigation. *Vice News*, 6 November 2015. Retrieved online on 20 July 2023 from https://www.vice.com/en/article/j59g5b/the-most-militarized-universities-in-america-a-vice-news-investigation.
18. Katz B. *The analytic edge: leveraging emerging technologies to transform intelligence analysis*.CSIS. 2020. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201008_Katz_Analytica_Edge_0.pdf (19 December 2023, date last accessed).
19. Kozanglu DC, Abedin B. Understanding the role of employees in digital transformation: conceptualization of digital literacy of employees as a multi-dimensional organizational affordance. *J Enterp Inf Manag* 2020;**34**:1649–72.
20. Office of the Director of National Intelligence (ODNI). The augmenting intelligence using machines (AIM) initiative: a strategy for augmenting

intelligence using machines. *Report*. 2019. https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2019/3286-the-aim-initiative-a-strategy-for-augmenting-intelligence-using-machines (19 December 2023, date last accessed).

21. Regens J. Augmenting human cognition to enhance strategic, operational, and tactical intelligence. *Intell National Secur* 2019;**34**: 673–87.
22. Vogel K, Reid G, Kampe C, Jones P. The impact of AI on intelligence analysis: tackling issues of collaboration, algorithmic transparency, accountability and management. *Intell National Secur* 2021;**36**:827–48.
23. The White House. President's Budget FY22, information technology and cybersecurity funding. 2021, 239. https://www.whitehouse.gov/wp-content/uploads/2022/03/ap_16_it_fy2023.pdf (19 December 2023, date last accessed).
24. Landon-Murray M. Big data and intelligence: applications, human capital, and education. *J Strateg Secur* 2016;**9**:92–121.
25. Dawson M. National cybersecurity education: bridging defense to offense. *Land Forces Acad Rev* 2020;**25**:68–75.
26. The White House. *The Comprehensive National Cybersecurity Initiative*. 2009. https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative (20 December 2023, date last accessed).
27. Evans K, Reeder F. *A human capital crisis in cybersecurity: technical proficiency matters*. CSIS, 2010, 24. https://www.csis.org/analysis/human-capital-crisis-cybersecurity (20 Decemeber 2023, date last accessed).
28. International Information System Security Certification Consortium (ISC)2. A resilient cybersecurity professional charts the path forward: (ISC)2 cybersecurity workforce study. 2021, 20. https://iapp.org/media/pdf/resource_center/ISC2_Cybersecurity_Workforce_Study_2021.pdf (20 December 2023, date last accessed).
29. Crumpler W, Lewis JA. *The cybersecurity workforce gap*. Center for Strategic and International Studies (CSIS), 2019. https://www.csis.org/analysis/cybersecurity-workforce-gap (19 December 2023, date last accessed).
30. CyberSeek. Cybersecurity jobs heat map tool. 2022. https://www.cyberseek.org (19 December 2023, date last accessed).
31. Westbrook C. *DHS sprint to hire cybersecurity professionals*. Federal Career Connection, 2021. https://www.federalcareerconnection.org/blogs/dhs-sprint-to-hire-cybersecurity-professionals (20 December 2023, date last accessed).
32. Kennard J. Nine remote working trends to look out for in 2022 and 2023. *Unleash*, 19 October 2022. https://www.unleash.ai/future-of-work/remote-working-trends/ (19 December 2023, date last accessed).
33. Petruzzelli E, Sharma N. Closing the gaps in cybersecurity. *Chem Eng Prog* 2019;**115**:35–9.
34. Oltsik J. *The life and times of cybersecurity professionals 2020, a cooperative research project by ESG and ISSA*. The Enterprise Strategy Group Research Report, 2020, 36. https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf (20 December 2023, date last accessed).
35. Oltsik J. *The life and times of cybersecurity professionals 2020, a cooperative research project by ESG and ISSA*. The Enterprise Strategy Group Research Report, 2020, 23. https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf (20 December 2023, date last accessed).
