Journal of Political Science
(A Peer-Reviewed, Open Access Journal; JPPS Star Ranked and Indexed in NepJOL)
ISSN 2362-1273 (Print); ISSN 2773-8132 (Online)
Volume 26, February 2026
https://www.nepjol.info/index.php/JPS
Published by
Department of Political Science, Prithvi Narayan Campus, TU, Pokhara, Nepal
Email: polsc@pncampus.edu.np

Electronic Warfare and Cybersecurity and Its Threats in Arab National Security

Mohammad Salim Al-Rawashdeh, PhD
Department of Basic Sciences and Humanities/ Princess Alia University College,
Al-Balqa Applied University, Jordan

Prof. Aktham Abed Elmajeed AL-Sarayreh
Department of Financial and Administrative Sciences
Amman University College for Financial and Administrative Sciences
AL-Balqa Applied University, Jordan

Yousef Salameh Almseidin
Department of Basic Sciences/ AL-Balqa Applied University
Amman University College for Financial & Managerial, Jordan

Corresponding Author*: Mohammad Salim Al-Rawashdeh, Email:* jordanresearch@bau.edu.jo.

DOI: https://doi.org/10.3126/jps.v26.i1.90783

Submitted 8 July. 2025; Reviewed 22 July. 2025; Accepted 22 Dec. 2025; Published 15 Feb. 2026

Abstract

The implications of electronic warfare on the security of Arab states were explored in this work, and the range of geological information operations was discussed, as well as the implications of cybersecurity threats on different fields of society and its crucial infrastructures in the Middle East. It is predicted to answer the correlations between the level of cyber threats and cybersecurity and information security knowledge rates, and their impacts on national security performance.The research employed a cross-sectional quantitative research design, and a convenience sample of 567 participants in the Arab states were self-administered questionnaires. The questionnaires that were self-administered provided quantitative information about the identified variables, such as the frequency of cyber threats, cybersecurity awareness, its impact on national security, and public trust.

Structural Equation Modelling (SEM) was employed to analyze the effect of the independent and mediating variables. The cyber threats are observed to harm national security (-0.50) and public trust (-0.83). Some of the moderating effects were accounted for by cybersecurity awareness and literacy (.26) and had a positive influence on national security (.26) and public trust (.21). However, the global correlation profile is negative, indicating that despite all these advantages, cybersecurity threat is still a significant issue. Cyber threats are a significant issue as a threat, and this has been demonstrated in this study: simultaneously, their role in enhancing cybersecurity. Nonetheless, in dealing with them, there is a binding obligation to pursue education and awareness, among other interventions, use of creativity and innovation, particularly through technology, establishment of regional cooperation and collaborations and good governance systems.

Keywords: *Arab national security, credibility, e-security, germ warfare, threats*

Introduction

On a more dynamic concept, national security in an ever-linked globalized world (Smith 2020) is susceptible to areas that are full of tensions (Jones 2019). The digital change management process has enhanced the potential threat of cybersecurity to analysts and policymakers (Mohee, 2023). Iftikhar (224) discussed in this paper the experience of Arab countries in the practice of electronic warfare and their national security (Iftikhar, 2024).

Cyber threats, as well as the risks associated with them (Khan, 2022), and risks of classical warfare (Adams, 2020), in addition. Electronic warfare transforms the adversary with the electromagnetic spectrum that affects the state sovereignty and stability (Electronic warfare) (Al-Kasassbeh, Ghazleh, and Ma’moon Juma'h, 2023). These cybersecurity threats in the Arab states need to be understood due to the history and the geopolitics of such states. The paper will examine the relationship between EW strategy and national security and explain the preventive actions that should be undertaken to maintain the stability of a region according to the existing trends in electronic attack (El-Sayed, 2023), like hacking (Hassib and Ayad, 2023) (East, Economics, and Past, 2023).

The study further enhances the digital age security debate (Patel, 2020), particularly with regard to the requirement of Arab countries to have proper cybersecurity structures (Hassan, 2022). New cyber threats are particularly dangerous as the connectedness of systems has increased susceptibility to cyber threats, and their effect on national security is enormous (Sofge, 2021; Al-Tawaiti and Hassan, 2020). The energy, information, and social-security industries of the Middle Eastern states are at risk due to the cyber threats that, in turn, affect the economic, political, and social spheres of the states (Jimada-Ojuolape et al., 2024; Wan et al., 2021). However, in most cases, individuals in the population are likely to experience poor perceived risk in spite of the observed discrepancy between perceived risks and risk-reduction practices in the user group. Thus, the holistic and combined vision of cybersecurity ought to include the hardware and software needs of computer networks and human actions (Lee, Mujammami, and Kim, 2024).

The issue of cybersecurity also applies to threats in electronic warfare, where the security of Arab nations is a critical concern. It is important to present the salient issues of security, such as security based on artificial intelligence, threat intelligence frameworks, and knowledge raising about security. Particularly in the Middle East, both the political instability and the situational critical infrastructure dependency do not mention the recent accelerated technological development that suggests certain cyber risks. Recent studies generally presuppose the ability to generalize findings in other regions of the world to the present state of cybersecurity.

These areas are the most sensitive ones since the region depends on energy, water systems, and transportation, as these are the most critical infrastructures. However, it has not been sufficiently addressed in the interaction with these vulnerabilities, in particular, the element of electronic warfare. As an illustration, in a study by Wan et al. (2021) about global cases, other challenges that may be faced by specific sectors, like the oil and gas sectors in Arab countries, were not considered; hence, introducing a partial estimation of the consequences on national security.

The reviewed literature revealed that the role of human factor in cybersecurity in the Middle Eastern region has been under-explored, especially because the cultural and educational influence of the Arab nations receives little research, even though they increase the number of cyber threats due to the high rate of ignorance and impunity (Kostyuk and Wayne, 2020). Not many studies are oriented to the Arab nations regarding the implementation and deployability of the advanced cybersecurity solutions and strategies, such as the literature of Jada and Mayayise (2023), which is rather theoretical and contains few practical details. The existing literature has not given enough focus to the cybersecurity policies in Arab nations and their compatibility with the international standards, and there is no adequate policy governance in dealing with the issue without any legislative and collaboration issues within the Arab region which have been concealed (Saeed et al., 2023).

Limited is deployed to explore regional collaboration and information exchange between the Arab nations to counter cyber threats as most of the studies are tinted with the globalization facets without a clear understanding of the regional response to counter the international cyber threat (Jimada-Ojuolape et al., 2024). In addition, the limited literature that dictates clear economic implications of deliberate cyberattacks on situations in the Middle East and the study of potential mitigation strategies are minimal; publications such as Cheng and Wang (2022) do not significantly define the economic risks and weaknesses of countries of the Middle East that have ceased here (Al-Masaeed, Yaseen, Al-Adwan, Altarawneh, and Alhjouj, 2023).

Considering the nations of the Middle East as assets with sufficient wealth and geopolitical position, the practice of electronic warfare and cybersecurity among them determines the national security (Al-Omoush et al., 2020). Consequently, the military strategies have been reduced to electronics and cyber, and countries employ the cyber modality to disable the systems of their enemies (Khan et al., 2021). That shift underlines how data and information authenticity, security, and accessibility play an important role in virtual combat zones (Mansour, 2022). Both state and non-state actors make cybersecurity threats more hazardous because they can now access cyber capabilities. The issues being experienced by the Middle East countries can be exemplified by the instances of cyber espionage and data breach, critical infrastructure attack, and destabilization of national security (Zarif et al., 2021). Cybersecurity issues were caused by the unpredictability of the political situation in some geographical regions and the use of cyberspace by militias (Al-Shehri, 2022).

