2023 IEEE 17th International Conference on Application of Information and Communication Technologies (AICT) | 979-8-3503-0356-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/AICT59525.2023.10313162

The GapApp: Matching Military Occupations and Civil Jobs in Cyber Security for Women

Callie Balut, Rachelle S. Heller, Costis Toregas,
Rabaab Dhingra, Amarachi Elekeokwuri, Cora Sula
School of Engineering and Applied Science (SEAS)
The George Washington University
Washington, DC, USA
sheller@gwu.edu, toregas1@gwu.edu

Araz Yusubov
School of IT and Engineering (SITE)
ADA University
Baku, Azerbaijan
ayusubov@ada.edu.az

***Abstract* —This paper describes the activities and results of a George Washington University – USA Department of Defense Cyber Scholarship Program capacity building project during the 2022 academic year. In particular, the report provides information about the design and development of the GapApp, an application based on the outcome recommendations of the May 2021 conference. The GapApp is intended to streamline and to make accessible the multitude of competing information streams for careers, especially in the high demand field of cyber security to active women military nearing separation from the service. The existing workforce role and skill taxonomies in cyber security and military were studied, a technique for mapping one to another and evaluating the match was proposed. A working pilot application on a platform that can be ported to a mobile phone was successfully demonstrated.**

Keywords —career transition, cyber security, computer security, women's issues, military operational specialties, cyber work role, mobile applications

I. INTRODUCTION

"Closing the Gap: A Department of Defense (DoD) Conference on Reentry for Women Veterans into Cybersecurity Careers" [1] addressed the crucial need to fill the exponentially growing cyber security gap (whether it is a talent gap of skilled cyber security workers or a gap in the time between jobs in the military and the cyber workforce), as well as to address the gender imbalance in the field. In order for the USA to remain a world leader in various fields of science and technology, a robust and educated cyber workforce is required.

A. Literature Review

The Center for Strategic and International Studies (CSIS) notes in [2] that "a recent CSIS survey of IT decision makers across eight countries found that 82 percent of employers report a shortage of cyber security skills, and 71 percent believe this talent gap causes direct and measurable damage to their organizations." The report refers to CyberSeek, an initiative funded by the National Initiative for Cybersecurity Education (NICE), which estimated the shortage of almost 314,000 cyber security professionals as of January 2019 in the USA, while the country's total employed cyber security workforce was just 716,000. "According to data derived from job postings, the number of unfilled cyber security jobs has grown by more than 50 percent since 2015. By 2022, the global cyber security workforce shortage has been projected to reach upwards of 1.8 million unfilled positions."

While others [3] have indicated possible cohorts to fill these positions, such as under-represented minorities or green card holders, women veterans may be better positioned to fill this gap. Compared to the general population, veterans bring extensive technical skills to the marketplace [4]. Women, who have taken time off from their careers for family, military or personal reasons, are an under-looked, yet ready population positioned to enter or re-enter a high-tech career [5, 6, and 7].

B. "Closing the Gap" Conference

We hosted over 80 participants at the conference throughout the day (Fig. 1). By profession those included 13 academics, 10 government employees, 18 industry representatives, 3 members of the military and 11 veterans, 9 members of various non-profit organizations, 4 researchers, and 12 individuals who noted themselves as "other". Of equal importance is the distribution of participants by gender: 59 females, 14 males and 7 who either chose not to identify or whose responses were incomplete.

There are three key observations from the conference: 1) the value that women veterans bring to the table is not promoted by the women themselves by underselling themselves and not understood by the recruiter/employer,

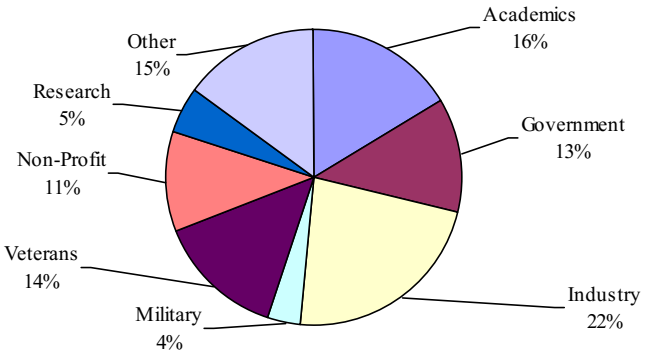

Figure 1. Conference attendance by profession.

