UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

A Swarm Intelligence Approach to Prioritizing the CIS Controls V8.0 Implementation

HAYAT ABDULLA ASAD CUE, THIRIMACHOS BOURLAI, MARK LUPO

CLTC WHITE PAPER SERIES

A Swarm Intelligence Approach to Prioritizing the CIS Controls V8.0 Implementation

HAYAT ABDULLA ASAD CUE, THIRIMACHOS BOURLAI, MARK LUPO

September 2024

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

EXECUTIVE SUMMARY 1

INTRODUCTION 3

SECTION 1: UGA CyberArch 5

The CIS Controls V8.0 as a Base Framework for Cybersecurity Assessments 6

From Qualitative to Quantitative Assessments 8

The CIS Controls V8.0 Security Criteria Prioritization 10

The CIS Community Defense Model V2.0 11

The CIS Cost of Cyber Defense V1.0 12

SECTION 2: Practical Application of Swarm Intelligence (SI) Algorithms in Cybersecurity 14

Swarm Intelligence (SI) and Cybersecurity Overview 14

Particle Swarm Optimization (PSO) Applications in Cybersecurity 16

Proposed Approach: Swarm Particle Optimization for Criteria Prioritization 17

SECTION 3: A City School System Case Study 19

CONCLUSIONS 24

REFERENCES 25

ACKNOWLEDGMENTS 30

ABOUT THE AUTHORS 31

EXECUTIVE SUMMARY

In the public service and outreach field, supporting organizations such as rural hospitals, city-county governments, K–12 school systems, and small businesses in strengthening their cybersecurity posture is essential yet challenging due to resource limitations. Although the Center for Internet Security (CIS) framework has been recognized for its effectiveness in guiding enterprises toward adopting effective cybersecurity measures, it often presents a daunting task for many organizations due to uncertainties about security action prioritization.

This paper proposes a unique approach to enhancing the implementation process of the CIS Control V8.0 framework. The proposed approach generates sets of prioritized security actions based on expert recommendations. This aligns with industry evidence on cyber threats, which is not commonly found in traditional academic approaches due to the limited availability of real-world data. This approach enriches the body of knowledge of the researchers working in the field while applying practical solutions relevant to this research area.

The present work aims to address the multicriteria prioritization challenges by developing a model based on swarm intelligence (SI) that orders security actions based on specific criteria, such as the mitigation of cyber attacks and the cost of implementation. The study employs quantitative data analysis, leveraging the systematic work of CyberArch, a cybersecurity clinic at the University of Georgia (UGA). The SI-based model studies implementation scenarios and analyzes the empirical data gathered through cybersecurity risk reviews using particle swarm optimization (PSO).

The objective is to determine an optimal, cost-effective sequence of prioritized controls to maximize cybersecurity resilience in practical settings.[1] This research contributes to the public interest in cybersecurity by offering a data-driven solution for enhancing the cybersecurity posture of target-rich, resource-poor organizations. This approach:

1. Tailors the roadmap for implementing the CIS Controls V8.0 framework Implementation Group 1 (IG1) using SI algorithms.
2. Bridges the cybersecurity knowledge by incorporating subject-matter expert recommendations, enabling organizations to make complex cybersecurity decisions effectively.

1 Cyber resilience is defined as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources" (NIST SP 800-160, 2021).

3. Automates incorporating two main security management criteria to improve organizations' defenses against increasingly sophisticated cyber threats.

The results show significant gaps between the cybersecurity needs and the resources available for implementing security programs in multiple organizations. In addition, the initial data processing confirmed these enterprises had different baselines in setting the implementation priorities for a standard set of security actions. This indicated that there is a diversity in terms of setting priorities in the controls' implementation for these organizations. Applying the SI-based algorithms showed significant promise in addressing the challenges of redirecting the priority orders of implementation to align with the CIS recommendations for IG1.

Since the study results directly apply to the outcomes generated throughout the assessment processes, partner organizations can benefit from integrating subject-matter experts' knowledge into their decision-making processes. As we plan to extend the research to include a larger pool of organizations, we expect to reach more generalized results and provide additional recommendations for guiding the implementation of the first tier of security measures contained in the CIS Controls V8.0 framework. Moreover, this approach could be significantly extended to cover other cybersecurity frameworks' assessment and prioritization processes.

INTRODUCTION

Implementing effective security programs is not just a necessity but a matter of urgency for today's enterprises, particularly public service organizations and small- to medium-sized businesses. These entities, which are often entrusted with vast amounts of sensitive information — from social security numbers and medical data to financial account details — are alarmingly vulnerable to cyber threats.[2] They struggle to invest in comprehensive cybersecurity infrastructure and specialized IT knowledge because they operate under critical financial and human resource constraints. These vulnerabilities make them prime targets for cybercriminals, who exploit their limited defenses in several ways.[3]

The cybersecurity clinic model, developed by the founding institutions of the Consortium of Cybersecurity Clinics, offers a promising solution for resource-constrained environments. This model establishes partnerships through which students from colleges and universities are trained to provide pro bono digital security assistance to public service organizations. Access to clinic resources empowers these organizations to identify vulnerabilities and areas of improvement needed to strengthen their systems effectively. In recent years, cybersecurity clinics have expanded and diversified their approaches while offering practical solutions and expertise that may otherwise be out of reach for the organizations they serve. These clinics provide hands-on support in executing risk reviews and devising security strategies tailored to each organization's unique requirements and threat landscape. These clinics' services are essential as they go beyond theoretical concepts and general recommendations to provide practical advice customized to help partner organizations combat cyber threats.[4]

In addition to the direct benefits they provide to organizations, these clinics also serve as crucial and dynamic learning environments for students, fostering the next generation of cybersecurity professionals. However, despite the clinics' contributions, these organizations are often challenged in their cybersecurity efforts due to decision-making complexities regarding resource allocation and the prioritization of security areas. To address this challenge, this paper proposes a data-driven solution improve the systematic work of the CyberArch program, the University of Georgia's cybersecurity clinic, by using a swarm intelligence priority-based approach to guide the implementation of the Center for Internet Security's Controls V8.0 framework.

2 NIST (2020), CISA (2022), and DHHS (2023).
3 Tsiodra et al (2023), CISA (2022), and Szczepaniuk (2020).
4 The Consortium of Cybersecurity Clinics (2024).

The proposed approach leverages the group's collective intelligence and optimization capabilities. Combining multidisciplinary research with public service and outreach expertise and the recently adopted quantitative assessment is expected to play a critical role in building UGA CyberArch's partner organizations' preparation to handle future security issues more competently.

This paper is structured into three main sections. Section 1 introduces the UGA cybersecurity clinic, CyberArch, and the base cybersecurity framework used to conduct the cybersecurity risk reviews. The section also discusses the clinic's shift from qualitative to quantitative assessment methodologies, and explores the prioritization of security criteria within the CIS Controls V8.0 Implementation Group 1(IG1). Additionally, it introduces the CIS's Community Defense Model V2.0 and Cost of Cyber Defense V1.0 to provide insights into community-based defense strategies and the financial implications of adopting IG1 cybersecurity measures.

Section 2 explores swarm intelligence algorithms and their cybersecurity applications. It starts with an overview of SI's origin from natural phenomena and its adaptation into algorithmic solutions that imitate collaborative behaviors observed in groups of animals, such as insects or birds. The section further explores specific applications demonstrating how these algorithms enhance threat detection and system resilience through distributed problem-solving capabilities, focusing on particle swarm optimization (PSO) for prioritizing security criteria.