The majority of the key sectors, such as energy, finance, and telecommunications, are interrelated, thus resulting in the amplification of risks. The economic aberration, lack of public confidence, and loss of life in such sectors will result from such cyber-attacks, where the cyber attackers will have gotten the spoils (Hassan and Al-Khaldi, 2023). This has raised the issue of the necessity to invest in effective cybersecurity. The current paper examines the connection between Electronic Warfare and Cyber Security threats in Arab national security to further explain the threats of the region and provide references to improve cybersecurity against the new threats. Policymakers, military, security analysts, and other interested parties should value such characteristics, especially in preventing sovereignty threats in the info age (El-Sayed, Mahmoud, 2023).

Problem Statement

In the contemporary Middle Eastern state, there has been a growing trend of electronic warfare and threats to cyberspace as significant security threats. There is a belief that the degree of the area risk exposure to cyber threats is increasing because both state and non-state actors are adopting advanced strategies to disrupt critical information systems. The spread of cyber tools has grown the shares of cyber spying, hacking, and cyber-war, developing massive infrastructural effects with catastrophic effects on national stability in case of a black swan event (Zarif et al., 2021). The failure of critical infrastructure sectors is that they make more risks dependent, and a cyberattack may lead to further failures (Hassan and Al-Khaldi, 2023). It is even more so in the face of the continuously shifting political environment, which is the issue of cybersecurity (Al-Shehri, 2022). Moreover, the technological development is evolving at an extremely rapid pace, and the character of the wars also requires knowledge of the connection between electronic warfare and cybersecurity. Nowadays, the conflict has moved to the new spheres of data battle, which demand, among others, data integrity, confidentiality, and availability (Eslami and Vieira, 2023a).

This still emphasises the present requirement of greater security for the digital property and data of a nation. New security threats in the GCC region, which has witnessed electronic warfare specifically in the Middle East, undermine the national security of Arab countries, thus necessitating a study of the condition and infrastructures to counter the new age threats. This study seeks to explain these vulnerabilities and give suggestions on how the threat of cyber warfare in the region can be contained (Rawindaran et al., 2023).

Research Questions

The following are the research questions of the study:

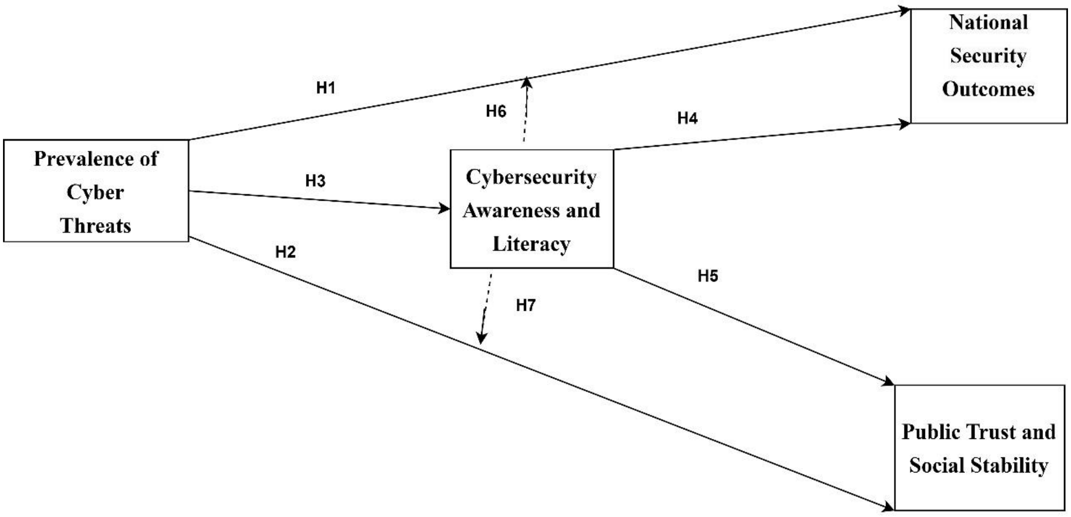
1. How does the prevalence of cyber threats affect the performance of national security?
2. What degree and what is the impact of the occurrences of the cyber threats on the degree of public trust and the degree of social stability?
3. Differently stated, how does the degree of threat presently out there in cyberspace compare with the degree of cybersecurity awareness and knowledge across the general population?
4. What is the extent to which cybersecurity awareness or lack affect national security?
5. Appreciating how cybersecurity awareness and literacy affect social stability and trust of the populace of a nation.
6. What is the moderating effect of cybersecurity awareness and cybersecurity literacy in the relationship between the level of cyber threats and the effects on national security?
7. How much cybersecurity awareness and literacy intervention would account for the relationship between the occurrence of value threats, public trust, and the stability of society?

Research Objectives

1. To observe the widespread diffusion of cyber threats and the immediate correlation with the indicators of national security.
2. To investigate how the various threats that might occur in cyberspace affect the stability and trust of people in society.
3. To examine how the rate of cyber threats can also differ depending on the level of cybersecurity awareness and literacy.
4. In the study of how cybersecurity awareness and literacy affect national security results, the authors had the following objectives.
5. This study has measured the influence of CS-C Awareness and CS C Literacy on PT-S Stability.
6. To test how cybersecurity awareness and cybersecurity literacy moderated the relationship between the prevalence of cyber threats and national security performance.
7. To determine the hypothesis that cybersecurity awareness and literacy is a moderator to the interplay between the degree of danger posed by cyber threats, public trust, and social stability.

Figure 1

Proposed Research Model


National Security Outcomes
H1
H6
H4
Prevalence of Cyber Threats
H3
Cybersecurity Awareness and Literacy
H2
H5
H7
Public Trust and Social Stability

Hypotheses

H1: The study established that the higher the degree of cyber threats, the more unfavorable in terms of national security in the given countries.

H2: They disclosed that even though the presence of cyber threats is rather high, it is destroying the confidence of the population and social peace.

H3: The other facet of the correlation between the described subtopics is that the rates of cyber threats highly depend on the rates of cybersecurity literacy.

H4: awareness and literacy play a pivotal role in improving cybersecurity and, hence, improving the security situation of a country.

H5: The level of trust in the state of cybersecurity knowledge and education affects the level of social cohesion of the population positively.

H6: Cybersecurity awareness or cybersecurity literacy dilutes the association between the occurrence of cyber threats and the effects on national security.

H7: Cybersecurity education and sensitization is a mediator between the occurrence of cyber-skewed threats and social stability and trust in society.

Methodology

Research Design

The survey research approach was employed in this paper to examine the relationship between the prevalence of cyber threats, cybersecurity awareness, and knowledge and their outcomes on security, trust, and stability. This study provides a critical discussion of the research questions using empirical data analysis as well as statistical data analysis (Ali and Ahmmad).

The design used in this research study was a cross-sectional design where data were only collected once to give a cross-sectional analysis of the present cyber threat and the variables of interest. Through this method, it is possible to determine the frequency of cyber threats, the degree of cybersecurity awareness, and its implications on the national security and social relations among the Arab states in the Middle East (AlBenJasim, Dargahi, Takruri, and Al-Zaidi, 2024).

The population of the Arab countries in the Middle East, that comprised of Saudi Arabia, the United Arab Emirates, Qatar, Bahrain, Oman, Kuwait, Jordan, Lebanon, and Egypt, formed the target population of this study. This study will have a total respondent population of 567 respondents who will be chosen in the mentioned countries. The sample size was considered adequate to give results that are significant and real to a great extent. The respondents will be suitably stratified in the countries using variables like the population size and Internet usage rate among the population in order to achieve a sample set of effective and efficient responses (Naz, Karim, Houcine, and Naeem, 2024).

