IJICTR
International Journal of Information & Communication Technology Research

Volume 17- Number 1 – 2025 (50-62)

A Novel Framework for Cyber Situational Awareness at the National Level

Fatemeh Imanimehr
Network Faculties
ICT Research Institute (ITRC)Tehran, Iran
f.imanimehr@itrc.ac.ir

Alireza Enayati
Network Faculties
ICT Research Institute (ITRC)
Tehran, Iran
enayati@itrc.ac.ir

Hossein Gharaee*
Network Faculties
ICT Research Institute (ITRC)
Tehran, Iran
gharaee@itrc.ac.ir

Received: 24 June 2024 – Revised: 17 July 2024 - Accepted: 4 October 2024

Abstract—**In response to the critical need for protecting critical infrastructure and managing cyber crises, this article introduces an operational framework for establishing national-level Cyber Situational Awareness (Cyber SA). The Information Sharing and Alerting System (ISAS), as the central authority, integrates the cyber situational awareness postures of Information Sharing and Analysis Centers (ISACs) across infrastructures, forming a unified international Cyber SA posture. Our framework offers a quantifiable and coherent metric for national-level Cyber SA, based on cybersecurity risk, determined by the impact of cyber threats on sector-specific macro missions and their interdependencies. Application to cyberattack scenarios demonstrates the framework's accuracy in reflecting situational dynamics and assessing the relative significance of different sectors and ISACs. In summary, our framework simplifies national Cyber SA measurement, enhances cyber crisis management and decision-making, and systematically addresses interdependencies among critical infrastructures.**

Keywords: cyber situational awareness at national level, macro missions, national cyber SA framework, ISAC traffic, Critical infrastructure.

Article type: Research Article

Publisher: ICT Research Institute

I. INTRODUCTION

In the modern era, thriving societies are built upon a complex web of critical infrastructure systems. These essential networks—delivering vital services such as water, electricity, and transportation—sustain not only our economic prosperity but also the very fabric of communal life [1,2,3].

Recent incidents in 2023 have underscored the vulnerabilities inherent in these infrastructures, highlighting the urgent need for secure and resilient systems. For example, a fire at the Isfahan Power Plant in Iran illustrated the importance of effective crisis management and rapid response, exposing the fragility of essential services. Similarly, a gas shortage during Iran's harsh winter led to widespread power outages and civil unrest, further emphasizing this vulnerability [5]. These events demonstrate how local disruptions can trigger cascading effects, resulting in chaos and economic losses at both national and international levels.

Critical infrastructure sectors form the foundational framework of modern societies, influencing numerous facets of life, including economic stability, community well-being, governance, and national security. The risk of failure in one critical infrastructure leading to a

* Corresponding Author

series of failures across others is a well-documented phenomenon. This is particularly evident in energy infrastructure, characterized by its extensive interconnectivity; a single disruption can initiate a domino effect, undermining the integrity and security of the entire network. For instance, a cyberattack on the electrical grid could lead to widespread power outages, impacting water treatment facilities, oil and gas operations, and even nuclear plants. The consequences can be severe, threatening economic stability, environmental safety, societal welfare, and national security.

Research has highlighted the significant risks associated with such cascading failures. A model proposed in [6] evaluates the risk of common-cause failures in critical infrastructures, revealing that these situations can be highly impactful, sometimes even more devastating than the cascading effects of high-order dependencies. Additionally, a study by Gibson et al. [7] examined the cascading effects of coastal flooding due to climate change on critical infrastructure in Torbay, UK. Utilizing a 3D visualization tool, the study demonstrated that failures in the electricity network had far-reaching consequences on water, transportation, healthcare, and emergency response systems, estimating both economic losses and recovery times for each infrastructure. These findings underscore the importance of understanding and quantifying the cascading effects of risks in critical infrastructures, as well as developing strategies to enhance their resilience and security.

Cyber crises can emerge from threats to critical infrastructure, leading to widespread disruptions of essential services and posing significant national security risks. Effective management and rapid response are crucial to preventing further escalation. By enhancing national cyber situational awareness, decision-makers can better detect, understand, and mitigate such threats, thereby strengthening crisis response and resilience [1,2,3].

In this study, we introduce an innovative framework for creating a national cyber situational awareness platform, taking into account the cascading effects of disruptions. In this study, we introduce an innovative framework for creating a national cyber situational awareness platform. This platform is designed with a clear mission focus [8,9,10] and provides a comprehensive national cybersecurity score to articulate cyber situational awareness effectively. Unlike conventional solutions that primarily focus on analyzing individual systems or components, our methodology shifts the spotlight to the missions and objectives inherent to each critical infrastructure sector, unveiling their intricate interconnections and mutual dependencies. Our definition of a 'mission' encapsulates a series of precisely orchestrated tasks or activities aimed at achieving specific objectives within a critical infrastructure sector.

At the heart of our approach lies a groundbreaking model based on 'mission consistency.' Mission consistency, as we define it, quantifies the degree to which the missions of various critical infrastructure sectors align and harmonize with each other. We contend that mission consistency plays a pivotal role in achieving national-level cyber situational awareness. It serves as a mirror reflecting the intricate interdependencies and relationships woven across diverse critical infrastructure sectors. By measuring and enhancing mission consistency, we can strengthen coordination and collaboration among stakeholders while proactively anticipating and mitigating potential consequences stemming from cyber incidents. These incidents have the potential to ripple across the broader landscape, affecting the performance and functionality of critical infrastructures. Our model for mission consistency is comprised of three fundamental components:

- Mission Importance: Signifying the criticality and indispensability of a mission within a given critical infrastructure sector.
- Mission Dependency: Indicating the degree to which a mission hinges on or influences other missions.
- Risk Score: Conveying the probability and impact of cyber threats or attacks targeting missions or a specific mission.

The principal contributions of this paper encompass:

- The proposition of a pioneering approach to craft a mission centric national cyber situational awareness platform.
- The introduction of an innovative model rooted in mission consistency for the measurement and enhancement of national-level cyber situational awareness.
- The practical implementation of a prototype system based on our proposed approach and model, incorporating real-world data from a multitude of sources.
- The rigorous evaluation of our prototype system through simulations, coupled with a comprehensive comparative analysis against existing solutions.
- A thorough exploration of the advantages, limitations, and promising future avenues stemming from our proposed approach and model.

The rest of this paper is organized as follows: Section 2 provides an exhaustive review of pertinent literature on cyber situational awareness at the national level. Sections 3 and 4 expound on the intricacies and nuances of our proposed approach and model. Section 5 unveils the practical implementation and exhaustive evaluation of our prototype system. Section 6 presents challenges and limitations in establishing national SA. Finally, Section 7 concludes the paper with a comprehensive summary, followed by a discussion of potential future work.