36. U.S. Bureau for Labor Statistics (BLS). *Occupational Outlook Handbook*. 2020. https://www.bls.gov/ooh/computer-and-information-technology/home.htm (19 December 2023, date last accessed).
37. Jebaraj D. Why you should rethink the sources of untapped tech talent. 2022. *Forbes: Technology Council*. https://www.forbes.com/sites/forbestechcouncil/2022/06/07/why-you-should-rethink-the-sources-of-untapped-tech-talent/?sh=fd8c3743fa0c (19 December 2023, date last accessed).
38. Gartner. Gartner survey reveals talent shortages as biggest barrier to emerging technologies adoption. *Press Release* 2021. https://www.gartner.com/en/newsroom/press-releases/2021-09-13-gartner-survey-reveals-talent-shortages-as-biggest-barrier-to-emerging-technologies-adoption (20 December 2023, date last accessed).
39. Raytheon. What We Do. 2016. https://www.rtx.com/raytheon/what-we-do/cyber/what-we-do (1 February 2024, date last accessed).
40. Regens J. Augmenting human cognition to enhance strategic, operational, and tactical intelligence. *Intell National Secur* 2019;**34**:673–87.
41. Vogel K, Reid G, Kampe C, Jones P. The impact of AI on intelligence analysis: tackling issues of collaboration, algorithmic transparency, accountability and management. *Intell National Secur* 2021;**36**: 827–48.
42. Office of Personnel Management [OPM]. *Policy, data, oversight*. 2022. https://www.opm.gov/policy-data-oversight/data-analysis-documentation/employee-surveys/ (19 December 2023, date last accessed).
43. Donald MN. Implications of nonresponse for the interpretation of mail questionnaire data. *Public Opin Q* 1960;**24**:99–114.
44. Rogelberg SG, Luong A, Sederburg ME, Cristol DS. Employee attitude surveys: examining the attitudes of noncompliant employees. *J Appl Psychol* 2000;**85**:284.
45. Ryu E, Couper MP, Marans RW. Survey incentives: cash vs. in-kind; face-to-face vs. mail; response rate vs. nonresponse error. *Int J Public Opin Res* 2006;**18**:89–106.
46. Cybersecurity and Infrastructure Security Agency (CISA). *What is cybersecurity?* 2021. https://www.cisa.gov/news-events/news/what-cybersecurity (1 February 2024, date last accessed).
47. National Initiative for Cybersecurity Careers and Studies (NICCS). About NICCS Website. 2022. https://niccs.cisa.gov/about-niccs#:∼:text=NICCS%20promotes%20cybersecurity%20awareness%2C%20training,cybersecurity%20professionals%20in%20the%20workforce (19 December 2023, date last accessed).
48. Healey J. Who's in control: balance in cyber's public–private sector partnerships. *Georget J Int Aff* 2017;**18**:120–30. https://doi.org/10.1353/gia.2017.0044.
49. Osborne S. *Public–Private Partnerships*. London: Routledge, 2000.
50. Kaltura. *Video and learning at work: the state of video in the enterprise 2019*. 2019. https://corp.kaltura.com/wp-content/uploads/2019/11/The_State_of_Video_in_Enterprise_2019.pdf (19 December 2023, date last accessed).
51. Baer S. Microlearning: the future of professional development. Forbes 2020. https://www.forbes.com/sites/forbeshumanresourcescouncil/2020/03/19/microlearning-the-future-of-professional-development/?sh=6026574e7faf (19 December, 2023, date last accessed).
52. Carrel-Billiard M, Guenther D, Rosa N, Taylor K. Engage, immerse and inspire with extended reality: immersive learning with XR. Accenture 2021. https://www.accenture.com/_acnmedia/PDF-164/Accenture-Immersive-learning.pdf (19 December 2023, date last accessed).
53. Henry-Nickie M, Frimpong K, Sun H. Trends in the information technology sector. Brookings Research Report. 2019. https://www.brookings.edu/articles/trends-in-the-information-technology-sector/ (19 December 2023, date last accessed).