Sampling Technique

In this study, a stratified random sampling technique was used to ensure representativeness of every Arab state. On the other hand, random sampling of each stratum will assist in decreasing bias during sampling and enhancing the external validity of the study, owing to country-based sampling, which will aid in classification based on region. This method enabled the study to receive a broad range of opinions and data that were relevant to the objectives of the study (Al-Musharafi).

Measurement and Data Collection System

The self-administered, structured survey questionnaires will be in electronic format in order to have a broad range of generated data and ensure complete credibility of the data. The interaction between the independent and dependent variables: the Prevalence of Cyber Threats, Cybersecurity Awareness and Literacy, National Security Outcomes, and Public Trust and Social Stability is theorized in line with the desired pathways (H1 to H7). The item of the 6-item measure based on the Williams et al. (2018) study will be used in the measure of the Prevalence of Cyber Threats as the dependent variable and will be relevant to the prevalence, nature, and severity of the threat. In between MA-SEC and IS-SEC, Cybersecurity Awareness and Literacy will have an 8-item questionnaire, borrowed from Parsons et al. (2017), to measure cyber threats and comprehensive protection. The National Security Outcomes will be considered through a 5-item scale on the perception of national equivalent stability, and Public Trust & Social Stability will be considered through a 7-item scale on admiration of institution and cohesiveness, respectively (Baldwin, 1997 and Fukuyama, 1995). All items that Taiwanese will accommodate will have 5-point Likert scales, which will fit the previous study. Structural Equation Modelling (SEM) direct and mediating effects will be established (Solar, 2023; Tzenios, 2023).

Data Analysis Tools

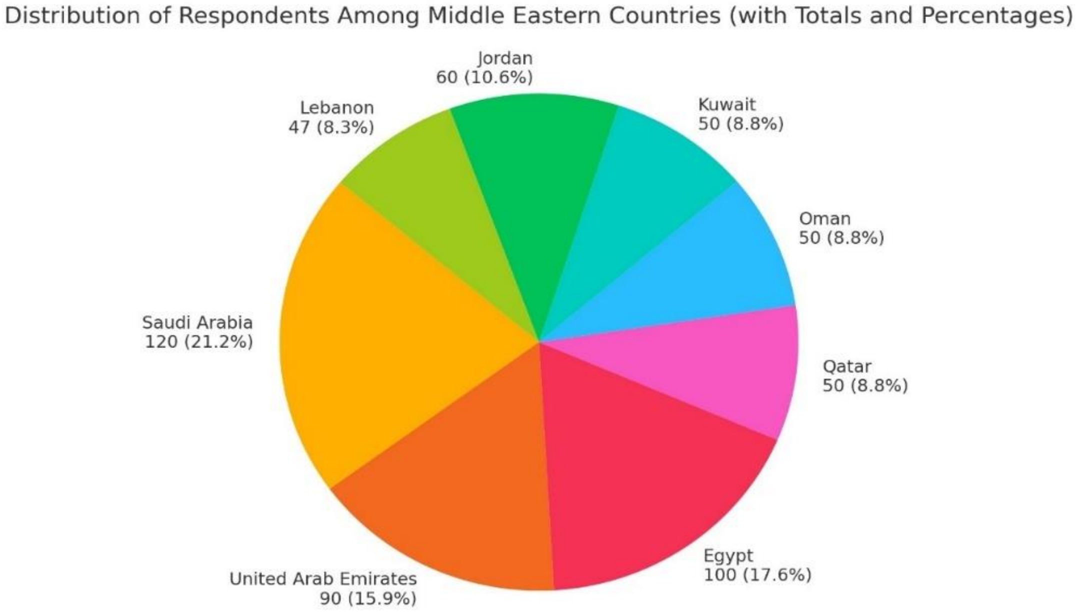
The data collected was analyzed through SPSS and Analysis of Moment Structures. software. These tools allowed the nominal and ordinal statistical analysis to take place. Evaluations such as descriptive analysis, multiple linear regression and Structural Equation Model will be embraced in testing the beliefs and demonstrating the relationship between the variables. SEM will also be useful in the moderation of cybersecurity awareness and literacy. In this research, Cronbach's alpha was also calculated on each group of items that were answered to verify the reliability of the measured constructs (Aslan, Aktuğ, Ozkan-Okay, Yilmaz, and Akin, 2023).

Data Distribution Among Arab States

The 567 respondents will then be distributed across the Arab states in proportion to make sure that more states are covered than others. Its rough distribution is divided as follows.

Figure 2

Respondents Demographic



Ethical Considerations

The letter will be conducted within the standard of ethics when carrying out the study. The objectives of the study will also be informed to the participants and the refusal to participate will be honored after refusing to participate. Certain measures will be undertaken to help to ensure the anonymity and confidentiality of the response and safeguard the identities of the respondents. In addition, the research will seek the approval of pertinent ethics institutions in case they should determine ethical requirements (Falowo, Ozer, Li, and Abdo, 2024).

Reliability and Validity

Considering Table 1 data, the internal consistency of the data and the construct validity of the variables are quite high. Construct reliability was also confirmed by the authors; all the values of CR were greater than the standard quantity of 0.7 that is accepted in the majority of academic studies. The convergent validity was also established through the composite reliability values that ranged between 0.70 and 0.87, and the AVE values of all the constructs were greater than 0.5. The AVE was stiffer than the MSV, hence indicating the discriminant validity of the constructs in question. Also, the inter-construct correlations indicated significant relationships: PTC and CAL had a strong relationship (r = 0.985; p < 0.001), whereas CAL was moderately associated with NSO (r = 0.356; p < 0.001) and PTSS (r = 0.436; p < 0.001). To be more precise, the NSO demonstrates a rather high positive correlation with the PTSS, 0.522, which confirms the stability of the measurement model as well. Based on these findings, it was possible to verify the reliability and validity of the used constructs in the analysis (Nuseir et al., 2024).

Table 1:

Reliability and Validity

	CR	AVE	MSV	MaxR(H)	PTC	CAL	NO	PTSS
PTC	0.83	0.748	0.97	0.83	0.669			
CAL	0.73	0.671	0.97	0.772	0.985***	0.521		
NO	0.806	0.755	0.126	0.81	0.334***	0.356***	0.674	
PTSS	0.719	0.673	0.19	0.732	0.404***	0.436***	0.164**	0.522

Model Fit

The overall chi-square test of the model fit indices presented in Table 2 is as follows: The chi-square value (CMIN = 319.051) with 203 degrees of freedom (DF) gives us a CMIN/DF of 1.572, which is below 3. Hence, acceptable, indicating that the fit is reasonable. Comparatively, the fit index for the current model, CFI = 0.958, is above the acceptability limit of 0.95, which shows an excellent incremental fit. Absolute fittest estimates were also excellent with a measure of SRMR = 0.045, which is less than the cut-off of 0.08, and the RMSEA = 0.032, which is below the cut-off of 0.06. Further, the PC loss value is 1, and it is greater than 0.05, which reinforces that RMSEA is not significantly different from zero. Overall, all these statistics proactively indicate that the suitability of the model to the forecast data is acceptable (Adhikari, 2024).