Finally, Section 3 concludes with a case study involving the quantitative compliance assessment of a city school system and the analysis of the cybersecurity vulnerabilities found. In addition, the section explores using the PSO algorithm alongside the systematic evaluations to illustrate enhanced decision-making processes in defining an optimized list of security actions that would improve the cybersecurity posture of the educational institutions, conforming such school systems against potential cyber threats.

SECTION 1: UGA CyberArch

The University of Georgia (UGA) CyberArch clinic program is one of the initial members of the Consortium of Cybersecurity Clinics. The CyberArch program was developed by UGA within the Public Service and Outreach division to support community entities in assessing and strengthening their cybersecurity posture. Each semester, the clinic partners with community organizations to conduct cybersecurity risk reviews, allowing the participant organizations to benefit from up-to-date best practices without incurring substantial costs for private consultancy services.

This partnership harnesses undergraduate and graduate students' knowledge, energy, and motivation while providing hands-on experience under the guidance of faculty and industry professionals. Offering students real-world exposure has proven to be a valuable experiential learning practice that bridges the gap between academic learning and practical applications.[5]

The clinic's effectiveness is evident through the testimonials of partner organizations, which have noted a better cybersecurity posture due to the comprehensive risk reviews, personalized recommendations, and guidance provided by the UGA CyberArch team. This pragmatic approach has fostered their organizations' improved cyber awareness and preparedness culture.

One healthcare partner organization emphasized the program's ability to uncover unnoticed vulnerabilities and assist in creating a more secure data management system. A representative from a local government office commended the clinic for helping to develop a comprehensive incident response plan, which proved vital during a subsequent cyber incident. Likewise, a K–12 school system reported significant improvements in cybersecurity awareness among staff and students, attributing them to the training interventions recommended by the program.

UGA CyberArch represents an essential channel between academic training and practical cybersecurity defense, fostering resilience in organizations that are often underserved due to their resource constraints. The testimonials of these partner organizations underscore the value and impact of the UGA CyberArch program and the cybersecurity clinic model broadly.

5 Lupo (2024).

THE CIS CONTROLS V8.0 AS A BASE FRAMEWORK FOR CYBERSECURITY RISK REVIEWS

Cybersecurity frameworks are essential tools and methodologies that help organizations tackle compliance challenges in cybersecurity policies. They offer a common language for IT professionals to identify the vulnerabilities that must be addressed to achieve specific cybersecurity maturity levels.[6] Using such frameworks enables enterprises to strategically plan their cybersecurity efforts, allocate resources effectively, and implement necessary security measures.[7] This section provides an overview of the Center for Internet Security (CIS) Controls V8.0 in the context of the most frequently used cybersecurity frameworks in the United States (U.S.).

In recent years, several cybersecurity frameworks (in their multiple versions) have been identified by experts in the field as the most popular and highly adopted.[8] These include the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), the Cybersecurity Maturity Model Certification (CMMC), the CIS Controls, the NIST/IEC 27000 series, the Payment Card Industry Data Security Standard (PCI), and the Health Insurance Portability and Accountability Act (HIPAA). While these frameworks have gained positive recognition among security practitioners, many address challenges at a systems level for specific applications, and lack scalability and adaptability in applying quantitative approaches. Therefore, ongoing research is being conducted to develop new theoretical frameworks built on top of these base frameworks, allowing for quantitative compliance assessment that can identify critical improvement requirements within organizations' cyber postures.[9]

The UGA CyberArch assessment process focuses on the CIS Controls as the foundational framework for its cybersecurity risk review. These controls have been widely recognized as best practices for securing IT systems and data and are designed to provide actionable guidance for improving an organization's cyber defense capabilities.[10]

The CIS is a nonprofit organization that has been in the cybersecurity field for more than 20 years. Its work provides a foundational framework of best cybersecurity practices for organizations to assess and enhance their cybersecurity programs. Based on the principle that most organizations face common threats and the need to comply with industry-specific security

6 Bejarano (2021) and Lourens (2022).
7 Allodi (2017), Dominguez-Dorado (2022), and Teodoro (2015).
8 Tarala (2023).
9 Gourisetti (2020), Leszczyna (2021), and Lippmann (2022).
10 CISA (2020), VERIZON (2023).

frameworks, the CIS addresses these challenges by defining specific security actions for organizations depending on the size, needs, and resources reflected in the implementation groups (IGs) represented within the framework.[11]

The CIS Controls V8.0 comprises 18 actionable controls, each with sub-controls or safeguards designed for different implementation groups. These IGs were developed based on an enterprise's risk profile and are structured to establish layered security defense: IG1 (Implementation Group 1) includes 56 safeguards, IG2 includes 130 safeguards, and IG3 encompasses 153 safeguards. Each IG builds upon the previous groups' security actions using a tiered security measures approach.[12] Our research is based on V8.0, and while the latest version, CIS controls V8.1, was released in June 2024, there are no significant changes in the security actions between the two versions.[13] The following table shows the IGs, the number of safeguards, and the correspondent risk profiles.

Table 1. The CIS Controls V8.0 implementation groups

Implementation Group (IG)	Risk Profile	Number of Safeguards	Description
IG1	Lower risk levels	56	Foundational measures of cybersecurity defined as cyberhygiene
IG2	Moderate risk levels	30	Builds upon IG1 with additional safeguards enhancing security measures
IG3	Higher risk levels	153	Includes all safeguards from IG1 and IG2 for more comprehensive protection

One of the values of incorporating the CIS's controls as the base for developing security programs is the framework's comprehensiveness in covering primary areas like data, accounts, networks, devices, applications, etc.[14] In addition, the CIS has enabled the ability to map its controls to other frameworks, which is sometimes strictly required for operations in specific sectors,

11 CIS V 7.1.
12 CIS V8.0 (2020).
13 CIS Controls V8.1 (2024).
14 VERIZON (2024).

such as HIPAA, FERPA (Family Educational Rights and Privacy Act), PCI, and CMMC. This feature adds to the framework's transferability to different industries and regulatory environments.[15]

FROM QUALITATIVE TO QUANTITATIVE ASSESSMENT

Cybersecurity compliance assessments can be carried out using qualitative or quantitative approaches. Qualitative assessments focus on subjective analysis through expert opinions, interviews, and observations to determine the effectiveness of security controls and procedures. They provide deep insights into the context-specific nuances of cybersecurity practices and are valuable in understanding non-measurable aspects such as organizational culture and user behavior. However, due to their subjective nature, qualitative assessments can be prone to bias and may lack consistency.[16]

Quantitative assessments, however, involve measurable, data-driven metrics such as the number of incidents, compliance scores, or implementation percentages. These methods offer objectivity and ease of comparison over time and across different departments or organizations.[17] Moreover, they facilitate straightforward reporting and decision-making. Both methods have their place in a comprehensive cybersecurity strategy, with qualitative assessments providing depth and context, while quantitative methods add scalability, repeatability, reproducibility, and comparability of assessment results.[18]

In Spring 2022, the UGA CyberArch clinic began conducting its initial risk reviews for two organizations. Led by eight student interns trained in cybersecurity, these risk reviews focused on asking specific questions and generating reports and recommendations to help organizations understand areas of improvement in their cybersecurity posture. The approach aligned various questions using other established risk assessment models as a reference.[19] Although this was a good first approach to assessing the cybersecurity posture of the partner organizations, we identified the need to incorporate a more comprehensive framework in laying the ground for serving a more diverse range of organizations.