This work was supported by George Washington University (GW) – U.S. Department of Defense Cyber Scholarship Program capacity building project (Grant No. H98230-19-1-0320).

2) the transition phase needs to be pre-transition, during transition, and post-transition, and 3) a wealth of information and resources is available to help women veterans.

There are many efforts by different organizations, on different administrative levels, but an effort needs to be made to evaluate the current resources, how well they are working, and how suitable they are to the cyber security field. The USA federal government needs to take the lead in creating a consolidated platform for the many resources available. Such a platform needs resources, a roadmap, and guidance for the specific career path. This latter observation led the research team to consider developing an accessible application for the target audience i.e. the woman veteran.

C. Methodology

New research problems benefit from brainstorming sessions to ensure the inclusion of a variety of ideas on how to proceed. A designathon was scheduled for students, veterans, and visiting faculty interested in a project intended to be accessible on a mobile device, targeting women and/or related to military veterans. Unlike a hackathon, whose goal is to create functioning software or hardware by the end of the event, the goal of our low-tech and high-level designathon was to generate ideas on what a mobile app would look like, what it might include, and how it might flow or function without being caught up in the programming details.

The designathon provided a jumpstart in both a plethora of ideas and a deeper understanding of the challenges, not the least of which was the December deadline imposed by the remaining timeframe on the grant. What evolved were conceptual, semantic, technological, and human design challenges to creating the GapApp.

Two teams were organized, led by faculty/seasoned researchers and including two students each: Data Resources team and Technical Analysis team. The former provided the latter team with appropriate data tables in order to design and implement the application.

D. Team Selection

A goal of the project, in addition to creating the GapApp, was to engage students in authentic research problems. A call was posted indicating the opportunity to work on a funded research project until December 2022, with the primary effort commencing after spring term finals. Requirements included strong technical skills and coding experience. We specifically chose female students for this project as they reflected, in some ways, the target audience.

Two computer science students were selected for the Technical Analysis team and one student who had worked on the original conference grant and one biomedical engineering student who expressed strong interest in data collection and representation were selected for the Data Resources team.

Given the travel and location sites for our team, except for the designathon, all events were held on Zoom with most meetings recorded. The entire team and the focused sub-teams met in alternate weeks to maintain a steady workflow between newly assigned tasks and reported progress.

II. Analysis and Design

As part of the initial analysis, the Data Resources team studied the existing workforce role and skill taxonomies in cyber security and military.

A. Databases

One of the most common ways for a veteran to describe the skills and tasks related to their military roles is for them to use the Military Occupational Specialties (MOS) [8]. Each branch of the military has its own set of codes and descriptors. The Marine Corps alone have 80 possible fields describing the qualifications and opportunities for assignment [9].

For example, “Information Assurance Technicians (MOS 0689) are now called Cyber Security Technicians and are responsible for the security of all information systems and its integrity, authentication, and confidentiality” while the Army Cyber Operations Specialists (MOS 17C) are tasked with safeguarding Army intelligence and information. They safeguard information by protecting digital data, maintaining security measures like firewalls, and introducing new cyber security.

The National Institute of Standards and Technology (NIST) has undertaken to codify the careers and positions with cyber security in the NICE [10]. The workforce framework for cyber security work roles [11] is organized by category, specialty area work role and work role definition a sample of which is shown in Table 1.

The MOS and NICE databases provide thorough descriptions of possible cyber security positions. It would be optimal for a veteran to be able to enter their MOS role into the GapApp and be pointed to a series of possible cyber security careers for which they have had pertinent training or experience.

The biggest limitation to the design of the GappApp is that there is no direct, or even modestly direct, route to matching between the two.