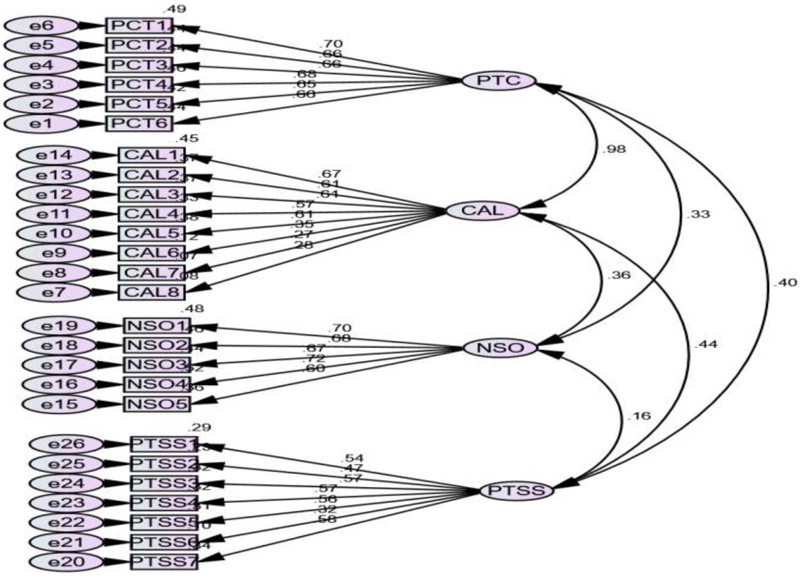
Table 2

Model Fit

Measure	Estimate	Threshold	Interpretation	Measure	Estimate
CMIN	319.051	--	--	CMIN	319.051
DF	203	--	--	DF	203
CMIN/DF	1.572	Between 1 and 3	Excellent	CMIN/DF	1.572
CFI	0.958	>0.95	Excellent	CFI	0.958
SUMMER	0.045	<0.08	Excellent	SUMMER	0.045
RMSEA	0.032	<0.06	Excellent	RMSEA	0.032
PClose	1	>0.05	Excellent	PClose	1

Figure 3

EFA Model



Factor Loading

The table will provide the loadings of four constructs: Self-perceived Cybersecurity Awareness and Literacy (S-CAL), the Consequence of National Security (C-NSO), the

Extent of Cyber Threats (C-PCT) and the Impact toward Public Trust and Social Stability (C-PTSS). The loadings show the magnitudes of the correlation between the items and the five scales that constitute the scales. In the case of CAL, internal consistency reliability of all (CAL1 to CAL5) was acceptable (0.57 to 0.668), and that of CAL6 to CAL8 was low, implying that they make little contribution to the CAL construct in this study. The range of NSO α coefficients was between 0.601 and 0.721, and this is very reliable when it comes to this construct. PCT is found to have a satisfactory degree of construct validity and substantial AVE of between 0.649 and 0.699, therefore suggesting a definite measurement model. Finally, the PTSS loadings were moderate to very low: 0.317 -0.581, with the PTSS6 having the smallest contribution to the construct. Overall, the low loadings might require certain adjustments, possibly by purging the item and even raising the crud factor in an attempt to improve the construct validity and reliability of the measurement model (Nobanee, Alodat, Bajodah, Al-Ali, and Al Darmaki, 2023).

Data Presentation

Hypotheses Testing:

H1: When testing H1, the path coefficient between independent variable cyber threats (PCT) and dependent variable national security outcomes (NSO) will be negative and significant (-0.50 mean value of the coefficient) and proved that an increase in PCT will reduce the NSO significantly. This confirms H1 and demonstrates that cyber threats hurt the national security of the country.

H2: Again, hypothesis ten is also supported, where the path coefficient between cyber threats (PCT) and public trust and social stability (PTSS) is negative (-0.83). This outcome greatly favors H2, which states that higher risks in cyberspace result in a reduction in the level of public trust and social stability.

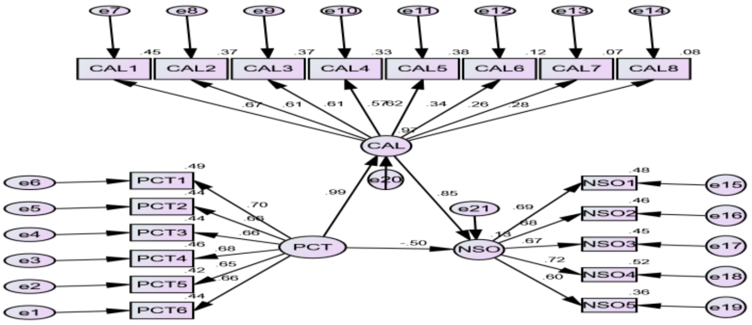
H3: The path coefficient between the first and cyber threats and PCT and CAL is positive and significant (0.97). It indicates that experience of cyber threats is positively correlated with cybersecurity knowledge. As such, the findings of the study supported **H3.** The path coefficient between the first and cyber threats and PCT and CAL is positive and significant (0.97). It indicates that experience of cyber threats is positively correlated with cybersecurity knowledge. As such, the findings of the study supported H3.

H4: The findings show that the path coefficient of cybersecurity awareness and literacy (CAL) and national security outcomes (NSO) is positive and significant (0.26). This demonstrates that higher levels of information concerning issues relating to cybersecurity enhance the performance of national security, hence supporting H4.

H5: The path coefficient of the relationship between the cybersecurity awareness and literacy (CAL) and the public trust and social stability (PTSS) is positive and significant, with a path coefficient of 0.21. H5 is proven by the fact that increased cybersecurity awareness and literacy increase trust as well as social cohesion among people.

Figure 4

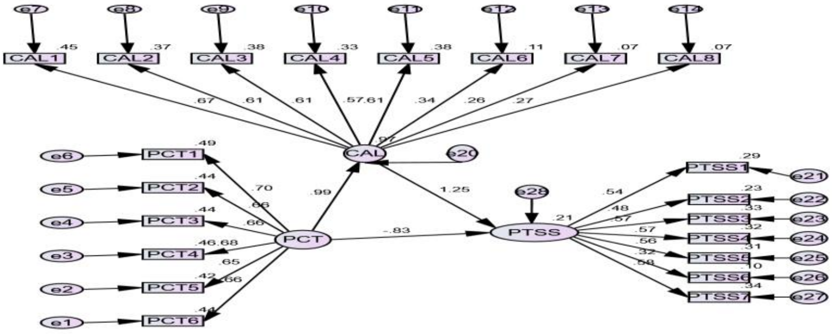
SEM of H6



H6: The effect of the PCT construct on NSO outcomes is found to be (-) 0.50, which is statistically significant and exhibits strong physical existence and negative associations. This demonstrates that the effects of national security are felt in the case of the existence of cyber threats. However, the indirect effect via cybersecurity awareness and literacy (CAL) is positive 0.252, which is estimated as 0.97 × 0.26. This shows that the adverse impacts of cyber threats are, to some extent, balanced out by CAL in NSO. The net effect is the negative value, which implies that though CAL helps to keep the relationship between PCT and NSO, the general trend in the line is downward. The fact that the indirect effect of CAL is also significant contributes to the fact that it also proves the partial mediation; that is, CAL helps to reduce but not eliminate the adverse effect of cyber threats on the national security outcomes (Petrosyan, 2024).

Figure 5

SEM of H7



H7: The effect of the PCT on PTSS implies that the PCT directly negatively affects PTSS with a value of - 0,83. This depicts the susceptibility and the degree of damage that cyber threats cause to the essential frameworks of society. The indirect impact via cybersecurity awareness and literacy (CAL) is 0.2037, which is a product of 0.97 X 0.21, with the path coefficient taking a positive value that is significant. This indicates that CAL can help in reducing some of the negative effects of cyber threats on the PTSS. The overall effect is negative, which further attests to the previous result that CAL has a positive effect, but PTSS is otherwise harmful to PCT. Similar to H6, it is partially supported by indicating that whereas CAL can have a bi-directional negative effect on cyber threats to increase the public trust and social stability, it fails to remove the harmful effects on them (Freilich, Cohen, and Siboni, 2023).

Table 3

Path Coefficient of Direct Relationship

Hypothesis	Path	Path Coefficient	Significance	Result
H1:	PCT → NSO	-0.5	Significant	Supported
H2:	PCT → PTSS	-0.83	Significant	Supported
H3:	PCT → CAL	0.97	Significant	Supported
H4:	CAL → NSO	0.26	Significant	Supported
H5:	CAL → PTSS	0.21	Significant	Supported

Figure 6

Path Coefficient of Direct Relationship

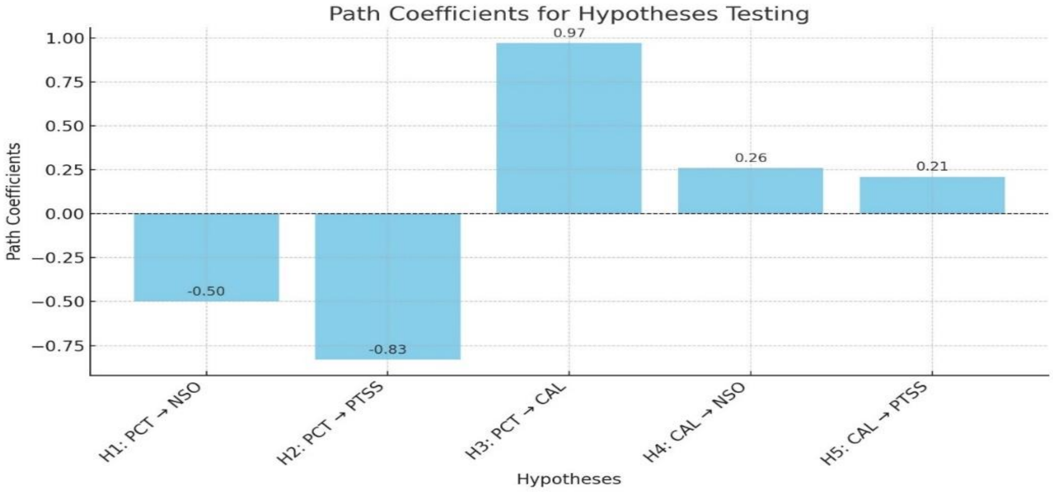


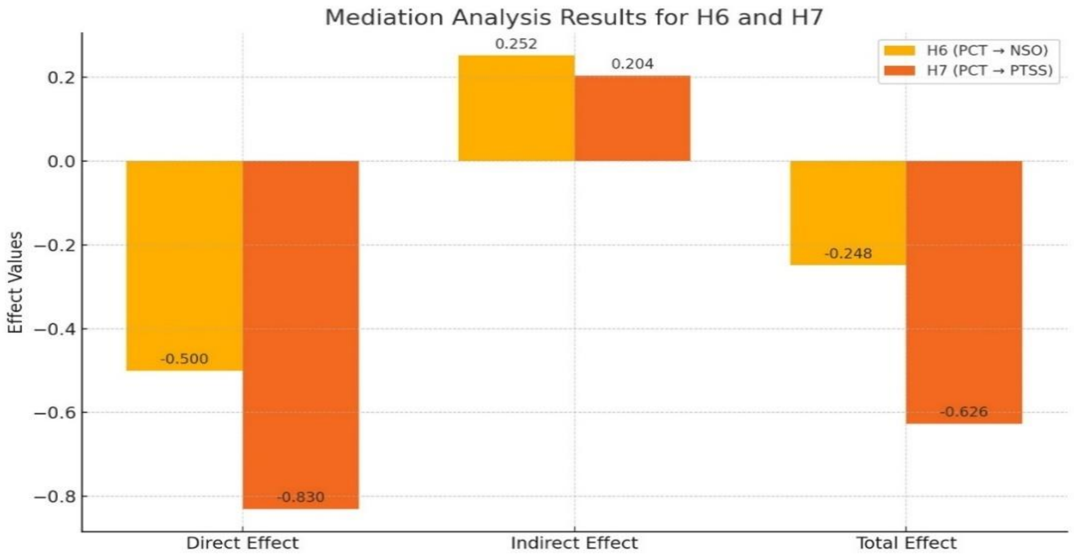
Table 4

Mediation Analysis Results

Hypothesis	Effect	Path	Value	Interpretation
H6:	Direct Effect	PCT → NSO	-0.5	Significant negative effect.
	Indirect Effect	PCT → CAL → NSO	0.97 × 0.26 = 0.252	Positive and significant indirect effect.
	Total Effect	PCT → (CAL) → NSO	TRUE	Significant negative overall relationship.
	Mediation Type		Partial	Direct and indirect effects are both significant.
H7:	Direct Effect	PCT → PTSS	-0.83	Significant negative effect.
	Indirect Effect	PCT → CAL → PTSS	0.97 × 0.21 = 0.2037	Positive and significant indirect effect.
	Total Effect	PCT → (CAL) → PTSS	TRUE	Significant negative overall relationship.
	Mediation Type		Partial	Direct and indirect effects are both significant.

Figure 7

Mediation Analysis



Discussion

The results of the path coefficients are conception rich to offer a multi-chain of cyber threats, national security, public trust, and cybersecurity education and knowledge chain. The findings support all the hypotheses put forward in this work and emphasize the complexity of cyber threats and literacy on cybersecurity (Sufi, 2023).

Cyber Threats' Influence on the Security Development Outcomes of Nations (H1)

The negative and significant effect of cyber threats (PCT) on the national security outcomes (NSO) is significant because the path coefficient is -0.50. The influence of cyber threats on the vital fabric of societies, such as critical infrastructure, by introducing their resilience, exposing them to sensitive government information, and becoming access points to seize non-critical infrastructure, is evidence of this finding. The article by Bada and Nurse (2020) expounds on the problem of the increasing complexity of cyber threats to state-level security structures, just as the article. The threats are not solvable unless there are effective cybersecurity guidelines and international collaboration to reduce the effects (KUMAR, 2023).

Effects of Cyber Threats on Social Acceptance and Civil Unity (H2)

A highly significant negative value of -0.83 between the independent variable PCT Cyber threats and the dependent variable PTSS Public trust and social stability was also indicated by the path coefficient analysis to reinforce the extent to which cyber incidents undermined the level of trust. Leaking of data daily, misinformation, and threats to the availability and integrity of services have generated higher levels of insecurity and losses in community cohesion. These findings were mapped by the Pew Research Centre (2022) against the extreme societal impact of cyber-attacks. This necessitates the implementation of policies that will make cyber threats responsible and instill more confidence in the population regarding the management of threats by the policies (Holstein and McLaughlin, 2023).

The Correlation Between Cyber Threats and Levels of Awareness and Literacy of the Cybersecurity Threat (Hypothesis 3).

Surprisingly, the path coefficient, which connects both cyber threats (PCT) and cybersecurity awareness and literacy (CAL), is positive and significant with a value is 0.97. But these are the negative threats, as they promote greater awareness and activism regarding cybersecurity among individuals and organisations. Therefore, the same was observed by McGuire and Dowling (2021), who also admitted that the greater risks the necessity of cybersecurity training and materials. This fact highlights the importance of taking advantage of heightened awareness since there is a possibility of establishing a cyber-resilient society (Montasari, 2023).

Cyber Readiness: Influence of Cybersecurity Awareness and Literacy on National Security Results (H4)

Essentially, the understanding and value of cybersecurity risk (CAL) is positively and significantly associated with national security gains (NSO), and the correlation coefficient is 0.26. Unlike the role of increasing awareness in reinforcing protection by equipping clients, both individual citizens and governmental institutions, with information and required tools against cyber threats, the absence of awareness prevents the creation of appropriate defence mechanisms. Von Solms and Van Niekerk (2013) emphasised the significance of the seeming National favorites and the policies that reinforce the need for the new National Cyber security education to enhance the National security (Van Puyvelde and Brantly, 2024).

Effect of Protective Awareness and Information Security Literacy on Community Confidence and Social Order (H5)

Lastly, the path coefficient of 0.21 that demonstrated CAL and PTSS to be positively and significantly correlated signals questions improvement of education as a means of creating resilience in society. The lack of awareness and literacy levels is substituted by the enhanced ability that allows the human person and communities to combat the cyber threats and restore the lost trust and balance. These findings follow the same trend as the argument of Renaud and Goucher (2018), who contend that more people need populistically oriented cybersecurity education to enhance their security and assurance (Eslami and Vieira, 2023b).

Analysis of the Study Outcomes in Terms of Moderation

The mediation analysis of the correlation between PCT and NSO and the one between PCT and PTSS gives useful data regarding the significance of CAL in reducing the adverse impact of cyber threats. Together, the findings support the assumption that, although CAL can, to some degree, reduce the pernicious effect of cyber threats, it cannot, nevertheless, get rid of it, which is revealed by a partial mediating effect (Hasan, 2023).

Counselling of Cyber Security Awareness and Literacy on the Link Between Cyber Threats and National Security Performance.

The findings also indicate that the direct correlation between the cyber threat (PCT) and national security outcomes (NSO) is negative and statistically significant (-0.50), which is again a support of the negative effect of cyber threat on national security. Nevertheless, the overall indirect impact of 0.252 and denoted as significant depicts the alleviating influence of cybersecurity education and awareness, which is offered under CAL. This means that though awareness cannot nullify the fact that there are new kinds of threats in the cyber world, it equips a person or an organization with skills to deal with these threats in a more convenient way. Similarly, Bada and Nurse (2020) authors also indicated the great role of education in making the nation more resilient to cybercrimes by creating awareness about cybersecurity and preventive steps instead of being susceptible to cyber offences (M.-S. Al Ashry, 2024).

Despite all these mitigations, the overall impact is still negative, which can only continue to accentuate the existing threats of cyber threats. It can be explained by the fact that Von Solms and Van Niekerk (2013) argue that awareness programs are helpful but that they must be supplemented by a systematic approach to protection against cyber-attacks (Miniaoui, Muammar, Muhammad, Al Muraqab, and Atalla, 2024).

C Mediation of Cybersecurity Awareness and Literacy on the Association Between Cyber Threats and Public Trust & Social Stability

In addition, the effect of cyber threats (PCT) on social stability (PTSS) and the effect of cyber threats (PCT) on the public trust are strongly negative and statistically significant (-0.83), which highlights the devastating harm that cyber threats cause to the cohesiveness of society and the trust of the citizens. The indirect impact of CAL, 0.2037, is notable and positive; nonetheless, to substantiate the argument that cybersecurity awareness and literacy contribute to overcoming the adverse effects of cyber threats, there is also some evidence that individuals and communities increase their knowledge and preparedness to cyber threats. Similarly, Renaud and Goucher (2018) assumed that the human-oriented approach to cybersecurity training makes society resilient, builds confidence in online spaces, and unravels the societal turmoil caused by cyber-attacks.

Nonetheless, the net effect is still adverse, and this implies that, as much as CAL is critical to organizations, it does not go all the way in neutralizing the hostile effects that cyber threats pose to the struggle. This coincides with McGuire and Dowling (2021), who stated the significance of Systemic and policy-level responses to help individual and organizational awareness initiatives (Douzet, Petiniaud, Salamatian, and Samaan, 2023).

Partial Mediation and Possibilities of Change

The partial mediation was set up in both NSO and PTSS results, which confirms that CAL is an important tool of coping with the effects of cyber threats, but is not eliminated. This also leads to the end of appreciation of cybersecurity awareness as a means of dealing with cyber risks, but heightens appreciation of cybersecurity weaknesses. It has been suggested by Von Solms and Van Niekerk (2013) that when a cybersecurity program has implemented some measures but lacks education, technological solutions, and powerful policies, then it is dealing with cyber threats using a single tool (Salim, Moustafa, and Reisslein, 2024).

Findings

All such results combined demonstrate that cyber threats are both a menace and a motivator towards augmented cybersecurity awareness. They emphasise the application of holistic strategies, which transcend the emphasis on the aftermath of the cyber threats, but employ them to improve the chances of coming up with sustainable and viable national and societal structures. Future studies can be based on this research to investigate the interaction of the various levels of literacy with the various types of threats to implement the correct intervention measures (Conduit, 2024).

Considering the results of the research, CAL can be regarded as a significant mediating variable that reduces the effects of cyber threats on NSAs, social cohesion, and confidence of people, yet cannot fully eliminate these effects. This will involve combined activities of structural and awareness measures, technology and policies, cross-regional and international collaboration, and effective governance to provide a layer of protection and Social Cyber Defense (M. S. AlAshry and Al-Saqaf, 2024).

Implications of Findings

The current research suggests certain important lessons to policymakers, organizations, and educators that they should make a real effort to react to cyber threats strategically and that CAL is effective in minimizing their impact. The implications of the conclusions made in this paper are as follows.

Broad Strategies for Improving the Nation’s Security and Safeguarding it From Cyber Threats.

This is the reason why cyber threats are taken as a threat, but not an opportunity to influence the outcomes of the national security with equal -0.50. In the case of governments and organizations, enhancement of the cybersecurity system must continue to be one of the top priorities since vital assets and vital data are still at risk. This includes investing in more advanced equipment, such as artificial intelligence in the field of threat detection, and the introduction of cross-border cooperation to defeat international cybercrimes. It conforms to the strategy that Von Solms and Van Niekerk (2013) suggested that information security ought to be approached as a system with technology, education, and policy being the most important intervention drivers (M. S. AlAshry and Al-Saqaf, 2024).

Creating the New Mathematical Discourse for Establishing Public Trust and Reinforcing Stability

The social cost of cyber threat as a negative factor is quite large, and its effects on the degree of trust and social stability of a population is a staggering -0.83. In turn, the findings present the significance of the communication processes, including the population and the proper reporting and remedial tools to restore trust. One of the recommendations should be the use of educational programs and awareness campaigns to make sure that the population is properly prepared to recognize fake news to combat it as advised by Renaud and Goucher (2018). Lastly, the increase in digital literacy in society could have a significant impact on the preservation of a more consistent societal structure that can also resist the adverse impact of cyber threats (Al-Khawajah, Al-Billeh, and Manasra, 2023).

Using the Positive Influence Brought About by Cybersecurity Awareness and Literacy

The substantive correlations of CAL with both the national security index (0.26 and the correlation of public trust and social stability 0.21 are positive and strong, which indicates the influential power of education and awareness in the preparation against cyber threats. Policy makers and educationists must take advantage of this, hence integrating cybersecurity education in schools, educational faculties, and engagement activities. This is in line with

McGuire and Dowling (2021), who indicate that the mandatory cybersecurity training has been increasing along with the increase in cyber threats (Al-Khatib, Ibrahim, and Alnadi, 2024).

Solving the Contradiction of Cyber Threats

It is revealed that even though cyber threats pose a risk to the sovereignty and social order, they raise awareness about cybersecurity (0.97). This paradox reveals the importance of being proactive about the security of the computer systems across the organization to turn the obstacles into benefits. The higher the threat awareness can assist governments and organizations with good practices such as updates, adopting robust authentication procedures, and security exercises as a priority (Alieksieienko and Kovalyshyn, 2024).

The Role of Mediation: Partial Pelenization of Adverse Effects

The partial mediation effects indicate that the role of CAL was in the reduction of the impact of cyber threats on national security and people's trust. Indicatively, CAL has a positive moderating indirect effect on the relationship between cyber threats and NSO, with (-0.50) and 0.252, respectively. Similarly, it diluted the impact of the PTSS (-0.83), yet its indirect estimation was 0.2037. This reveals the necessity to give CAL more strategic focus in the national cybersecurity systems as we take its limitations into account. Bada and Nurse (2020) state that one can improve the application of CAL in reducing inequality by integrating educational interventions with systemic and professional technological interventions (Alsheyab, 2023).

The importance of Integrated and Multidisciplinary Frameworks

This paper demonstrates that CAL cannot adequately react to multiple threats that are emerging in cyberspace. Knowledge and training, however, ought to be used in a combined and complete management system in which there is profound institutional empowerment. Moreover, exemplary technological platforms and extensive collaboration with other sectors. It is time that the top leadership ought to consider incorporating a sustained and collaborative national approach towards cybersecurity that would encompass the aspects of education, legislation and technologies that will enable everybody to become less susceptible to the dilemmas (Horak, 2023).

Building the Next Generations of Research and Innovation

Finally, the study offers avenues for future research to examine how CAL reacts to various types of cyber threats and other parameters of interest to develop more effective precision-based mitigation measures. It might also be informative to explore the actions that can be undertaken by novel technologies, such as blockchain and quantum, to construct cybersecurity models (Tungohan).

In these implications, the interactive quality of threats and the augmented relevance of the subjects in the sphere of cybersecurity can also be seen. With the investment in education, the belief in the citizenry, and the adoption of a systems perspective, societies can overcome the cyber threats and simultaneously exploit them to create stability and resiliency (Haastrup, 2024).

Limitations of the study

Thus, this study can be used to draw valuable insights into the importance of electronic warfare and cybersecurity threats to Arab national security vulnerability, but it is limited. The fact that Lebanese results apply only to the Arab countries in the Middle East, but not to the rest of the world, is bound to be incorrect. In this instance, there was no effort made by a cross-sectional research design to deal with the problem of time or threats. Another aspect that is not discussed in this study is operational efficiency or the use of advanced technology in the Middle East market, such as artificial intelligence and blockchain. It focuses on the collaboration on the regional level and does not suggest how cooperation in the sphere of intelligence and creation of collective responses could be realised. This study did not go deep into the specifics of cultural, education and behavioural aspects influencing the cybersecurity awareness and attitudes in the Arab societies. One of the risks of the biases that might have been new in sampled studies is the use of structured questionnaires and self-reported measures. This study also provides a limited scope of critical realms of the new world of governance and fails to evaluate more critically the long-term cost-implicating resource-contingent Arab economies. It does not sufficiently address critical legislative and institutional barriers to creating cybersecurity policies in the area (Alsheyab, 2023).

Conclusion

In this study, the authors underline the relationship between cyber threats and national security implications, social trust and cybersecurity awareness and literacy CAL. The study confirms that despite the fact that cyber threats are considered a threat to national security (-0.50) and societal stability (-0.83), the threats are the forces that drive higher cybersecurity awareness (0.97). This issue suggests that a multi-disciplinary solution and systems thinking are required for the table that the cyber threat poses

The indirect protective effect that CAL has on the impacts of cyber threats is rather sensitive to actions aimed at preventing the effects on national security (r = 0.252) and public trust (r = 0.2037). The partial mediation, however, implies that CAL is only capable of neutralising the negative impact of threat in cyberspace to some extent. This demonstrates the necessity to deliver education with unquestionable systemic peculiarities, high-tech solutions, and sound policies. The paper, therefore, recommends that governments, organizations, and educators to improve and adopt cybersecurity literacy as a means of resilience to society. In this case, policymakers and governments need to be more worried when formulating harmonised and integrated national cybersecurity plans in areas of technology in education and legislation in order to provide sufficient responses to emerging threats.

As the information about the cybersecurity threats and the personal and organizational response to these threats has been growing over the years, so have the consequences of the cyber threat, which define the necessity of investing in Cybersecurity Measures International collaboration and research. More studies are needed to determine the way CAL can interact with the emerging giants in the fields of technology, such as blockchain and quantum computing, to develop acute, focused solutions to the impacts of climate change. This hybrid strategy of cyber security and cyber development will bring the digital ecosystem safer and more stable, and will transform the vulnerabilities and threats of cyber criminals into change chances.

Rapid developments in the field of cybersecurity and electronic warfare pose previously unknown threats to the Arab national security. With a growing level of digitization in the Middle East, state and non-state actors are using sophisticated cyber assets to develop disruption in critical infrastructure, manipulate the information environment, and undermine political stability. It is evident through this analysis that electronic warfare is no longer confined to battlefields. Nowadays, it is found in all sectors, including defense and energy as well as media and finance. The ineffective implementation of the cybersecurity policies, the limited cooperation of the Arab nations, and the disastrous dependence on the foreign technologies are the main causes of the vulnerability of the region. To overcome these growing risks, Arab countries have a pressing need to focus on regional cybersecurity cooperation, establish local cyber capability, and come up with full-scale policies that would integrate cyber defense as part of the national security approaches. Through a single, proactive strategy, the Arab world will be able to protect its digital sovereignty and enhance its resilience against the multifarious challenges of the 21st century. It is high time we do it, as far as our security, stability, and future are concerned.

References

Adhikari, L. D. (2024). Exploring the relationship between national security risks and economic factors: A Nepalese perspective. *Journal of Political Science*, 39–56. DOI: https://doi.org/10.3126/jps.v24i1.62853

AlAshry, M.-S. (2024). Arab journalists have no place: Authorities use digital surveillance to control investigative reporting. *Communication & Society*, 37(1), 61–77. https://doi.org/10.15581/003.37.1.61-77,

AlAshry, M. S., & Al-Saqaf, W. (2024). Constraints on AI: Arab journalists' experiences and perceptions of governmental restrictions on ChatGPT. *Journal of Information Technology & Politics*, 1–21. 10. 1080/19331681.2024.2421388.

AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2024). Fintech cybersecurity challenges and regulations: Bahrain case study. *Journal of Computer Information Systems*, 64(6), 835–851. https://doi.org/10.1080/08874417.2023.2251455.

Alieksieienko, I., & Kovalyshyn, L. (2024). The ethno-political context of the median hedging of Turkey as a model for ensuring national stability. *Social Development and Security*, 14(2), 124–131. DOI: https://doi.org/10.33445/sds.2024.14.2.11.

Ali, W. W., & Ahmad, Y. K. Ministry of Higher Education & Scientific Research, University of Kurdistan-Hewler, Diplomacy and International Law Department.

Al-Kasassbeh, F. Y., Ghazleh, A. M. A., & Ma'moon Juma'h, M. K. (2023). International and national efforts to protect cyber security: Jordan case study. *International Journal of Cyber Criminology*, 17(2), 350–363. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/263

Al-Khatib, S. F., Ibrahim, Y. Y., & Alnadi, M. (2024). Cybersecurity practices and supply chain performance: The case of Jordanian banks. *Administrative Sciences*, 15(1), 1. https://doi.org/10.3390/admsci15010001.

Al-Khawajah, N., Al-Billeh, T., & Manasra, M. (2023). Digital forensic challenges in Jordanian cybercrime law. *Pakistan Journal of Criminology*, 15(3). https://www.pjcriminology.com/wp-content/uploads/2023/09/3.-Digital-Forensic-Challenges-in-Jordanian.pdf.

Al-Masaeed, S., Yaseen, H., Al-Adwan, A. S., Altarawneh, A. M., & Alhjouj, A.-H. A. (2023). Social media effect on national security. *Journal of Southwest Jiaotong University*, 58(1). https://jsju.org/index.php/journal/article/view/1490.

Al-Musharafi, N. F. Russia and the Middle East: The geopolitical implication of Russia's growing presence in the Gulf region.

Al-Rawashedeh, M. S. (2015). Scenarios of strategic balance and instability in the Middle East. SSRJ; *International Journal of Humanities & Social Science Studies (IJHSSS)*, *2*(5). 43-57. https://www.internationaljournalssrg.org/IJHSS/paper-details?Id=189.

Al-Rawashedeh, M. S. (2019a). Middle East and the international strategic shifts. *International Research Journal of Human Resource and Social Sciences*, *6*(8). 20-51. https://www.academia.edu/125576183/Middle_East_and_the_International_Strategic_Shifts

Al-Rawashedeh, M. S. (2019b). The dimensions of the internationalization of political and security media on security of the community in the Middle East. *SSRG International Journal of Humanities and Social Science (SSRG-IJHSS)*, *6*(5), 1-10. https://doi.org/10.14445/23942703/IJHSS-V6I5P107.

Al-Rawashedeh, M. S. (n.d.). The repercussions of the global crisis in the Middle East. *Review of History and Political Science*, *7*(2). RL: https://doi.org/10.15640/rhps.v7n2a5.

Alsheyab, M. S. A. (2023). Legal recognition of electronic signature in commercial transactions: A comparison between the Jordanian electronic transactions law of 2015 and the United Arab Emirates electronic transactions and trust services law of 2021. *International Journal for the Semiotics of Law – Revue internationale de Sémiotique juridique*, 36(3), 1281–1291. https://philpapers.org/rec/ALSLRO.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333. https://www.mdpi.com/2079-9292/12/6/1333.

Conduit, D. (2024). Digital authoritarianism and the devolution of authoritarian rule: Examining Syria’s patriotic hackers. *Democratization*, 31(5), 979–997. https://doi.org/10.1080/13510347.2023.218778.

Douzet, F., Pétiniaud, L., Salamatian, K., & Samaan, J.-L. (2023). Digital routes and borders in the Middle East: The geopolitical underpinnings of Internet connectivity. *Territory, Politics, Governance*, 11(6), 1059–1080. https://doi.org/10.1080/21622671.2022.2153726.

East, M., Econornics, H., & Past, P. (2023). The future of. *Middle East*, 9(1). https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/prolif56_tira_oksl_v2.pdf.

Eslami, M., & Vieira, A. V. G. (2023a). *The arms race in the Middle East: Contemporary security dynamics*. Springer Nature.

Eslami, M., & Vieira, A. V. G. (2023b). Introducing the arms race in the Middle East in the twenty-first century: A "powder keg" in the digital era? In *The arms race in the Middle East: Contemporary security dynamics* (pp. 3–13). Springer.

Falowo, O. I., Ozer, M., Li, C., & Abdo, J. B. (2024). Evolving malware & DDoS attacks: Decadal longitudinal study. *IEEE Access*.

Freilich, C. D., Cohen, M. S., & Siboni, G. (2023). *Israel and the cyber threat: How the startup nation became a global cyber power*. Oxford University Press.

Haastrup, T. (2024). *Global conflict trends: Planning for the future*. https://research.manchester.ac.uk/en/publications/global-conflict-trends-planning-for-the-future/.

Hasan, A.-B. H. (2023). Cybersecurity challenges in the transportation industry. https://www.mdpi.com/2079-8954/12/10/397.

Hassib, B., & Ayad, F. (2023). The challenges and implications of military cyber and AI capabilities in the Middle East: The geopolitical, ethical, and technological dimensions. In *The arms race in the Middle East: Contemporary security dynamics* (pp. 49–65). Springer.

Holstein, W. J., & McLaughlin, M. (2023). *Battlefield cyber: How China and Russia are undermining our democracy and national security*. Rowman & Littlefield.

Horak, G. (2023). *Personal details exposed: Spyware and human rights in the Middle East and North Africa*. Harvard University.

Iftikhar, S. (2024). Cyberterrorism as a global threat: A review on repercussions and countermeasures. *PeerJ Computer Science*, 10, e1772. https://peerj.com/articles/cs-1772/.

Kumar, R. (2023). Securing the digital seabed: Countering China's underwater ambitions. *Journal of Indo-Pacific Affairs*, 6(8). https://www.airuniversity.af.edu/JIPA/Display/Article/3588497/securing-the-digital-seabed-countering-chinas-underwater-ambitions/.

Lee, S., Mujammami, A. A. H., & Kim, K. (2024). Leveraging social networks for cyber threat intelligence: Analyzing attack trends and TTPs in the Arab world. *IEEE Access*.

Mahmoud, K. Evolution of Israeli military doctrine: Adaptability in response to shifting strategic environments.

Miniaoui, S., Muammar, S., Muhammad, N., Al Muraqab, N., & Atalla, S. (2024). Do cybercrime laws address emergent IoT security threats? The case of UAE federal cybercrime law regarding RFID technology. *Security Journal*, 37(3), 1112–1122. https://doi.org/10.1057/s41284-023-00408-y.

Mohee, A. (2023). The impact of the Israeli-Iranian cyberwar on Arab regional security.

Montasari, R. (2023). *Countering cyberterrorism: The confluence of artificial intelligence, cyber forensics, and digital policing in US and UK national cybersecurity* (Vol. 101). Springer.

Naz, F., Karim, S., Houcine, A., & Naeem, M. A. (2024). Fintech growth during COVID-19 in MENA region: Current challenges and prospects. *Electronic Commerce Research*, 24(1), 371–392. https://doi.org/10.1007/s10660-022-09583-3.

Nobanee, H., Alodat, A., Bajodah, R., Al-Ali, M., & Al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime*, 30(6), 1736–1754. https://nchr.elsevierpure.com/en/publications/bibliometric-analysis-of-cybercrime-and-cybersecurity-risks-liter/.

Nuseir, M. T., Alquqa, E. K., Al Shraah, A., Alshurideh, M. T., Al Kurdi, B., & Alzoubi, H. M. (2024). Impact of cyber security strategy and integrated strategy on e-logistics performance: An empirical evidence from the UAE petroleum industry. In *Cyber security impact on digitalization and business intelligence* (pp. 89–108). Springer. https://nchr.elsevierpure.com/en/publications/impact-of-cyber-security-strategy-and-integrated-strategy-on-e-lo/.

Petrosyan, M. (2024). The role of non-state actors in modern warfare: The case of Syria and Nagorno-Karabakh. *Journal of Balkan and Near Eastern Studies*, 26(2), 149–163. https://ideas.repec.org/a/taf/cjsbxx/v26y2024i2p149-163.html.

Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in Industry 5.0: A comparative study between Saudi Arabia and the United Kingdom. *Digital*, 3(3), 200–231. https://doi.org/10.3390/digital3030014.

Salim, S., Moustafa, N., & Reisslein, M. (2024). Cybersecurity of satellite communications systems: A comprehensive survey of the space, ground, and links segments. *IEEE Communications Surveys & Tutorials*.

Solar, C. (2023). *Cybersecurity governance in Latin America: States, threats, and alliances*. State University of New York Press.

Sufi, F. (2023). A new social media-driven cyber threat intelligence. *Electronics*, 12(5), 1242. https://doi.org/10.3390/electronics12051242.

Tungohan, E. Managing the multidimensional security threat of cyber attacks: An opportunity to enhance global cyberspace governance.

Tzenios, N. (2023). *How does cultural psychology influence the perception of national security threats?* Charisma University.

Van Puyvelde, D., & Brantly, A. F. (2024). *Cybersecurity: Politics, governance and conflict in cyberspace*. John Wiley & Sons.