II. Related Works

In this section, we delve into a comprehensive review of the state-of-the-art in cyber situational awareness at the national level.

According to Endsley [11], situational awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. Cyber situational awareness refers to the understanding of cybersecurity risks and vulnerabilities affecting the IT environment, as well as the ability to anticipate the potential impacts of these threats [12]. It empowers organizations to gather, analyze, and respond to threat data, thereby enhancing their cyber defense and cyber security risk management capabilities. In this paper, cybersecurity risk, abbreviated as 'risk,' refers to the potential for financial loss, disruption, or damage to a firm's reputation resulting from failures in its information technology systems due to cyber-attacks [13]. Risk assessment [15] supports cyber situational awareness by identifying threats (perception), analyzing their impact (comprehension), and forecasting future risks (projection), aligning with the Endsley model's levels. This integration helps in anticipating security challenges and making informed decisions.

A. *Developing a National Cyber Situational Awareness Platform: Challenges and Solutions*

Cyber situational awareness constitutes the capability to grasp the current landscape of cyber threats and vulnerabilities within a given environment while foreseeing potential repercussions on various objectives and missions [16]. It is crucial for protecting critical infrastructures from cyberattacks that can disrupt their normal operations, cause physical damage, or compromise sensitive data. Such attacks can have severe consequences for national security, public safety, economic stability, and social welfare. Therefore, it is essential to develop a national cyber situational awareness platform that can provide a holistic view of the cyber status and potential impacts of cyber incidents across different sectors and domains [16]. Such a platform can enable timely detection, assessment, mitigation, and recovery of cyber incidents, as well as facilitate coordinated response actions among various stakeholders [16]. However, developing a national cyber situational awareness platform poses several challenges, such as: How to collect, integrate, analyze, and share cyber information from diverse sources? How to ensure the quality, reliability, security, and privacy of cyber information? How to model the interdependencies and cascading effects among critical infrastructures? How to predict the future scenarios and outcomes of cyber incidents? How to alert the relevant stakeholders and provide actionable recommendations? How to cope with the dynamicity, complexity, uncertainty, and scalability of cyber situations? Several solutions have been proposed to address these challenges, such as: using data fusion techniques to combine cyber information from multiple sources [17]; using ontologies and semantic web technologies to represent and reason about cyber information [17]; using graph theory and network analysis to model and analyze the interdependencies among critical infrastructures [18]; using simulation and optimization methods to predict and mitigate the impacts of cyber incidents [19]; using alert generation and dissemination mechanisms to notify and advise the stakeholders [20]; using adaptive and scalable architectures to cope with the changing and growing cyber situations [21].

In [22] the authors aim to provide a framework for national cybersecurity awareness that helps governments and organizations better understand cyber threats and respond effectively. The article highlights the role of education, information sharing, and collaboration between various sectors (government, critical infrastructure, and organizations). It emphasizes that national cybersecurity awareness requires a comprehensive and integrated approach to protect national interests.

B. *Mission-Centric Approach to Cyber Situational Awareness*

The majority of existing solutions predominantly target the system or component level of cyber situational awareness, overlooking the mission or objective level [8,9,10]. They often fail to consider the missions or goals of individual critical infrastructure sectors and their intricate interrelationships. These solutions fall short in measuring or enhancing the consistency and compatibility of missions concerning their cyber status and potential impacts. Consequently, they do not provide a comprehensive depiction of national cyber situational awareness that encapsulates the interdependencies and relationships among distinct critical infrastructure sectors.

In contrast, our work introduces a groundbreaking model designed to calculate cyber situational awareness at the national level. This model centers around the concept of macro missions and ISACs (Information Sharing and Analysis Centers). Macro missions represent the core functions or objectives of each critical infrastructure sector essential for their operation and service delivery. ISACs, on the other hand, are non-profit organizations tasked with coordinating cyber information sharing and analysis among their sector members. Our model seamlessly amalgamates current threats and ISAC situational awareness scores for each sector and its macro missions, incorporating weights and dependence coefficients. The result is a quantifiable and coherent measure of cyber situational awareness at the national level.

Our work extends beyond theory into practical application. We applied our model to ten distinct cyberattack scenarios, which we present and discuss in detail in section 4.

III. Cyber Situational Awareness at the National Level

Effective crisis management in the realm of cybersecurity necessitates a powerful tool, one that can provide a comprehensive understanding of the national cyber landscape. This tool is known as "cyber situational awareness," a concept that aims to create a dynamic and evolving picture of the national cyber environment. At its core, cyber situational awareness at the national level seeks to identify potential crises by

assessing the interdependencies among critical infrastructures.

While various definitions of situational awareness exist, they all offer unique insights and build upon the foundational concept introduced by Endsley [23]. For instance, Stiffler [25] applies this concept to military operations, defining situational awareness as "the ability to see and understand the current and near future situation for friendly forces and enemy forces". This interpretation emphasizes the importance of understanding both the present and the anticipated future states of relevant elements in the environment. Similarly, Pio [25] expands on Endsley's concept by identifying specific dimensions of situational awareness, such as spatial awareness, goal-oriented understanding, system comprehension, resource awareness, and force awareness. These dimensions provide a more detailed framework for understanding situational awareness, further illustrating the depth and complexity of this concept.

Building upon Endsley's definition, cyber situational awareness at the national level, particularly in the context of mission-based analysis, becomes a crucial tool for gathering information related to incidents, crises, threats, and the degree of risk in the missions. This comprehensive collection of data allows for a deeper understanding of the interdependencies among critical infrastructures and their respective missions. Furthermore, it enables the comprehension of the current state of risk in these missions. Looking ahead, it facilitates the projection of near-future states of these missions, including the potential cascading effects of the risk of one mission on others. This comprehensive approach to cyber situational awareness, therefore, provides a solid foundation for informed decision-making. It not only considers the current cybersecurity landscape but also anticipates future scenarios, thereby enhancing the resilience of critical infrastructures.

Cyber situational awareness (Cyber SA) is the ability to understand and anticipate the cyber environment and its impact on the missions and objectives of an entity [14]. To achieve this goal, the hierarchy of cyber-SA At the national level, abstractly, can be understood as a multi-tiered system that involves three levels: national, critical infrastructure, and organizational. Each level has different roles and responsibilities in forming and maintaining cyber-SA and different sources and types of information to support their decision-making.