The NICE tables use English sentences or phrases to identify the tasks and operations for each work category. The MOS database on the other hand typically uses 3-4 word phrases to describe skills and full English sentences to describe summaries of the specialty. If the databases could be made more equitable using the same terms and same short phrases to define the tasks one would do in a specific job.

B. Mapping and Matching

Therefore, the Data Resources team had three tasks to resolve: 1) create a database from the MOS skills that could be mapped to NICE work roles, 2) resolve the NICE formulation into similar phrases, and 3) develop a technique for mapping from one database to another and evaluating the match. For example if a user entered a specific MOS, the GapApp would return an ordered list of possible matches for the veteran to pursue toward a career in cyber security.

TABLE I. A SAMPLE NICE WORK ROLE AND TASKS DEFINITION

NICE Work Role	Network Operations Specialist
Work Role ID	OM-NET-001
Task ID	**Tasks**
T0035	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).
T0065	Develop and implement network backup and recovery procedures.
T0081	Diagnose network connectivity problem.
T0121	Implement new system design procedures, test procedures, and quality standards.
T0125	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
T0126	Install or replace network hubs, routers, and switches.
T0129	Integrate new systems into existing network architecture.
T0153	Monitor network capacity and performance.
T0160	Patch network vulnerabilities to ensure that information is safeguarded against outside parties.
T0200	Provide feedback on network requirements, including network architecture and infrastructure.
T0232	Test and maintain network infrastructure including software and hardware devices.

The Data Resources team spent many hours reviewing the content and formulation of both databases. In order to make the project viable, only three MOSs and five work roles were selected as a proof of concept challenge (Fig. 2).

The decision for the mapping match was as follows: Let T be the set of all possible tasks, hence $T = \{t_1, t_2, t_3, \ldots t_N\}$, where N is the maximum task index. We observe that every MOS and work role can be described as a subset of the T. Consider $MOS[i] = \{t_{i1}, t_{i2}, t_{i3}, \ldots t_{in}\}$, where $n > 0$ is always true, also $WorkRole[j] = \{t_{j1}, t_{j2}, t_{j3}, \ldots t_{jm}\}$, where $m > 0$. A simple naive matching function would look like

$$|MOS[i] \cap WorkRole[j]| / |WorkRole[j]|, \qquad (1)$$

where $X \cap Y$ denotes conjunction or intersection of sets X and Y, and $|X|$ denotes the size or number of elements in a set X.

C. Tool Selection

The challenges for the Technical Analysis team was to identify a tool that could be used to rapidly design, implement, and launch the GapApp. The tool requirements included a simple learning curve which meant avoiding new programming languages, database support, easy user interface design, easy incorporation of graphics, a ready technical support community to help answer implementation questions, easy work sharing to enable the team members to work jointly, but remotely, on the application, and no subscription or user fees. The team reviewed Crowdbotics, SWIFT, AppCode, AppyPie, Flutter (with Firebase) and Xcode, among others, and settled on FlutterFlow[1]–the drag and drop version of Flutter.

III. GAPAPP IMPLEMENTATION

With the teams selected, each team moved into solving its own core problems. The Technical Analysis team, as noted above, moved forward with FlutterFlow and its allied database, Firebase, as the tool with most of our required characteristics. While Flutter had a good drag and drop methodology and a series of model apps, the team was challenged to move deeply into the technical structure. Firebase is not the typical SQL database with which students had become familiar. The presence of online videos helped as FlutterFlow and Firebase documentation.

Implementing the MOS search for the proper NICE job categories was expedited by the Data Resources team's decision to use only a subset of the available data. The pilot version (Fig. 3) was completed with additional efforts on the look and feel of the user interface, the addition of visuals and the linkages to available online content and videos.

A. Successes and Challenges

One of the early challenges for the Technical Analysis team was the lack of pre-existing roadmaps. The students were more used to a well-defined problem where such classroom assignments are often partially or completely structured. Solving the problem often means using a programming language you know, building on techniques you've learned, and solving the problem. In the case of GapApp, no one had "been here before". The students were often frustrated without the roadmap and the faculty leading the technical team was as new to the use of the chosen tools as the students. The process often shook the students' confidence in their own ability, but in the end, success was that students experienced solving a problem they had never seen before, one with dead end alleys and one that ultimately was completed.