In Fall 2022, the number of student interns grew to 24; we began using the CIS V8.0 framework in the assessment process, relying on a more thorough, industry-acknowledged cybersecu-

15 CIS Controls Mapping Tool (2024).
16 NIST (2012) and Fujs (2019).
17 NIST (2012), Crotty (2022), Munteanu (2006), and Ganin (2020).
18 NIST (2012).
19 MIT course (2021), U.S. DoD (2023), and White (2004).

rity framework. By mapping a set of initial questions to the CIS Controls IG1 safeguards, we shifted the analysis and recommendations to assess compliance with these security actions as basic cyber hygiene. It is important to emphasize that the assessment process until this point was qualitative, and the previously mentioned questions were extracted from the MIT model, the CCSMM (Community Cyber Security Maturity Model), and the CMMC frameworks. The participants evaluated the answers to more than 100 questions as "Satisfactory" or "Area to Strengthen." But it was limiting to use a binary system to identify areas of improvement and establish benchmarks for generating comprehensive final reports and recommendations for practical settings. Through the study of the answers provided by partner organizations and the process of report drafting, we identified the need for the following:

(a) A more granular compliance measurement process, and

(b) A final score that reflected the overall cybersecurity posture.

In Fall 2023, the program took a significant step in incorporating the academic research aspect by partnering with the UGA Multispectral Imagery Laboratory (MILAB). Its principal investigator served as an advising research faculty member in developing a novel scoring system, marking a transition from qualitative to quantitative assessment methodologies.[20] The previous ranking-based scoring system was designed specifically to evaluate compliance levels. The emphasis was on integrating security measures such as the CIS Controls V8.0, linked to the most frequent attack techniques, as reflected in industry reports like the Verizon Data Breach Investigations Report (DBIR).[21]

This system employed a six-level sub-control coverage scale and a combination of quantitative methods. In addition, it included four rank-weight methods and their harmonic mean normalized combination. The purpose of incorporating these specific quantitative methods was to assign a numeric score when a particular IG1 safeguard was implemented. Thus, our scoring system provided a quantitative framework for assessing cybersecurity posture in practical scenarios through a specific numerical value. Simultaneously, it delivered a more precise understanding of the security posture of partner organizations, effectively highlighting critical security criteria that required attention, thus enabling more efficient responses to cybersecurity threats.

Currently, the UGA CyberArch clinic includes more than 30 student interns, who lead the assessment processes and work with partner organizations as follows:

20 UGA MILAB (2024).
21 Verizon (2023).

1. Groups of four or five UGA CyberArch interns assess one organization through questionnaires and one on-site visit.
2. The quantitative assessment results are entered into the UGA CyberArch system.
3. These interns analyze the results and generate a report with recommendations that include a prioritized set of security actions.
4. The supervising faculty review each report.
5. The results are delivered to the assessed organization.

This approach offers weighted coverage per safeguard implementation,[22] enhancing the organization's overall classification of its cybersecurity posture as "satisfactory" or "needing improvement." Although the previous scoring system was designed for CIS Controls V8.0, the approach can be extended to other cybersecurity frameworks that require a user to implement a finite number of security actions.

THE CIS CONTROLS V8.0 SECURITY CRITERIA PRIORITIZATION

A critical element that stood out during the development and application of the previous scoring system and the literature review was the importance of prioritizing security criteria.[23] This is especially evident in the management of real-world organizations, where allocating time and resources is vital for operations.[24] Resource-constrained organizations often require more technical expertise than is available to take the best security action. Target-rich, resource-constrained organizations can face significant challenges with answering questions such as, what order should we follow in implementing a specific cybersecurity framework? What is the best order of steps we can take to prepare for the most frequent cyber-attack types? And how can we minimize associated costs?

Adopting specific security actions, such as the CIS Controls, can be a good step in the right direction. However, implementing these controls can present challenges regarding immediate applicability. In the previous versions (before V7.1), these controls and sub-controls were intended to be implemented sequentially, based on their order of appearance in the general guidelines.[25] However, V8.0 emphasizes implementing the IG1 safeguards as basic cyber hygiene to protect from cyberattacks. This means that IG1 safeguards should be prioritized for all enter-

22 The weighted coverage englobes the degree of implementation and the importance of the safeguard being implemented. The rank weight reflects this importance.

23 Abdulla (2024), Kim (2014), Fletcher (2011), and Park (2016).

24 Fischer (2005).

25 Marchany (2021).

prises; medium and large enterprises should only begin covering IG2 safeguards after IG1 is fully addressed. Lastly, larger-sized organizations should reinforce their systems by implementing IG3 safeguards.[26] Thus, questions about prioritization remain: What order should enterprises follow within the IG1, IG2, and IG3 implementation sequence? Should they be numerically ordered within each group? And what other factors should be considered?

When analyzing the CIS's Community Defense Model (CDM) V2.0, the uncertainties regarding the implementation order become more evident.[27] It is also evident that the priorities change when the financial cost of implementation is factored in when setting priorities. The following sections will explain two CIS guidelines for prioritizing the CIS Controls V8.0 IG1 safeguards.

The CIS Community Defense Model

The CIS Community Defense Model (CDM) V2.0 focuses on empirical data and recommendations from community subject-matter experts to effectively guide the implementation of security controls against real-world threats. The primary objective of the CDM is to help organizations, especially small- and medium-sized enterprises, implement cybersecurity controls effectively. These guidelines link the CIS Controls to specific attacks against which they are most effective.

The CDM process involves utilizing data from industry reports and the MITRE ATT&CK framework to map attack techniques and convert them into actionable best practices. The MITRE Enterprise ATT&CK framework V8.2 is a widely accepted method for detailing the technical aspects of cyber attacks.[28] It addresses the tactics attackers employ and the specific technical actions used within those tactics. This approach analyzes real-world threat data to identify prevalent and relevant attacks affecting enterprises.

The CDM model uses a data-driven methodology to determine which controls are necessary for defending against the most common attack vectors. By analyzing incidents and attack techniques commonly recorded in various industries, this model suggests specific CIS controls for each attack type that should be prioritized.[29]

26 The CIS Controls V8.0 (2020).
27 The Community Defense Model V2.0 (2023).
28 MITRE ATT&CK framework V8.2.
29 The Data Breach Investigations Report (2023).

The guidance is structured to assist in gradually implementing the CIS Controls V8.0 in the three implementation groups to enhance an organization's security posture over time. Furthermore, this model promotes a community-driven approach to cybersecurity, leveraging the experiences and insights of others to fortify their defenses.

When we analyze the CIS Community Defense Model, which presents information about the number of ATT&CK (sub-) techniques that the implementation of these safeguards prevents, we find that some are not included in the IG1 (Cyberhygiene group), although they map to a higher number of ATT&CK (sub-) techniques in comparison with other safeguards that are included in IG1. Specifically, safeguards 18.3, 6.8, 18.5, and 2.5, which rank among the top ten mapped to over 100 ATT&CK (sub-) techniques, are not included in the basic Cyber Hygiene IG1 security actions. Other safeguards, such as those covered in Controls 1 through 3, which pertain to inventories and are considered by experts as the basic principles of IT foundational management, are linked to fewer ATT&CK (sub-) techniques.[30]

The CIS Cost of Cyber Defense

The Cost of Cyber Defense V1.0 is a CIS resource that outlines the economic aspects of implementing effective cyber defense measures using the CIS Controls framework. The document emphasizes the cost-effectiveness of these controls, particularly for small- to mid-sized organizations looking to enhance their cybersecurity posture. It highlights the importance of achieving "essential cyber hygiene" through implementing the IG1 safeguards, which forms the basis of the CIS's cost-of-defense model.[31]

Implementing the protective measures requires using tools that might be acquired as open source, developed internally, procured with commercial suppliers' assistance, or included as an additional feature or capability in an IT product. The methodology employed by the CIS in estimating the costs of IG1 implementation involves categorizing the safeguards into ten areas. These areas are mapped to tool types, and three hypothetical Enterprise Profiles (Tier 1, Tier 2, Tier 3) are created based on factors like employee count, number of IT staff, and annual budgets. Each Enterprise Profile is designed to assist enterprises in estimating the cost of implementing IG1 based on their specific characteristics and requirements.