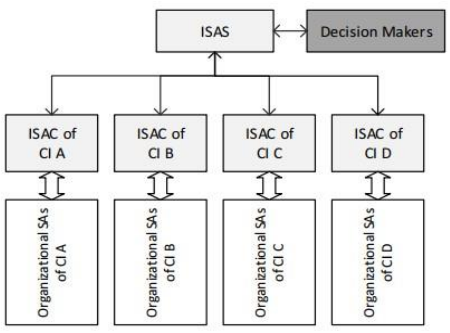

Figure 1. Hierarchy of Cyber Situational Awareness: From Organizational to National Level [14].

As depicted in Figure 1, the foundational entities in our conceptual architecture are those that contribute to organizational situational awareness. Each organization contributes to its own Situational Awareness (SA) by disseminating information amongst relevant sectors. Every Critical Infrastructure (CI) is equipped with its own Information Sharing and Analysis Center (ISAC). An ISAC serves as a node within a CI, enhancing situational awareness by collecting data on cyber threats and facilitating two-way information exchange between the CI and its associated private and public organizations. At the apex of this structure, contributing to national-level cyber situational awareness is the Information Sharing and Alerting System (ISAS). ISAS collates SA data from a variety of infrastructures and disseminates this information to ISACs of other infrastructures after updating the national situational awareness. This tiered structure ensures a holistic and synchronized approach towards maintaining national cyber situational awareness. In [14], the conceptual architecture of the ISAS system is outlined, providing a detailed explanation of the system's key components and their interrelationships.

The process of generating cyber situational awareness at the organizational level [25] involves certain steps, where we can map the awareness gained from these steps to the levels of awareness in the Endsley model [22]: perception, comprehension, and projection. This process begins with observing events and incidents, which corresponds to the perception level. The organization then extracts features and processes patterns from these observations, leading to content processing and decision-making, which aligns with the comprehension level. Finally, the organization monitors the effectiveness of missions and takes action to control, determine the source, manage, and respond to the incident, which falls under the projection level. For instance, Security Operations Centers (SOCs) within an organization could use various tools and techniques to detect and analyze cyber-attacks, assess their impact on the mission objectives, and implement appropriate countermeasures [2, 26]. This approach ensures a comprehensive and coordinated effort to maintain cyber situational awareness at the organizational level.

Moving up to the infrastructure level, the same three key levels of Endsley's model - perception, comprehension, and projection - are applied. The process begins with pre-processing data generated from SOCs at organizational levels, aligning with the perception level. The infrastructure then evaluates and refines the status of missions, which determines the current situation of the infrastructure, corresponds to the comprehension level. Finally, the infrastructure makes decisions about the cyber situational awareness and the next status of missions, and monitors the state of the infrastructure territory, falling under the projection level. In addition, the infrastructure level could coordinate and collaborate with other infrastructures to share information and resources, thereby enhancing the overall resilience and security of the critical systems. This approach ensures a comprehensive and coordinated effort to maintain cyber situational awareness at the infrastructure level.

At the national level, maintaining cyber situational awareness also adheres to Endsley's model, involving the three key levels: perception, comprehension, and projection. The process commences with receiving information about incidents and crises of critical infrastructure missions at the national level in time and space intervals, aligning with the perception level. The national level then interprets and understands threat information to deal with crises, corresponding to the comprehension level. Lastly, the national level determines the levels of dependence between infrastructure missions in continuous events and visualizes the future state of the infrastructure mission in the near future, falling under the projection level. For instance, the national level could use predictive models and simulations to forecast the potential outcomes and risks of different scenarios and to plan and execute the best course of action. This approach ensures a comprehensive and coordinated effort to maintain cyber situational awareness at the national level.

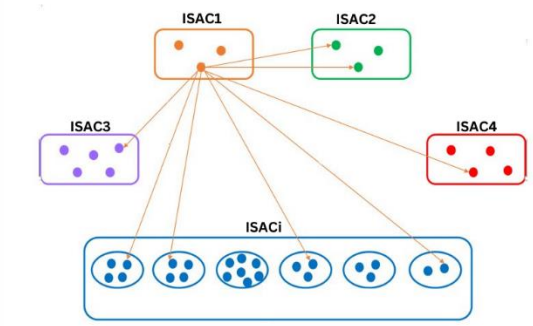

Figure 2. Interdependencies among critical infrastructures

As shown in Figure 2, the missions of the ISACs are interconnected, creating a complex network of dependencies. Each ISAC focuses on its own mission, gathering and analyzing information related to its specific critical infrastructure. However, due to the interdependencies between different missions, the actions taken by one ISAC can have significant effects on others.

Managing these dependencies is a complex task that goes beyond the capabilities of individual ISACs. This is where the ISAS becomes operative. Operating at a higher level, the ISAS has a comprehensive view of the entire network of ISACs and their missions. It receives situational awareness information from various infrastructures and updates the national situational awareness accordingly. By doing so, the ISAS can effectively manage the dependencies between different missions, ensuring a coordinated response to cyber threats and enhancing the overall resilience and security of the critical systems. This highlights the crucial role of the ISAS in maintaining national cyber situational awareness.

IV. Proposed Solution

The significance of cyber situational awareness is particularly pronounced at the national level, as it directly impacts the functioning and stability of critical infrastructure systems that underpin our modern society [11]. These systems are interconnected and interdependent, forming a complex network that is susceptible to cascading failures and adverse effects resulting from cyberattacks. Consequently, policymakers and practitioners face the crucial task of calculating the national cybersecurity score by considering the dependency network of these critical infrastructure systems. However, there is currently a dearth of a comprehensive and systematic framework to measure and assess the national cybersecurity score in relation to the interconnections of critical infrastructure systems.

Generally, National Cyber SA Posture refers to the comprehensive understanding and real-time awareness of the state of cybersecurity at the national level. It involves the aggregation and analysis of information from various sources, including government agencies, private sector organizations, and intelligence entities, to provide a holistic view of the cyber threat landscape. In the mission centric view [8,9,10], which is considered in this paper, the National Cyber SA Posture is defined as the assessment of how cybersecurity threats affect the missions of critical infrastructures. The objective of the National Cyber SA Posture is to present a comprehensive view of the condition of these critical infrastructure missions and to evaluate the impact of cyber threats on their effectiveness.

The national cybersecurity score quantifies the extent to which critical infrastructures are exposed to cyber threats and the degree to which these threats have disrupted the missions of these infrastructures. Essentially, the national cybersecurity score indicates the level of risk in the missions [15] of critical infrastructures. This risk is not only due to direct cyber threats but also includes risks resulting from dependencies on other missions that have been disrupted. Therefore, the national cybersecurity score provides a comprehensive view of the overall impact of cyber threats on the functioning of critical infrastructures. It takes into account both the direct effects of cyber threats and the cascading effects resulting from interdependencies among different missions. This score is crucial for assessing a country's vulnerability to cyber threats and its ability to maintain the functioning of its critical infrastructures in the face of such threats. National cyber situational awareness posture is numerically expressed as the national cybersecurity score.

Our proposed solution, as depicted in Figure 1, is based on the hierarchy of situational awareness. In this abstract model, ISAS is connected to all ISACs, while there isn't necessarily a direct relationship between ISAS and the organizational levels of situational awareness. For the effective operation of ISAS, each ISAC must provide ISAS with the following information in the form of situational awareness posture of the relevant infrastructure when faced with a threat:

1. The ISAC cybersecurity score of the relevant infrastructure reflects the extent to which the missions of the critical infrastructures are implicated in cyber threats and the degree of risk these threats pose to the infrastructures' missions.

2. A list of observed threats that have an impact on the missions of relevant infrastructure. For each threat, the information includes:

- Details of threat information, including the type of attack, attacker, campaign, malware, and tools used by the attacker [27].
- The threat exposure phase
- The threat risk score
- The threat risk score per mission, which quantifies the potential impact of cyber threats on the specific objectives of each critical infrastructure mission. [28]

The threat exposure phase indicates the stage of the threat lifecycle that the infrastructure is currently facing [29]. It is divided into five distinct stages: Identify, Protect, Detect, Respond, and Recover. Each of these stages carries a different weight, reflecting their relative importance in the process of maintaining cyber situational awareness. ISAC updates the risk score of the threat at different threat exposure phase and immediately sends it to ISAS. Threats with an impact are those for which a risk score greater than zero has been calculated.

To establish the missions of infrastructure and interdependencies, we undertook extensive surveys, research studies, and expert interviews within various sectors to identify their macro missions and interdependencies. Additionally, in our methodology, we assign initial weights to the submissions based on their perceived importance and the degree of dependency. It is crucial to note that these initial weights are not static; they are designed to be updated in response to the empirical performance of the framework. This dynamic adjustment ensures that the model remains accurate and reflective of the actual operational environment. The weights play a pivotal role in our analysis, as they determine the influence of each sub-mission on the overall mission dependency. By continuously refining these weights, our framework can adapt to changing conditions and maintain its effectiveness in assessing the resilience of critical infrastructures.

To ascertain the interdependencies between missions with greater precision, we deconstructed each mission into its constituent sub-missions. The inter-mission dependence is then determined by a weighted aggregation of the dependency degrees of these sub-missions. This method allows for a nuanced analysis of how disruptions in one area can propagate through the network of missions. For example, if a sub-mission within the energy sector's macro mission—such as maintaining the operational integrity of the power grid—is compromised, it can be quantitatively assessed how this perturbation might influence a sub-mission in the transportation sector, like the functionality of traffic control systems.

Upon receiving the situational awareness information from each ISAC, ISAS promptly computes a new situational awareness posture. The cyber situational awareness posture at the national level encompasses several key components:

1. National Cybersecurity Score

2. National cybersecurity score of different infrastructures

3. The risk of the missions of different infrastructures

4. The impact of risk of a mission of an infrastructure on the missions of other infrastructures

5. The risk of missions affecting the risk of other missions

In calculating the cyber situational awareness at the national level, certain considerations are taken into account:

Critical infrastructures are essential components of the built environment that ensure the interconnectivity and good operability of any major urban area. Examples of critical infrastructures include transportation, energy, health care, and communication systems. The national value of each critical infrastructure depends on how much it contributes to the overall security and the functioning of society's vital systems. In our proposed solution, we assign a value coefficient to each infrastructure to reflect its relative importance and resilience. The value coefficient is determined by considering the impact, vulnerability, and interdependency of each infrastructure on national security and public welfare. Likewise, the missions of each critical infrastructure have different significance for protecting cyber assets from the viewpoint of cyber situational awareness. Cyber situational awareness is the ability to monitor, analyze, and respond to cyber threats and incidents in real-time. Therefore, our solution aims to enhance the cybersecurity and resilience of critical infrastructures by using the value coefficient as a guide for prioritizing and allocating resources.

The missions of each critical infrastructure vary depending on the nature and function of the sector [30]. For instance, the mission of the transportation sector is to ensure the safe and efficient movement of people and goods, while the mission of the energy sector is to provide reliable and affordable power supply. However, both sectors face similar cyber threats, such as ransomware attacks, denial-of-service attacks, or sabotage attacks, that could disrupt their operations and cause significant economic and social impacts. Therefore, our solution assigns a high-value coefficient to these sectors, and prioritizes the protection of their cyber assets, such as control systems, sensors, or networks, from potential attacks. Our solution also provides them with real-time cyber situational awareness, which enables them to detect, analyze, and respond to any cyber incident that may occur, and to coordinate with other sectors and authorities to mitigate the consequences. In this way, our solution helps these sectors to achieve their missions and to maintain their security and resilience.

In the subsequent sections, we provide an in-depth exploration of our methodology. We begin by delineating the critical infrastructure sectors, elucidating their macro missions, and illuminating the web of interdependencies. Finally, we present our methodology for calculating national situational awareness, both for individual sectors and their constituent macro missions.

A. *Calculation of National Cyber Situational Awareness*

Some definitions and basic assumptions:

- I: Number of critical infrastructures
- M_i: Number of Missions in Infrastructure No. i.
- W_i: Coefficient representing the value and importance of each infrastructure sector or element. It satisfies the condition: $\sum_{i=1}^{I} W_i = 1$
- m_j^i: Coefficient representing the value and importance of mission number j from infrastructure i. It satisfies the condition: $\sum_{j=1}^{M_i} m_j^i = 1$ and $\sum_{i=1}^{I}\sum_{j=1}^{M_i} m_j^i = I$
- $(RS_x^i, RS_x^{i,1}, \dots, RS_x^{i,Mi})$: The understanding of risk state 'x', which is linked to infrastructure 'i', encompasses the following elements:
  - RS_x^i: Total risk score of threat x reported from infrastructure i
  - $RS_x^{i,j}$: The amount of threat risk score per mission number j in infrastructure i related to the threat x

To calculate the threat score at the ISAS level, it's crucial to consider that similar threats may be reported from various infrastructures. Therefore, the risk associated with the threat across all infrastructures is factored in. Additionally, for visualization and future prediction, we take into account the impact of disrupted missions caused by this threat on other missions. Moreover, to normalize the threat score and align it with the importance of the reporting infrastructure, it's multiplied by the coefficient corresponding to the exposure mode weight. Formula (1) outlines the calculation process for threat situational awareness at the national level.

$$RS_x^{isas} = \sum_{i=1}^{I}(w_i \times WS_x^i \times RS_x^i) + dep_x^i \quad (1)$$

Here, WS_x^i represents the weight of the exposure mode reported by ISAC, and its values are determined as per Table 1. RS_x^i stands for the threat score reported by ISAC number i. Lastly, dep_x^i indicates the value that specifies the impact of risks in the missions of infrastructure number i due to threat x on the missions of other infrastructures. The method for calculating this value will be explained further below.

TABLE I. WEIGHT RELATED TO DIFFERENT EXPOSURE SITUATIONS IN A THREAT

exposure mode	WS
Identify (ID)	W_I
Detect	W_D
Respond	W_{res}
Recover	W_{rec}

Formula (2) illustrates how we calculate the dependence coefficient (dep) for infrastructure number i concerning threat x and its impact on the missions of other infrastructures. In this equation: m_j^i is the coefficient representing the value and importance of mission number j in infrastructure number i. $RS_x^{i,j}$ stands for the threat risk score per mission number j in infrastructure number i due to threat x. B_j^i signifies the extent of dependence of missions from other infrastructures on mission number j in infrastructure number i.

$$dep_x^i = \sum_{j=1}^{M_i}(m_j^i \times RS_x^{i,j} \times B_j^i) \quad (2)$$

Formula (3) details how we calculate the weight of dependence B_j^i for the jth mission in infrastructure i concerning its reliance on missions from other infrastructures. In this equation: $me_{l,k}^{j,i}$ denotes the weight of dependence of mission j in infrastructure i on mission l in infrastructure k, as determined by experts. m_l^k represents the coefficient of value and importance of mission number l in infrastructure number k. This complex interplay allows us to assess the dependencies between missions across different infrastructures, crucial for accurate threat score calculations.

$$B_j^i = \sum_{k=1,k\neq i}^{I} w_k \sum_{l=1}^{Mk} m_l^k me_{l,k}^{j,i} \quad (3)$$

B. *Calculating the cyber situation at the national level*

The calculation of the national cyber situation based on the score of current threats has an effect that is new at the ISAS level. And the reported cyber situation of infrastructures is done according to formula 4.

$$SA_{ISAS} = w_{CT}\sum_{x\in(current\ threats)} RS_x^{ISAS} + w_{SA_{ISAC}}\sum_{i=1}^{I}(wi \times SA_{ISAC_i}) \quad (4)$$

Where:

- SA_{ISAS} is the cybersecurity score of the national cyber SA calculated by ISAS
- w_{CT} is the weight assigned to the current threats component of the formula
- RS_x^{ISAS} is the risk score of the x-th current threat calculated by formula 1
- $w_{SA_{ISAC}}$ is the weight assigned to the ISAC situational awareness component of the formula
- W_i is the weight assigned to the i-th ISAC
- SA_{ISAC_i} is the situational awareness score reported by the i-th ISAC

The current threats component of the model represents the current level of exposure and potential damage of the national cyber situation to cyber threats. The ISAC situational awareness component of the model represents the current level of awareness and preparedness of each sector to cyber threats. The weights assigned to each component and each ISAC reflect their relative importance or contribution to the national cyber situation. The weights are determined by using a multi-criteria decision analysis method based on expert judgment.

In this section, we will discuss some of the advantages and limitations of using our model for calculating the cyber situation at the national level.

One of the advantages of using our model is that it can capture the dynamic and complex nature of the cyber situation by considering both the current threats and the ISAC situational awareness. For instance, our model can reflect how a new threat or a change in ISAC awareness can affect the national cyber situation score.

One of the limitations of using our model is that it relies on the quality, accuracy, timeliness, and completeness of the data collected and reported by ISAS and ISACs, which may vary or be inconsistent across different sources and levels. For example, some ISACs may have more or less data than others, or some data may be outdated or inaccurate.

In the hierarchical model presented, it is assumed that ISAS is connected with ISACs of critical infrastructures and only receives significant and impactful threats from them. Given that critical infrastructures in each country are limited and experience has shown that the number of significant and impactful threats is not high, scalability considerations are not addressed in the proposed solution.

These are some of the pros and cons of using our model for calculating the national cyber situation at the national level. In the next section, we will provide some scenarios to illustrate how our model works in practice.

V. Experiments and Results

This chapter presents the experiments and results of the study. The purpose of the study was to evaluate the proposed model for calculating Cyber SA at the national level, based on the concept of macro missions and the cybersecurity scores of ISACs. The study also introduced the ISAS, a central authority that receives, analyzes, and disseminates Cyber SA information from various critical infrastructures, and coordinates and executes the best course of action to deal with cyber crises and their impact on national security and resilience.

Iran has faced numerous cyberattacks on its critical infrastructures in recent years. These attacks have been attributed to various state and non-state actors, posing serious threats to Iran's national security and economy. As a result, Iran has been under increasing pressure to enhance its cyber situational awareness at the national level. In this section, we will summarize some of these attacks and evaluate our proposed model for calculating the cyber SA at the national level. MITRE's ATT&CK framework provides a comprehensive view of the tactics and techniques employed in these cyberattacks, aiding in the understanding and mitigation of such threats [31]. In this section, we will summarize 9 cyberattacks that Iran has faced on its critical infrastructures in recent years. We will also evaluate our proposed model for calculating the cyber situation at the national level in each scenario.

Table 1 provides a detailed introduction to the cyberattack scenarios, listing the threat number, type of attack, and the infrastructure affected. Table 2 provides a comprehensive overview of each threat scenario, detailing the date, condition, threat risk score, threat risk score per missions, SAISac, and final situational awareness number.

For instance, consider the cyberattack on the National Iranian Gas Company (NIGC) (Threat 1, Row 1 in Table 2). This attack disrupted the gas distribution network, causing widespread outages at gas stations across Iran. The initial situational awareness score for this attack was calculated at the identification stage (ID) with a threat risk score of 30 and threat risk score per missions distribution as follows: M18 = 20, M17 = 7, and M16 = 3. The situational awareness score (SAISac) at this stage was 30, leading to a final situational awareness number of 16.94.

During the response phase, the threat risk score for the gas company attack was adjusted to 25, with recalibrated mission scores of M18 = 17, M17 = 6, and M16 = 2. This resulted in a situational awareness score (SAISac) of 25, leading to a final awareness score of 14.12. Simultaneously, a cyberattack on the Iran Railway Company was identified with an initial threat risk score of 15 and a situational awareness score of 15, resulting in a final score of 17.58. As recovery progressed for the gas company attack, the threat risk score decreased to 2, with mission scores adjusted to M18 = 1, M17 = 0.5, and M16 = 0.5, giving a SAISac of 2 and a final awareness score of 5.45. Meanwhile, the railway attack entered the response phase with a threat risk score of 13 and a SAISac of 13, resulting in a final awareness score of 5.02.

By the end of the incident, all scores will return to zero, indicating the resolution of the crises. The detailed tracking and adjustment of scores through each phase illustrate how the framework effectively quantifies the impact and response to cyber threats, providing a clear picture of situational dynamics and aiding in decision-making.

TABLE II. Quantitative Information of Threats

Threat Num.	Type of Attack	Infrastructure
1	Cyberattack on National Gas Company	Energy
2	Cyberattack on Iran Railway Company	Transportation
3	Cyberattack on Intelligent Fuel System	Energy
4	Cyberattack on Television	ICT
5	Cyberattack on Ports Organization	Transportation
6	Cyberattack on Ministry of Transportation	Transportation
7	Cyberattack on Mahan Airlines	Transportation
8	Cyberattack on Nuclear Facilities	Energy
9	Cyberattack on Telewebion	ICT

From Table 2, we can see that our model can capture the changes in the cyber situation at the national level as different attacks occur, progress, or end in different phases. It reflects the relative importance of different components and ISACs in determining the situational awareness score. For example, the attack on the

intelligent fuel distribution system has a higher impact on the situational awareness score than the attack on the radio and television because Energy-Oil-Oil Products-Distribution or Energy-Gas-Distribution has a higher weight than ICT-Communications. Furthermore, it is essential to consider the wide-ranging implications of our method for enhancing cyber defense strategies and informing policymaking endeavors. Our approach serves as a strong tool that empowers nations to strategically allocate their resources and efforts in safeguarding critical infrastructures against cyber threats. By systematically identifying the most vulnerable or invaluable components and ISACs, it enables countries to prioritize their cybersecurity initiatives effectively. Moreover, our model equips nations with the capability to maintain real-time vigilance over their national cyber landscapes. This is achieved by offering a quantifiable and easily understandable metric that can be readily communicated and comprehended by diverse stakeholders. This real-time assessment capability is pivotal for swiftly responding to emerging threats and ensuring the continual resilience of critical infrastructure. As shown in Figure 3, the situational awareness scores varied significantly across different stages of the cyberattack, highlighting the effectiveness of our model in tracking these changes. In addition, our platform provides real-time cyber threat analysis, as illustrated in Figure 4, showcasing various charts and metrics that help in monitoring and responding to threats promptly.

In summation, our framework represents a significant advancement in the realm of national-level cyber situational awareness. Anchored in current threats and ISAC situational awareness scores, it has been rigorously tested across various cyberattack scenarios targeting critical infrastructures. Our comprehensive evaluation highlights its effectiveness and utility in enhancing cyber situational awareness. Additionally, we have pinpointed potential areas for further refinement and future research to advance both our system and its broader applications.

TABLE III. SITUATIONAL AWARENESS SCORES OF DIFFERENT SCENARIOS OF CYBERATTACKS ON IRAN'S CRITICAL INFRASTRUCTURES

			Inputs			Output
Threat Number	**date**	**Condition**	**Threat Risk Score**	**threat risk score per mission**	**SAISac**	**Final Situational Awareness Number**
1	xxx-xx-xx	ID	30	M18 = 20, M17 = 7, M16 = 3	30	16.94
1, 2	xxx-xx-xx	Respond, ID	25, 15	M18 = 17, M17 = 6, M16 = 2, M2 = 15	25, 15	14.12, 17.58
1, 2	xxx-xx-xx	Recover, Respond	2, 13	M18 = 1, M17 = 0.5, M16 = 0.5, M2 = 13	2, 13	5.45, 5.02
1, 2, 3, 4	xxx-xx-xx	End, Recover, ID, ID	0, 2, 40, 30	M1 = 0, M2 = 2, M10 = 20, M18 = 20, M2 = 30	0, 2, 40, 30	3, 0.46, 22.95, 41.65
2, 3, 4	xxx-xx-xx	Recover, ID, Respond	2, 40, 37	M2 = 2, M10 = 20, M18 = 20, M2 = 37	2, 40, 37	No change, No change, 40.29
2, 3, 4	xxx-xx-xx	Recover, Respond, Respond	2, 36, 37	M2 = 2, M10 = 18, M18 = 18, M2 = 37	2, 36, 37	No change, 38.4, No change
2, 3, 4	xxx-xx-xx	End, Recover, Recover	0, 2, 2	M2 = 0, M10 = 1, M18 = 1, M2 = 2	0, 2, 2	37.58, 18.47, 2.06
3, 4	xxx-xx-xx	End, End	0, 0	M10 = 0, M18 = 0, M2 = 0	0, 0	0.94, 0
4	xxx-xx-xx	ID	30	M2 = 30	30	14.6
4, 5, 6, 7	xxx-xx-xx	ID, ID, ID, ID	30, 8, 5, 3	M2 = 30, M2 = 8, M2 = 5, M2 = 3	30, 8, 5, 3	No change, 15.91, 17.06, 17.75
4, 5, 6, 7	xxx-xx-xx	Respond, ID, ID, ID	28, 8, 5, 3	M2 = 28, M2 = 8, M2 = 5, M2 = 3	28, 8, 5, 3	16.81, No change, No change, No change
4, 5, 6, 7	xxx-xx-xx	Respond, Respond, Respond, ID	28, 6, 4, 3	M2 = 28, M2 = 6, M2 = 4, M2 = 3	28, 6, 4, 3	No change, 16.35, 16.12, No change
4, 5, 6, 7	xxx-xx-xx	Recover, Recover, Recover, Respond	1, 2, 2, 2	M2 = 1, M2 = 2, M2 = 2, M2 = 2	1, 2, 2, 2	3.47, 2.54, 2.08, 1.85
4, 5, 6, 7	xxx-xx-xx	End, End, End, Recover	0, 0, 0, 1	M2 = 0, M2 = 0, M2 = 0, M2 = 2	0, 0, 0, 1	1.38, 0.92, 0.46, 0.23
7, 8, 9	xxx-xx-xx	End, ID, ID	0, 5, 30	M2 = 0, M22 = 3, M1 = 1, M3 = 0.5, M2 = 0.5, M2 = 30	0, 5, 30	0, 6.51, 20.57
8, 9	xxx-xx-xx	Respond, Respond	4, 28	M22 = 2, M1 = 1, M3 = 0.5, M2 = 0.5, M2 = 28	4, 28	20.02, 19.09

8, 9	xxx-xx-xx	Recover, Recover	1, 1	M22 = 1, M1 = 0, M3 = 0, M2 = 0, M2 = 1	1, 1	13.67, 1.02
8, 9	xxx-xx-xx	End, End	0, 0	M22 = 0, M1 = 0, M3 = 0, M2 = 0, M2 = 0	0, 0	0.47, 0

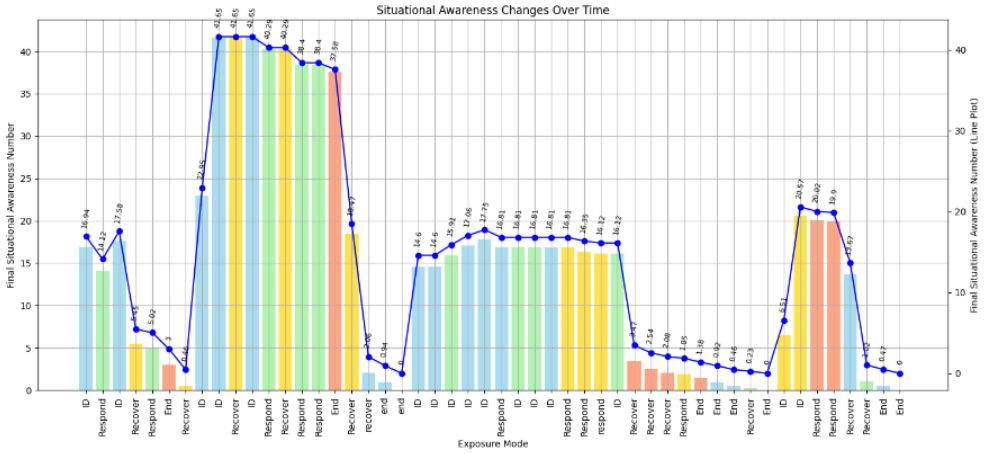

Fig. 3. Changes in Situational Awareness Scores Across Different Stages of Cyberattacks

Fig. 4. Platform Dashboard Showing Real-Time Cyber Threat Analysis

VI. Challenges and Limitations in Establishing National Cyber SA

This paper presents a framework for establishing national cyber situational awareness. Within this framework, in addition to an abstract overview of key nodes, the ISAS node is specifically examined, focusing on its collaboration with ISACs. However, creating an accurate and up-to-date national cyber situational awareness picture that can be effectively utilized for managing cybersecurity crises requires collaboration between hundreds, if not thousands, of government and private entities—posing numerous

challenges. This paper addresses a small portion of these challenges by providing a framework and model for visualizing cyber threat data and calculating situational awareness at the ISAS level. Below are some of the key challenges:

1. Integration of Multiple Data Sources: Comprehensive situational awareness necessitates the integration of data from a wide range of national and international sources, including government agencies, private sectors, and critical infrastructure. This process is often technically complex and time-consuming.

2. Timeliness and Accuracy of Information: For situational awareness to be effective, information must be both timely and accurate. Delays or inaccuracies in shared information via ISAS can lead to an incomplete or misleading national cyber posture.

3. Cross-Agency Coordination: National-level situational awareness requires close coordination between various entities, including law enforcement, intelligence agencies, and private sector organizations. Differences in objectives, operational processes, and technical capabilities can hinder effective collaboration.

4. Trust and Information Sharing: Building trust among ISAS participants is essential. Without sufficient trust, organizations may hesitate to share complete or sensitive threat information, which can undermine overall situational awareness.

5. Standardization of Data Formats: The absence of standardized formats for sharing threat data can complicate efforts to consolidate and analyze information from different entities. Ensuring interoperability between diverse systems remains a persistent challenge.

6. Evolving Threat Landscape: Cyber threats continuously evolve, and adversaries often employ sophisticated or novel techniques that may not be immediately recognized by ISAS. This limits the system's ability to provide a fully up-to-date and accurate picture of national cyber situational awareness.

7. Resource Constraints: Developing and maintaining national cyber situational awareness using ISAS requires significant resources, including skilled personnel, advanced technological infrastructure, and continuous updates. Resource limitations can diminish the system's effectiveness.

8. Legal and Policy Issues: Legal and policy barriers often complicate the sharing of threat information across entities or national borders. Balancing compliance with both national and international regulations while maintaining real-time situational awareness is a complex challenge.

9. Visualization of Complex Data: Translating vast amounts of threat intelligence into actionable insights for decision-makers is difficult. Effective visualization tools and dashboards are essential, but developing these for a national-level audience with varying levels of technical expertise presents a significant challenge.

VII. Conclusion

This paper introduces a robust framework designed to enhance Cyber SA at the national level, addressing the escalating threats to critical infrastructures. At its core, the framework uses ISACs across various sectors to improve threat detection, information sharing, and coordinated incident responses. The establishment of the ISAS as a centralized hub is pivotal; it processes and disseminates Cyber SA information, orchestrating a synchronized response to threats and thereby enhancing the resilience and security of national infrastructures. This framework not only integrates sector-specific insights to foster inter-sectoral collaboration and a unified defense posture but also introduces a novel approach to quantifying interdependencies within and across infrastructures, focusing on mission consistency. This strategic emphasis aids in understanding and mitigating the cascading effects of cyber incidents. Validated by practical applications and simulations, the framework demonstrates adaptability to evolving threats and the potential to integrate cutting-edge technologies. These features suggest its viability for long-term application. Ultimately, this framework provides a comprehensive strategy for advancing national Cyber SA, underscoring the necessity for advanced analytics and collaborative efforts in cybersecurity. Future research should explore how predictive analytics and machine learning could further refine and enhance cyber defense strategies. The adoption of this framework is poised to significantly elevate global cybersecurity practices, boosting proactive defenses against cyber threats.

References

[1] A. Kott, W. Cliff, and R. F. Erbacher. "*Cyber defense and situational awareness*", Vol. 62. Springer, 2015.

[2] A. J. Rashidi, k.d. Ahmadi, B. Nazarpoor, "*Cyber situational awareness*", Vol 1, Malek Ashtar University of Technology (MUT), 2018.

[3] C. Onwubiko, "CyberOps: Situational Awareness in Cybersecurity Operations," *arXiv preprint arXiv:2202.03687*, 2022.

[4] IRNA. "The fire in the cooling tower of one of the Isfahan power plant units was contained." https://www.irna.ir/news/85106588/ (accessed.

[5] IRNA, "Gas shortage in the second country with gas reserves; reasons and origins," 2022. [Online]. Available: https://www.irna.ir/news/85009527/.

[6] P. Kotzanikolaou, M. Theoharidou, and D. Gritzalis, "Cascading effects of common-cause failures in critical infrastructures," in *Critical Infrastructure Protection VII: 7th IFIP WG 11.10 International Conference, ICCIP 2013, Washington, DC, USA, March 18-20, 2013, Revised Selected Papers 7*, 2013: Springer, pp. 171-182.

[7] M. Gibson *et al.*, "Case study of the cascading effects on critical infrastructure in Torbay coastal/pluvial flooding with climate change and 3D visualisation," *Journal of Hydroinformatics*, vol. 22, no. 1, pp. 77-92, 2020.

[8] M. Yaniv, D. Zadok. "*Co-Analysis of Connectivity, Location, and Situation in Mission-Critical Hybrid Communication Networks.*" IEEE International Conference on Systems, Man, and Cybernetics (SMC). IEEE, 2020.

[9] M. Javornık, J. Komarkova, L. Sadlek, M. Husak "*Decision support for mission-centric network security management*", NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2020.

[10] F. R. L. Silva, P. Jacob. "*Mission-centric risk assessment to improve cyber situational awareness,*" Proceedings of the 13th International Conference on Availability, Reliability and Security. 2018.

[11] M. R. Endsley, "Situation awareness," in *The Oxford handbook of cognitive engineering.*, (Oxford library of psychology. New York, NY, US: Oxford University Press, 2013, pp. 88-108.

[12] A. Horneman. "Situational awareness for cybersecurity: An introduction, SEI Insight." https://insights.sei.cmu.edu/blog/situational-awareness-for-cybersecurity-an-introduction/ (accessed Jan. 15, 2024.

[13] C. Florackis, Ch. Louca, R. Michaely, M. Weber "Cybersecurity risk" The Review of Financial Studies, vol. 36, no. 1, pp: 351-407, 2023.

[14] F. Imanimehr, H. Gharaee, and A. Enayati, "An Architecture for National Information Sharing and Alerting System," in *2020 10th International Symposium onTelecommunications (IST)*, 2020: IEEE, pp. 217-221.

[15] A. Abdulmajeed, B. Duncan. "*Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence*", 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA). IEEE, 2020.

[16] N. Neshenko, E. Bou-Harb, and B. Furht, "Cyber Situational Awareness Frontiers," in *Smart Cities: Cyber Situational Awareness to Support Decision Making*: Springer, 2022, pp. 43-75.

[17] L. Matta and M. Husák, "A dashboard for cyber situational awareness and decision support in network security management," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2021: IEEE, pp. 716-717.

[18] M. Eckhart, A. Ekelhart, and E. Weippl, "Enhancing cyber situational awareness for cyber-physical systems through digital twins," in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2019: IEEE, pp. 1222-1225.

[19] C. Onwubiko *et al., Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20–21 June; Wales*. Springer Nature, 2023.

[20] H. Li, F. Wei, and H. Hu, "Enabling dynamic network access control with anomaly-based IDS and SDN," in *Proceedings of the ACM international workshop on security in software defined networks & network function virtualization*, 2019, pp. 13-16.

[21] Y. Nikoloudakis *et al.*, "Towards a machine learning based situational awareness framework for cybersecurity: an SDN implementation," *Sensors*, vol. 21, no. 14, p. 4939, 2021.

[22] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human factors*, vol. 37, no. 1, pp. 32-64, 1995.

[23] M. Vidulich, C. Dominguez, E. Vogel, and G. McMillan, "Situation awareness: Papers and annotated bibliography," *DTIC Document*, 1994.

[24] A. Munir, A. Aved, and E. Blasch, "Situational Awareness: Techniques, Challenges, and Prospects," *AI*, vol. 3, no. 1, pp. 55-77, 2022. [Online]. Available: https://www.mdpi.com/2673-2688/3/1/5.

[25] M. Dehghan, A. Mahdizadeh, B. Sadeghian: "A Model to Measure Effectiveness in Cyber Security Situational Awareness," Computer and Knowledge Engineering, vol. 7, No. 1, pp. 17-26, 2024.

[26] K. Renaud and J. Ophoff, "A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs," *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 1, no. 1, pp. 24-46, 2021.

[27] K. L. G. Snider, R. Shandler, S. Zandani, and D. Canetti, "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies," *Journal of Cybersecurity*, vol. 7, no. 1, 2021, doi: 10.1093/cybsec/tyab019.

[28] L. Zhang, A. Taal, R. Cushing, C. de Laat, and P. Grosso, "A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces," *International Journal of Information Security*, vol. 21, no. 3, pp. 509-525, 2022/06/01 2022, doi: 10.1007/s10207-021-00566-3.

[29] F. Cremer *et al.*, "Cyber risk and cybersecurity: a systematic review of data availability," *The Geneva Papers on Risk and Insurance - Issues and Practice*, vol. 47, no. 3, pp. 698-736, 2022/07/01 2022, doi: 10.1057/s41288-022-00266-6.

[30] A. S. Rafiee, H. Gharaee, F. Saghafi, M. Malekinia, "*The relevance, importance and dependence of critical infrastructures of the Islamic Republic of Iran from a cyber perspective*" , Journal of Information and Communication Technology, 2023.

[31] MITRE. "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)." MITRE. https://attack.mitre.org/ (accessed.

Fatemeh Imanimehr received her B.Sc. in 2001 and her M.Sc. in 2004 from Sharif University of Technology. She earned her Ph.D. in Computer Engineering (Software Engineering) from Amirkabir University of Technology (Tehran Polytechnic) in 2018. Since then, she has been a Research Assistant Professor at the ICT Research Institute (ITRC). Her research interests include Computer Security, with a particular emphasis on Information Flow Analysis, Information Sharing and Situational Awareness, Intrusion Detection Systems, and AI in Cybersecurity.

Alireza Enayati received M.Sc. degree in electrical engineering from Tarbiat Modares University in 2004. Since 2004, he has been with the ICT Research Institute. His research interests include Wireless Networks and Network Security.

Hossein Gharaee received his B.Sc. degree in Electrical Engineering from Khajeh Nasir Toosi University of Technology (KNTU), in 1998, and M.Sc. and Ph.D. degrees in Electrical Engineering from Tarbiat Modares University, Tehran, Iran, in 2000 and 2009 respectively. Since 2009, he has been with the Department of Network Technology in Iran Telecommunication Research Center (ITRC). His research interests include general area of VLSI with emphasis on Basic Logic Circuits for Low-Voltage Low-Power Applications, DSP Algorithm, Crypto Chip, Intrusion Detection and Prevention Systems.