The algorithm for identifying which MOS is related to which NICE job categories is a simple matching algorithm that compares the tasks of a given MOS with the tasks of each NICE work role stored in our database. This ability is dependent on terminology.

NICE has defined tasks with associated task IDs for each work role, however, the military has yet to publish a similar standardized structure describing each MOS. Furthermore, the terminology for cyber security-specific civilian work roles and military work roles drastically differ. For the prototype, our Data Resources team manually compared each NICE task with the descriptions of a MOS (provided by the associated branch website, American Council on Education Military Guide[2], National Cybersecurity Training&Education Center[3]-published occupation description, etc.) and assigned task IDs of the task that best matched the MOS descriptions.

[1] https://flutterflow.io/
[2] https://militaryguide.acenet.edu/
[3] https://www.ncyte.net/faculty/faculty-resources/mos-pathways

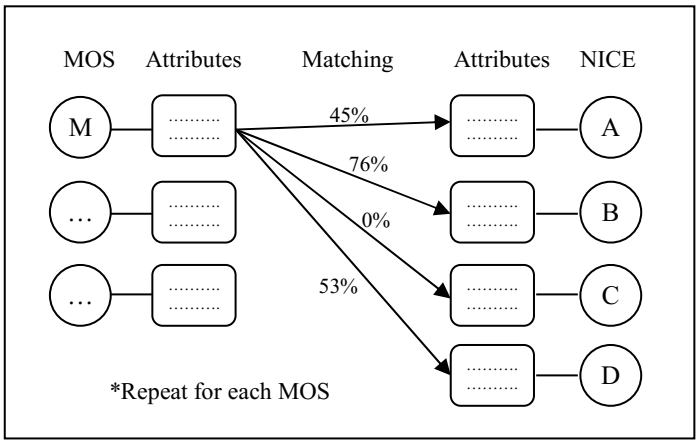

Figure 2. Mapping and matching evaluation technique.

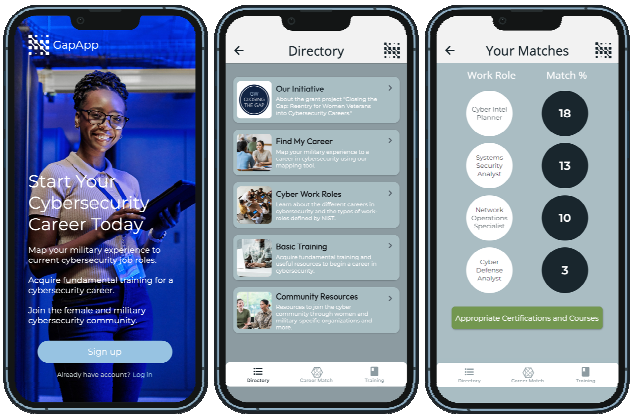

Figure 3. The Gap App pilot version user interface.

The problem with this method is it is subjective and takes time, meaning low replicability and high labor cost. This algorithm will be better streamlined if the military standardizes MOS descriptions and assigns tasks that utilize NICE work role terminology to allow for more accurate comparison.

IV. Conclusion and Future Work

The project revealed that the DoD and NIST classification databases consistently use varying terminology or wording for very similar career positions within their respective branches of the government. Not only did this limit the development of the GappApp, it limits the ability of anyone transitioning from the military to seek comparable placement in the cyber security field.

One intuitive suggestion would be to work on harmonizing these two frameworks. This would require the full participation of both the military and NIST leadership to come together in support of using the same terminologies and phrasing for both plans.

The current matching algorithm, described above, uses a model that considers all tasks equally important, so extension could be a representation of a work role as a set of pairs of task-importance $\{(t_1,i_{t1}), (t_2,i_{t2}),\ldots (t_n,i_{tn})\}$, where all i's would sum up to *1* or *100%*. If both work role and MOS use the same representation, then an alternative matching function (1) could be the sum of all i's in the work role description iterated over the tasks in the intersection set. Another variation would be to use the sum of minimums of each pair of i's from the matched MOS and work role iterated over the tasks in the intersection set.