The protective measures include essential practices such as proper configuration management, regular software updates, and strong access controls. The cost of implementing these mea-

30 The Community Defense Model V2.0 (2023)

31 The Cost of Cyber Defense (2023).

sures is estimated based on the licensing fees of commercially available tools across the ten categories. Evaluations in the CIS Cost of Cyber Defense document indicate that acquiring and deploying commercially supported versions should account for less than 20% of a typical IT budget for any size enterprise.

The control grouping orders are designed to be practical and adaptable across various industries, providing a framework that organizations can align with other compliance requirements. The model also includes vendor-neutral guides that help organizations securely configure their systems while better managing their cybersecurity investments by focusing on measures that provide the most substantial benefits in hindering cyber threats.

In summary, incorporating the CIS Controls V8.0 as a base cybersecurity assessment framework benefits small and medium-sized enterprises looking to enhance their cyber defenses efficiently. The CIS framework's structured approach focuses on mitigating common cyber threats with relevant security controls. The Community Defense Model and Cost of Cyber Defense guidelines aid in understanding these controls' practical implementation and financial costs.

SECTION 2: Practical Application of Swarm Intelligence (SI) Algorithms in Cybersecurity

In this section, we explore swarm intelligence (SI) algorithms and their applications in cybersecurity. We begin with an overview of SI, explaining its origin from natural phenomena and its adaptation into algorithmic solutions that mimic the collaborative behaviors of groups such as insects and birds. The section further presents the correspondence between the social behavior seen in biological swarms when facing threats and the social component of public service organizations when facing cyber threats. Later, we discuss the most common SI applications in cybersecurity, highlighting how these algorithms can optimize decision-making processes in complex cybersecurity environments. Finally, we discuss how particle swarm optimization (PSO) can prioritize security criteria to enhance system resilience through distributed problem-solving capabilities.

SWARM INTELLIGENCE (SI) AND CYBERSECURITY OVERVIEW

SI is a computational approach inspired by the collective behavior of natural systems. This approach encompasses algorithms such as PSO, Artificial Bee Colony (ABC), Ant Colony Optimization (ACO), and Whale Optimization Algorithms (WOA), among others. These algorithms rely on decentralized, self-organized systems in which individuals coordinate locally to achieve global optimization goals. SI emphasizes the interaction and distribution of simple agents, and is commonly known for its flexibility and robustness.[32]

Public service organizations can be viewed as interconnected systems that interact with each other and face various cyber threats throughout their life cycles. We could also identify how factors such as corporate culture, policy enforcement, and employee training, with critical social components, affect the cybersecurity of such entities as school systems, government

32 Beni (2020).

offices, rural hospitals, libraries, and utility companies.[33] Therefore, there are parallels between the global behaviors seen in public service organizations and biological swarms when facing threats. This analogy underscores the importance of unified and proactive approaches to cybersecurity in public service organizations. It emphasizes the importance of collective action and shared responsibility in protecting against and mitigating cyber threats effectively:

1. **Collective Behavior:** Similar to swarms, organizations often operate in networked environments where the actions of one entity can significantly impact others within the same ecosystem. For instance, a cyberattack on one utility company could have widespread effects on the entire power grid, much like a threat to one part of a swarm may prompt a collective response from the whole group.
2. **Shared Vulnerabilities:** The individual members of a swarm share common vulnerabilities. The entire group is at risk if a predator learns how to exploit one swarm member. Similarly, public service organizations often adhere to standardized policies and use similar technologies and protocols. This means that a vulnerability in one area could be exploited across other organizations, increasing the risk of widespread issues.
3. **Distributed Risk:** In swarms, risk is distributed across many members, which helps minimize the impact of an attack on an individual member. Similarly, public service organizations distribute cyber risks across various departments and services. While this can help manage the impact of an attack, it also means that the cybersecurity posture must be consistently strong across all areas to prevent systemic weaknesses.
4. **Adaptive and Responsive:** Swarms quickly adapt to threats and environmental changes, often changing formations or behaviors based on immediate threats. When effectively managing cybersecurity, public service organizations could adapt simultaneously by updating their security measures and protocols in response to new or evolving cyber threats.
5. **Interdependent Security Measures:** Just as the safety of a swarm depends on the coordinated movements and alertness of all its members, the cybersecurity of public service organizations relies on the coordination and compliance of all departments and entities within the organization. A breach in one area can compromise the entire network, making it crucial for these organizations to implement comprehensive and cohesive cybersecurity strategies.

33 Frandell (2022), Norris (2015), and Anastasopoulou (2020).

PARTICLE SWARM OPTIMIZATION (PSO) APPLICATIONS IN CYBERSECURITY

Bio-inspired computing has seen a growing application in cybersecurity, with swarm intelligence (SI) playing a significant role. SI algorithms are increasingly applied in cybersecurity due to their versatility in solving complex problems. Multiple studies have emphasized the potential of SI techniques in enhancing cybersecurity defenses in the face of evolving threats due to their ability to mimic the collective behavior of decentralized and self-organized systems.[34]

One of the most well-known algorithms in the field of SI is particle swarm optimization (PSO), which was introduced by Kennedy and Eberhart in 1995. In PSO, the whole group of possible solutions are represented as the "swarm," like a flock of birds. Each possible solution within that group is called a "particle," similar to an individual bird in the flock. Specific fundamental formulations govern the movement of particles within a search space, looking for the optimum solution. Particle movement is influenced by the entire population's best-known position as well as the position of the individual particles.[35]

This optimization method has applications in various fields, such as process optimization, communication networks, robotics, and cybersecurity. SI is often seen as a way for groups to adapt and solve problems together, offering advantages such as simple implementation and minimal parameter-tuning, i.e., adjusting the variables of a model until it reaches optimum performance.[36] However, PSO presents some limitations. It can settle on a solution too quickly, which is often referred to as "premature convergence." It also struggles with complex problems, such as when the problem's solution depends on many variables, and has challenges in handling discrete variables. These shortcomings have prompted the development of improved algorithm versions.[37]

PSO is the second most frequently used bio-inspired algorithm in cybersecurity after genetic algorithms (GA).[38] PSO has been widely used in intrusion and attack detection systems, cloud computing, anomaly classification, workflow planning, and scheduling, among other security and defense applications.[39] Although PSO has significant potential, the algorithm is not frequently used to support the implementation of cybersecurity frameworks. Our proposed

34 Chui (2024).
35 Kennedy (1995).
36 Wang (2009).
37 Kennedy (1997), and Freitas (2020).
38 Hassan (2005), Chui (2024), and Eberhart (2012).
39 Truong (2020), Chui (2024), Priyanka (2021), Bamakan (2015), and Shami (2022).

method focuses on closing this gap by applying PSO to guide the implementation of security controls within the CIS Controls framework.

PROPOSED APPROACH: SWARM OPTIMIZATION AND THE CIS CONTROLS V8.0 PRIORITIZATION

Security control prioritization is essential for establishing successful security programs and ensuring IT system protection.[40] Selecting and prioritizing the most effective measures is a complex multicriteria decision-making process that is often improved using quantitative techniques.[41] Multiple studies have emphasized the need for structured and cost-effective approaches to setting priorities based on security requirements. These studies underscore the importance of systematic and data-driven approaches for control prioritization in security programs.[42]

UGA CyberArch has been shifting our cybersecurity assessments from a qualitative to quantitative approach. The quantitative results set the baseline for addressing the CIS control implementation prioritization process in specific practical settings. As explained in Section 2, the PSO algorithm offers promising resolution methods to solve complex multicriteria problems. Therefore, we incorporate this algorithm to guide the prioritization process. In this way, we address the need to follow a specific cybersecurity framework and the practical challenges involved in the implementation.

Figure 1 represents the proposed approach to incorporate PSO in the UGA CyberArch risk reviews and the CIS control prioritization process at the system level. The process begins with determining an organization's compliance with the CIS Controls V8.0 IG1 framework and identifying areas for improvement. Then, the risk review results are used to establish the initial priority ranks, which we will refer to as baseline priority ranks. These ranks determine the organizations' initial prioritization of each safeguard. Later, the PSO algorithm updates the priority ranks order, incorporating the following criteria into the optimization function: (a) the CIS Community Defense Model and (b) the Cost of Cybersecurity.

40 CISA (2020), NIST (2020), CIS (2020).
41 Gourissetti (2019).
42 Breier (2013), Hadar (2019), Al-Safwani (2018), and Salinesi (2006).

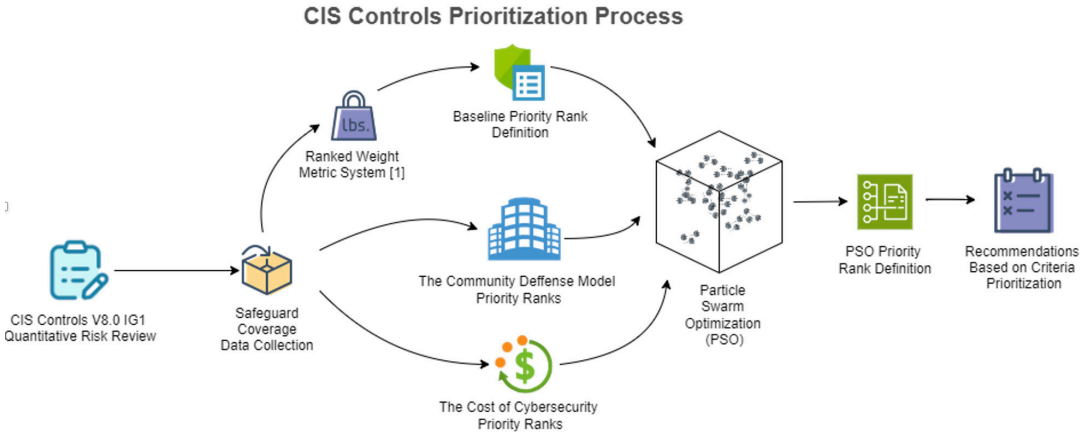

Figure 1. Incorporating PSO in the UGA CyberArch Risk Review Process

The PSO algorithm's output provides a list of prioritized ranks, which are included as recommended actions. These sub-controls are implemented in appearance order based on the safeguard coverage levels within the organization's specific context. The diagram emphasizes a systematic and data-driven approach to defining control prioritization, leveraging SI to optimize decision-making. This methodology aims to provide clear, actionable recommendations based on the CIS Controls V8.0 framework.

The proposed priority-based PSO approach is anticipated to improve the clinic's capacity to deliver thorough and systematic risk reviews through quantitative assessments aligned with proven cybersecurity principles. Based on the overall assessment results, the clinic aims to aid partner organizations in understanding and improving their current cybersecurity readiness to tackle cyber threats as they evolve.

SECTION 3: A City School System Case Study

The following section explores the proposed approach's practical application, illustrated through a case study featuring a rural city school system. This system consists of five schools, including elementary, middle, and high school levels. All identifying information about this organization has been removed to ensure security and privacy.

Because this organization's IT department consists of only two staff members, it is considered limited in terms of cybersecurity resources compared to larger U.S. school systems. During the risk review process, the UGA CyberArch team evaluated the organization's adherence to CIS Controls V8.0 through a survey questionnaire combined with an on-site visit. The IT personnel and other staff members answered questions about the IG1 safeguards. Figure 2 illustrates the levels of compliance extracted from their answers using a six-level scale, ranging from 0% to 100% coverage.[43] The quantitative compliance assessment results reveal critical insights into the organization's cybersecurity posture. They also show the variability in safeguard implementation for the 56 IG1 categories. The final compliance score was 51 out of 100 points in this case.

Based on the coverage levels observed, safeguard compliance could be classified into two main categories: safeguards with satisfactory implementation levels of 60% or above, and those with moderate to low implementation levels ranging from 40% to 0%. The first category indicates a relatively strong level of adherence to the specific aspects of the CIS Controls, reflecting their importance within the organization's cybersecurity strategy. The second category represents potential vulnerabilities within the organization's cybersecurity defenses. In other words, when a specific safeguard has been implemented up to 60% or more, it is an indicator that the organization prioritizes this security action. On the other hand, safeguards with coverage below 60% represent potential vulnerabilities within the organization's cybersecurity defenses.

The differences in these implementation levels highlight areas for improvement, potential incidents that could result from lack of implementation, and challenges for the organization to

43 Abdulla (2024).

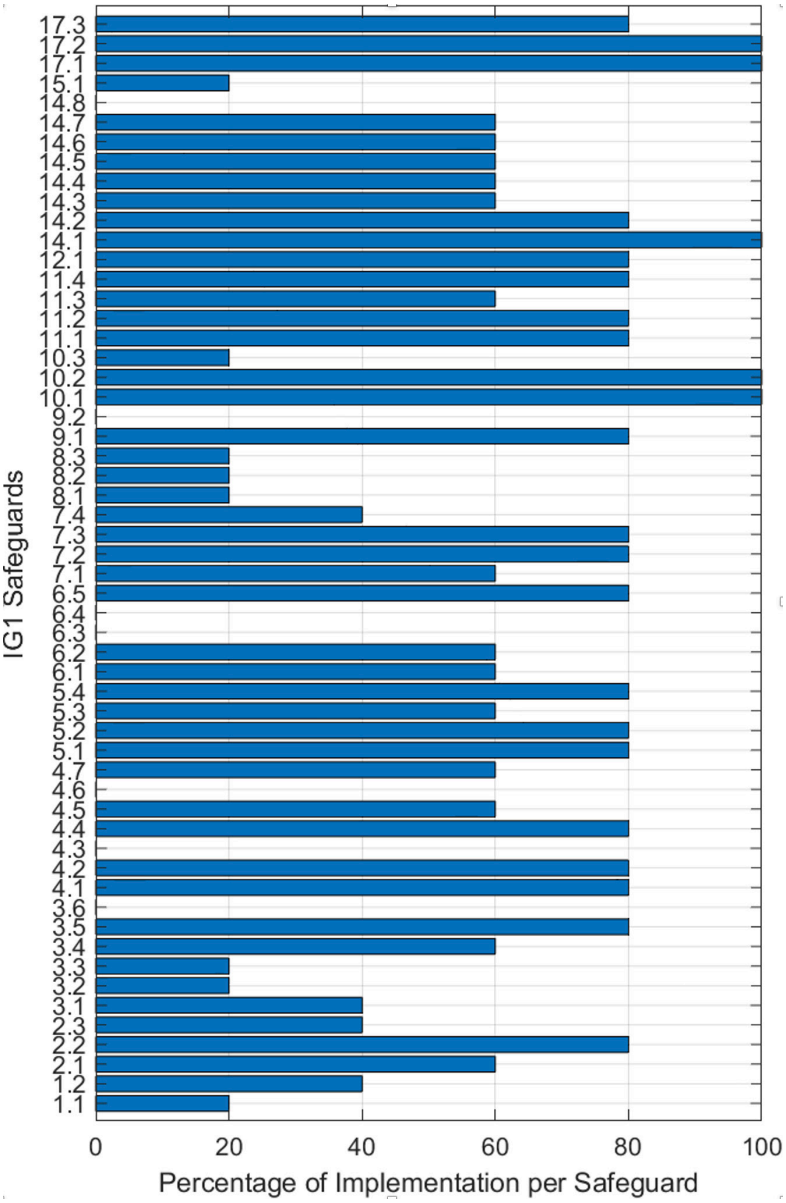

Figure 2. Risk review results for the rural city school system show variability in the CIS Controls V8.0 IG1 implementation levels.[39]

address. These challenges include (a) the need for further understanding or expertise in specific controls and (b) the influence of perceived risk and potential impact on the prioritization of safeguards. Table 2 shows the IG1 safeguards needing immediate attention to improve the organization's cybersecurity posture, as well as some potential associated incidents.

Table 2. Areas of Improvement Identified through the Assessment Process

Safeguard	Description	Coverage	Security Function	Potential Incidents[44]
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	20%	Identify	Lost and Stolen Assets
1.2	Address Unauthorized Assets	40%	Respond	Unauthorized Access
2.3	Address Unauthorized Software	40%	Respond	Software Exploitation
3.1	Establish and Maintain a Data Management Process	40%	Identify	Data Breach
3.2	Establish and Maintain a Data Inventory	20%	Identify	Data Loss
3.3	Configure Data Access Control Lists	20%	Protect	Unauthorized Data Access
3.6	Encrypt Data on End-User Devices	0%	Protect	Data Theft
4.3	Configure Automatic Session Locking on Enterprise Assets	0%	Protect	Session Hijacking
4.6	Securely Manage Enterprise Assets and Software	0%	Protect	Asset Misuse
6.3	Require MFA for Externally Exposed Applications	0%	Protect	Credential Theft
6.4	Require MFA for Remote Network Access	0%	Protect	Network Intrusion
7.4	Perform Automated Application Patch Management	40%	Protect	Vulnerability Exploitation
8.1	Establish and Maintain an Audit Log Management Process	20%	Protect	Undetected Breach
8.2	Collect Audit Logs	20%	Detect	Incident Detection Failure
8.3	Ensure Adequate Audit Log Storage	20%	Protect	Log Tampering
9.2	Use DNS Filtering Services	0%	Protect	Malicious Domain Access
10.3	Disable Autorun and Autoplay for Removable Media	20%	Protect	Malware Spread
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	0%	Protect	Phishing Attacks
15.1	Establish and Maintain an Inventory of Service Providers	20%	Identify	Third-Party Breach

As shown in Table 2, multiple areas require immediate intervention. Therefore, we would next incorporate the PSO prioritization process shown in Figure 1 into the assessment results reflected in Figure 2 and compare the resulting priorities in the form of ranks. It is important to mention that *smaller values in the rank numbers indicate top priorities*.

44 The Data Breach Investigation Report (2024).

Table 3 shows the top ten IG1 priority areas identified by the PSO-based algorithm with compliance levels below 60%. As previously explained, Baseline Ranks indicate the organizations' initial prioritization of each safeguard, and are calculated using the coverage and a set of preestablished ranked weights.[45] On the other hand, Swarm Ranks indicate the priority given to the safeguard by the PSO-based model. This rank considers the priorities established by the optimization function criteria: the community defense model (CDM) and the cost of cybersecurity.

Table 3. Top Ten Priority Safeguard Swarm Recommendations

Safeguard	Coverage	Baseline Rank	Swarm Rank	Priority
1.1	20%	15	1	1
1.2	40%	4	2	2
2.3	40%	9	5	3
3.1	40%	10	6	4
3.2	20%	26	7	5
3.3	20%	28	8	6
3.6	0%	50	11	7
6.4	0%	51	22	8
6.3	0%	52	29	9
4.3	0%	53	30	10

For example, if we analyze safeguard 1.1, we notice that the Baseline Rank is 15. This means the organization has given it a lower implementation priority than safeguards 1.2, 2.3, and 3.1, which have 4, 9, and 10 Baseline Ranks, respectively. In this case, once we factor the cost and the CDM in the PSO algorithm, the Swarm Rank is 1, shifting the priority of implementation from 15 to 1. This means that, based on the PSO algorithm, this safeguard should be implemented in the first order.

The previous table shows variable differences between Baseline Ranks and Swarm Ranks for several safeguards, indicating that the Swarm Ranks redirect the prioritization of these safeguards following the optimization criteria and not the coverage levels. The Swarm Ranks have correlation levels of 0.99 and 0.663 with the CDM and cost criteria, respectively. This indicates that the Swarm Rank sequence is more aligned with the Ranks set by the CDM than with the Cost, which is expected, given the importance of the criteria initially set in the optimization function.

45 Abdulla (2024)

For safeguards with coverage lower than 60%, the Swarm Ranks are always smaller than the Baseline Ranks. This means that these security actions are considered as more important for the PSO decision-making process than the security actions taken by the organization before the risk review. In this case, the UGA CyberArch clinic's recommendations to improve this organization's cybersecurity posture would follow the priority order suggested by the Swarm Ranks, focusing on a gradual increase of each safeguard coverage by 20%. For instance, the safeguards with 0% coverage would be worked out to reach 20% coverage, those with 20% to 40%, and finally those with 40% coverage to 60%.

Conclusions

This study underscores the potential of using swarm intelligence (SI) to guide the implementation of cybersecurity measures. It demonstrates the benefits of combining advanced algorithms with systematic evaluations, making cybersecurity subject-matter expert strategies accessible to resource-constrained organizations. By applying SI algorithms, such as particle swarm optimization (PSO), the study provides real-world insights into enhanced decision-making and strategic planning capabilities, particularly in protecting target-rich, resource-poor organizations from cyber threats.

The research demonstrates that PSO algorithms can help prioritize security actions by analyzing implementation scenarios and security criteria based on real-world data. This optimized prioritization considers essential factors like attack mitigation and the cost of implementation within the CIS Controls V8.0 framework. Moreover, incorporating these factors as decision criteria generates a more practical and actionable trail of steps than just following a list of security criteria.

It is recommended that target-rich, resource-poor organizations continue collaborating with clinics within the Consortium of Cybersecurity Clinics to leverage their knowledge and expertise. Additionally, these organizations should continue strengthening their security programs by systematically evaluating the compliance of their systems against comprehensive frameworks such as the CIS Controls.

Finally, this work is an example of how other cybersecurity clinics could significantly benefit from adopting quantitative methods to better capture the overall cybersecurity posture of their partner organizations and set the base for incorporating advanced numerical algorithms. Furthermore, once the numerical data gathered throughout this process becomes large enough, it could be used to train AI algorithms for multiple purposes, such as extracting hidden information, identifying correlations, and predicting future behavior.

Combining quantitative assessment approaches with SI optimization algorithms could lead to improved risk review outcomes. Future research should investigate the effectiveness of these algorithms in determining implementation priorities for common attack scenarios, such as denial of service, system intrusion, ransomware, and social engineering.

References

Abdulla, H., Bourlai, T., & Lupo, M. (2024). *A CIS Controls V8.0 scoring system using combined ranking-weight metho*ds. In Press, Proceedings of the 18th Annual IEEE SysCon Conference, Montreal, Canada.

Allodi, L., & Massacci, F. (2017). Security events and vulnerability data for cybersecurity risk estimation. In *Risk Analysis* (Vol. 37(8), pp. 1606–1627).

Al-Safwani, N., Fazea, Y., & Ibrahim, H. (2018). ISCP: In-depth model for selecting critical security controls. *Computers & Security*, (vol. *77*, pp. 565–577).

Anastasopoulou, K., Mari, P., Magkanaraki, A., Spanakis, E. G., Merialdo, M., Sakkalis, V., & Magalini, S. (2020). Public and private healthcare organizations: a socio-technical model for identifying cybersecurity aspects. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance* (pp. 168–175).

Bamakan, S. M. H., Amiri, B., Mirzabagheri, M., & Shi, Y. (2015). A new intrusion detection approach using PSO-based multiple criteria linear programming. *Procedia Computer Science* (Vol. *55*, pp. 231–237).

Bejarano, M. H., Rodríguez, R. J., & Merseguer, J. (2021). A vision for improving business continuity through cyber-resilience mechanisms and frameworks. In IEEE *2021 16th Iberian Conference on Information Systems and Technologies* (*CISTI*) (pp. 1–5).

Beni, G. (2020). Swarm intelligence. *Complex Social and Behavioral Systems: Game Theory and Agent-Based Models* (pp. 791–818).

Breier, J., & Hudec, L. (2013, September). On selecting critical security controls. In *Proceeding of the IEEE 2013 International Conference on Availability, Reliability and Security* (pp. 582–588).

Chui, K. T., Liu, R. W., Zhao, M., & Zhang, X. (2024). Bio-inspired algorithms for cybersecurity: a review of the state-of-the-art and challenges. *International Journal of Bio-Inspired Computation*, (vol. *23*(1), pp. 1–15).

Center for Internet Security. (2019). *CIS Controls V7.1*. https://www.cisecurity.org/controls/v7

Center for Internet Security. (2020). *CIS Controls V8.0*. https://www.cisecurity.org/controls/v8

Center for Internet Security. (2024). *CIS Controls V8.1*. https://www.cisecurity.org/controls/v8-1

The Cost of Cyber Defense: CIS Controls Implementation Group 1 (Version 1.0). (2023). https://www.cisecurity.org/insights/white-papers/the-cost-of-cyber-defense-cis-controls-ig1

The Community Defense Model (Version 2.0). (2023). https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

Center for Internet Security. (2024). CIS Critical Security Control Navigator. Online tool. https://www.cisecurity.org/controls/cis-controls-navigator

Crotty, J., & Daniel, E. (2022). Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. *Applied Computing and Informatics* (ahead-of-print).

Cybersecurity and Infrastructure Security Agency. (2020). *Insider threat mitigation guide*. https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide

Department of Health and Human Services. (2023). *Insider health industry cybersecurity practices: Managing threats and protecting patients (2023 edition)*. https://405d.hhs.gov/Documents/HICP-Main-508.pdf

Domínguez-Dorado, M., Carmona-Murillo, J., Cortés-Polo, D., & Rodríguez-Pérez, F. J. (2022). CyberTOMP: A novel systematic framework to manage asset-focused cybersecurity from tactical and operational levels. *IEEE Access*, *10*, 122454–122485.

Eberhart, R. C., Keller, J., Kraft, J., & Verdon, J. (2012, July). Plenary speakers and invited tutorial speakers. In *2012 IEEE Symposium on Computational Intelligence for Security and Defence Applications* (pp. 1–6).

Fischer, E. A. (2005). *Creating a national framework for cybersecurity: An analysis of issues and options* (Order Code RL32777). CRS Report for Congress. Received through the CRS Web.

Fletcher, K. K., & Liu, X. (2011). Security requirements analysis, specification, prioritization, and policy development in cyber-physical systems. In IEEE *2011 Fifth International Conference on Secure Software Integration and Reliability Improvement-Companion* (pp. 106–113).

Frandell, A., & Feeney, M. (2022). Cybersecurity Threats in Local Government: A Sociotechnical Perspective. *The American Review of Public Administration* (vol. *52*(8), pp. 558–572).

Freitas, D., Lopes, L. G., & Morgado-Dias, F. (2020). Particle swarm optimization: a historical review up to the current developments. *Entropy* (vol. *22*(3), pp. 362).

Fujs, D., Mihelič, A., & Vrhovec, S. L. (2019, August). The power of interpretation: Qualitative methods in cybersecurity research. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (pp. 1–10).

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*(1), 183-199.

Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Future Generation Computer Systems*, *105*, 410–431.

Gourisetti, N. G., Mylrea, M., & Patangia, H. (2019, January). Application of rank-weight methods to blockchain cybersecurity vulnerability assessment framework. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0206–0213).

Hadar, E., & Hassanzadeh, A. (2019, September). Big data analytics on cyber attack graphs for prioritizing agile security requirements. In *2019 IEEE 27th International Requirements Engineering Conference (RE)* (pp. 330–339).

Hassan, R., Cohanim, B., De Weck, O., & Venter, G. (2005). A comparison of particle swarm optimization and the genetic algorithm. In *Proceedings 46th AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics and materials conference* (CCWC) (p. 1897).

Kennedy, J., & Eberhart, R. (1995, November). Particle swarm optimization. In *Proceedings of ICNN'95-international conference on neural networks* (Vol. 4, pp. 1942–1948). Perth, WA, Australia https://doi.org/10.1109/ICNN.1995.488968

Kennedy, J., & Eberhart, R. C. (1997, October). A discrete binary version of the particle swarm algorithm. In *1997 IEEE International conference on systems, man, and cybernetics. Computational cybernetics and simulation* (Vol. 5, pp. 4104–4108).

Kim, A., Kang, M. H., Luo, J. Z., & Velasquez, A. (2014). A framework for event prioritization in cyber network defense. *DTIC Document*.

Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security* (vol. *108*, pp. 102376).

Lippmann, R. P., Riordan, J. F., Yu, T. H., & Watson, K. K. (2012). Continuous security metrics for prevalent network threats: introduction and first four metrics. *Lincoln Laboratory, MIT*.

Lourens, M., Dabral, A. P., Gangodkar, D., Rathour, N., Tida, C. N., & Chadha, A. (2022, December). Integration of AI with the Cybersecurity: A detailed Systematic review with the practical issues and challenges. In *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 1290–1295).

Lupo, M., Abdulla, H. (2023). *The UGA CyberArch Program – An Experiential Learning Opportunity*. The 32nd UGA Annual Public Service and Outreach Meeting and Award Luncheon. Training Day Presentation. Athens, GA.

Marchany, R. (2021). *What's new with the CIS Controls V8?* SANS Institute Webcasts. https://www.sans.org/webcasts/what-s-new-with-the-cis-controls-v8/

Massachusetts Institute of Technology (2021). *Cyber Security for Critical Urban Infrastructure*. Online Course. https://mitxonline.mit.edu/courses/course-v1:MITxT+11.S198x/

MITRE ATT&CK. Online Database. https://attack.mitre.org

Munteanu, A. (2006). Information security risk assessment: The qualitative versus quantitative dilemma. In *Managing Information in the Digital Economy: Issues & Solutions-Proceedings of the 6th International Business Information Management Association (IBIMA) Conference* (pp. 227–232).

National Institute of Standards and Technology. (2021). *NIST Special Publication 800-160, Volume 2: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-160v2r1

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments: SP 800-30 Revision 1*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800–53, Revision 5). https://doi.org/10.6028/NIST.SP.800-53r5

Norris, D., Joshi, A., & Finin, T. (2015). Cybersecurity challenges to American state and local governments. In *15th European Conference on eGovernment* (pp. 196–202). Academic Conferences and Publishing Int. Ltd.

Park, K. C., & Shin, D. H. (2017). Security assessment framework for IoT service. *Telecommunication Systems* (vol. *64*, pp. 193–209).

Priyanka, J., & Ramakrishnan, M. (2023). Security Establishment In Cybersecurity Environment Using PSO Based Optimization. *Wireless Personal Communications* (Vol. *129*(3), pp. 1807–1828).

Salinesi, C., & Kornyshova, E. (2006). Choosing a Prioritization Method-Case of IS Security Improvement. In *CAiSE Forum*.

Shami, T. M., El-Saleh, A. A., Alswaitti, M., Al-Tashi, Q., Summakieh, M. A., & Mirjalili, S. (2022). Particle swarm optimization: A comprehensive survey. *IEEE Access* (vol. *10*, pp. 10031–10061).

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security*, *90*, 101709.

Tarala, J. (2023). *Cybersecurity Standards Scorecard* (*2023 Edition*). SANS Institute Webcasts. https://www.sans.org/webcasts/cybersecurity-standards-scorecard-2023-edition/

Teodoro, N., Gonçalves, L., & Serrão, C. (2015). NIST Cybersecurity Framework Compliance: A generic model for dynamic assessment and predictive requirements. In *2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, pp. 418-425). https://doi.org/10.1109/Trustcom.2015.402

The Consortium of Cybersecurity Clinics (2024). https://cybersecurityclinics.org/

Truong, T. C., Huynh, T. P., & Zelinka, I. (2020). Applications of swarm intelligence algorithms countering the cyber threats. In *Proceedings of the 2020 Genetic and Evolutionary Computation Conference Companion* (pp. 1476–1485). https://doi.org/10.1145/3377929.3398119

Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber Risk Assessment and Optimisation: A Small Business Case Study. *IEEE Access*, (vol. 11, pp. 44467–44481)

U. S. Department of Defense (2023). *Cybersecurity Maturity Model Certification 2.0*. https://dodcio.defense.gov/CMMC/Model/

UGA MILAB (2024). https://milab.uga.edu/

Verizon. (2023). *2023 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/2023/2023-data-breach-investigations-report-dbir.pdf

Verizon. (2024). *2024 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

Wang, Y., & Yang, Y. (2009). Particle swarm optimization with preference order ranking for multi-objective optimization. *Information Sciences, 179*(12), 1944–1959. https://doi.org/10.1016/j.ins.2009.01.005

White, G. B., Dietrich, G., & Goles, T. (2004). Cyber security exercises: testing an organization's ability to prevent, detect, and respond to cyber security events. In *Proceedings of the* IEEE *37th Annual Hawaii International Conference on System Sciences, 2004.* (pp. 10–pp).

Acknowledgments

We would like to express our gratitude to all those who contributed to the successful completion of this project. First, we thank the UC Berkeley Center for Long-Term Cybersecurity for the generous funding, which provided financial support for our research and development efforts. Our heartfelt appreciation goes to the UGA CyberArch interns for their dedication and hard work during the on-site visits and data gathering. Their invaluable contributions and involvement have been instrumental in driving this project forward. We would also like to thank Google for supporting the UGA CyberArch cybersecurity clinic. This support has enabled us to expand our research capabilities, enhancing our cybersecurity initiatives. Finally, we would like to acknowledge the use of Grammarly and ChatGPT 4 to improve the fluency of some text sentences, ensuring clarity and coherence throughout the document.

About the Authors

Hayat Abdulla Asad Cue is a Ph.D. Student in Electrical and Computer Engineering at the University of Georgia. She is also a Graduate Research Assistant in the UGA CyberArch program at the Carl Vinson Institute of Government (CVIOG). Her research focuses on applying engineering principles to the fields of cybersecurity and public service and outreach. Before pursuing her doctoral studies, she was an assistant professor at the Electronic and Circuits Department at Simon Bolivar University, Caracas, Venezuela, where she taught Signals and Communication Systems, Circuits, and Electrical Measurement Courses. She holds a Master's in Biomedical Engineering from Simon Bolivar University and a Bachelor's in Telecommunication and Electronic Engineering from ISPJAE, Havana, Cuba.

Thirimachos Bourlai is an Associate Professor at the School of Electrical and Computer Engineering, a Courtesy Faculty at the School of Computing, and an Adjunct Faculty at the Institute for Artificial Intelligence, all at the University of Georgia. In addition to his academic role, he holds a Joint Appointment with the Savannah River National Labs. Dr. Bourlai serves as an adjunct faculty at West Virginia University (WVU) in the Lane Department of Computer Science and Engineering, as well as in the School of Medicine. He is the founder and director of the Multi-Spectral Imagery Lab and holds significant editorial roles. Dr. Bourlai is a Series Editor for Advanced Sciences and Technologies for Security Applications, an Associate Editor for the Elsevier Pattern Recognition Journal, and the IET Electronics Letters Journal. In the realm of organizational leadership, he is a member of the Board of Directors at the Document Security Alliance, the former VP of Education of the IEEE Biometrics Council, and a member of the Academic Research and Innovation Expert Group of the Biometrics Institute. Dr. Bourlai's substantial research contributions are evident in his authorship of five notable books with Springer, including "Face Recognition Across the Imaging Spectrum" (2016 / 1st Edition, 2024 / 2nd Edition), "Surveillance in Action" (2018), "Securing Social Identity in Mobile Platforms" (2020), and "Disease Control through Social Network Surveillance" (2022). Complementing his innovative work are three patents and a prolific publication record, encompassing over 140 contributions to journals, conferences, book chapters, and magazines in the domains of computer vision, biometrics, and related fields.

Mark Lupo is a Senior Public Service Associate with the Carl Vinson Institute of Government, Information Technology Outreach Service (CVIOG ITOS) and serves as the UGA CyberArch Coordinator. He joined The University of Georgia Small Business Development Center in Columbus in 2005 as a Business Consultant, was promoted to Area Director for the Columbus office in July 2012 and to the State Office as the Business Education and Resilience Specialist in November 2018, transferring to CVIOG ITOS in July 2022. Mr. Lupo is passionate about working with community organizations and helping others identify the path and the resources needed to develop a stronger cybersecurity infrastructure and posture against a rising threat landscape.


CLTC
Center for Long-Term
Cybersecurity
UC Berkeley