An interesting approach would be to apply natural language processing algorithms to automate the mapping that is matching virtually the same categories that are listed in different databases. This would also be useful for improved recommendation of job vacancies or industrial training opportunities that match the user profile.

With the proof of concept accomplished, there are several future pathways to pursue, including a request for supplementary funding to continue app expansion and utility, as well as creation of focus groups to review the Gap App pilot version.

Many ideas produced as the result of the designathon during the initial ideation stage were prioritized for the future stages of potential expansion.

For example, the GapApp could use the initial veteran information (as limited as, for example, date of birth, MOS, and target state) to recommend job or training opportunities from respective open databases. Using gamification methods could help with motivating users in their journey towards a successful career in cyber security. While designing the pilot product the backend was deliberately removed from the architecture. However, with anonymized data collected securely appropriate learner algorithms would help make better recommendations, share motivating success cases among the same cluster of users, such as veterans of the same MOS or same age group.

Acknowledgments

The project team would like to thank all contributors, including the conference and designathon participants. Special thanks go to Jonathan Buckland, former Marine Corps pilot and GW SEAS graduate student in cyber security and Dr. Stephen Kaisler, GW SEAS professor of engineering, for useful comments and insights.

References

[1] C. Balut, R. S. Heller, C. Toregas, T. Wash, “Closing the Gap: a Department of Defense (DoD) conference on re-entry for women veterans into cybersecurity careers,” in Journal on Teaching Engineering, vol. 2, no. 1 (2022), pp. 38-47, https://doi.org/10.24840/2795-4005_002.001_0004.

[2] J. A. Lewis and W. Crumpler, “The cybersecurity workforce gap” available at https://www.csis.org/analysis/cybersecurity-workforce-gap on 29 January 2019

[3] R. Feloni, “The head of Siemens US shares the workforce-altering story the media missed while covering Trump's 'Tim Apple' gaffe” available at https://www.businessinsider.com/siemens-usa-ceo-barbara-humpton-on-4-goals-for-american-workforce-2019-3 on 1 April 2019

[4] I. Denton, "Hiring America’s veterans: a smart business decision" available at https://blog.dol.gov/2021/07/22/hiring-americas-veterans-a-smart-business-decision on 22 July 2021

[5] Council of Foreign Relations, Demographics of the US Military, (2019) available at https://www.cfr.org/article/demographics-us-military on 3 February 2020

[6] C. R. Szelwach, J. Steinkogler, E. R. Badger and R. Muttukumaru, “Transitioning to the civilian workforce: issues impacting the reentry of rural women veterans,” in Journal of Rural Social Sciences (2011); 26 (3), pp. 83–112

[7] C. Zoli, L. Steinberg, “Building awareness of ETETE careers, pathways, and academic preparation for service members,” 2013, available at https://securitypolicylaw.syr.edu/wp-content/uploads/2017/10/ZOLI_STEINBERG_BUILDING_AWARENESS_OF_ETETE_CAREERS.pdf on 30 January 2020

[8] R. Powers, Complete List of Army Enlisted MOS, at LiveAbout website https://www.liveabout.com/complete-list-of-army-enlisted-mos-s-3346173

[9] The Marine Corps Numerical Index of Military Occupational Specialties, at the Official U.S. Marine Corps Website, https://www.marines.mil/Portals/1/Publications/NAVMC%201008-A%202022%20FY23.pdf

[10] C. Paulsen, E. McDuffie, W. Newhouse and P. Toth, "NICE: creating a cybersecurity workforce and aware public," in *IEEE Security & Privacy*, vol. 10, no. 3, pp. 76-79, May-June 2012, https://doi.org/10.1109/MSP.2012.73.

[11] The Workforce Framework for Cybersecurity (NICE Framework), at the National Institute of Standards and Technology (NIST) official website, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice