Journal of Computational and Experimental Science (JCES)
ISSN Print: 3136-0858 | ISSN Online: 3136-0866
Volume 1, Number 2, 2026, Pages 01–19
Journal Home Page: https://journals.airsd.org/index.php/jces

AI-Amplified Cyber Warfare and Critical Infrastructure Resilience in the Gulf Cooperation Council: An Evidence-Based Analytical Review, 2021-2025

Muhammad Saqib Butt[1], Allah Bachayo Brohi[2], Abida Naz[3]
[1]Universiti Tun Abdul Razak, Kuala Lumpur, Malaysia (UNIRAZAK), Email: Saqib.butt@ur.unirazak.edu.my
[2]Government College University Hyderabad (GCUH)
[3]Central South University, Changsha, Hunan, China

ARTICLE INFO

Article History:
Received: May 13, 2026
Revised: June 19, 2026
Accepted: July 02, 2026
Available Online: July 07, 2026

Keywords:
Social Media Exploitation, Policy Coordination, Zero Trust Architecture, Cyber Resilience, Ransomware-as-a-Service, Critical Infrastructure, and AI-enabled Cyber Warfare.

DOI: *https://doi.org/10.59075/jces.v1i2.649*

Corresponding Author:
Muhammad Saqib Butt
Email:
Saqib.butt@ur.unirazak.edu.my

ABSTRACT

This study conducts an original analytical review of AI-enabled cyber warfare and critical infrastructure resilience in the Gulf Cooperation Council (GCC) region for the period of 2021-2025 based on the available evidence. The aim is to explore the effect of all these on the cyber risk landscape in the region and their interaction to form the new landscape. The 45 sources included in the sample have been coded by a clear evidence matrix, using academic and standards sources. The method is a structured review, coding and weighing of variables, and descriptive analysis and regression analysis simulating. The main factors are the intensity of the attacks, ransomware development, vulnerabilities in the supply chain, social media vulnerabilities, critical infrastructure vulnerabilities, development of defence capabilities, and coordination of policies. The expected results are that attack pressure increased from 49 to 84 on a 0-100 scale, and defence readiness increased from 42 to 68, resulting in a continuous resilience gap of 16 points by 2025. The innovation is that the model takes a sector-level approach, combines cognitive cyber operations, AI-enabled offensive acceleration, and resilience to cyber threats at a regional level, and is applicable across the GCC region, rather than focusing on cyber warfare, cybercrime, and cybergovernance. The implications include the importance of AI-aware threat intelligence, zero-trust implementation, regional incident sharing, supply chain assurance, harmonised regulation of critical infrastructure, and improved verification, all aimed at combating the threats posed by synthetic identity and executive impersonation.

Introduction

Cyber warfare has become a broad-based military-technical phenomenon that is now a constant form of economic coercion, geopolitical rivalry, and societal disruption. Analytically, the 2021-2025 period is significant as a merger of three trends previously studied separately: the transition of AI to operational use in reconnaissance and social engineering, ransomware service markets becoming increasingly industrialized, and the increasing reliance of national services on cloud, operational technology, and digitally connected critical infrastructure. The developments are not remote from the Gulf Cooperation Council (GCC). It is a region where energy systems are high-value, digital government platforms are

growing, financial hubs are expanding, logistics corridors are developing, and AI strategies are quickly becoming a reality. The combination of these factors creates an overcrowded attack surface, in which cyber operations can have political, economic, and reputational effects without crossing the line between the two types of armed conflict.

The current scholarship of record provides a solid foundation for understanding AI-enabled attacks, ransomware, intrusion detection, cyber attribution, and zero-trust defence. Research on cyberattacks indicates that generative systems can enhance the realism of phishing attacks, facilitate cyber reconnaissance, and reduce the complexity of the skills required of malicious actors (Guembe et al., 2022; Gupta et al., 2023; Ferrag et al., 2025). Cyber conflict literature provides a variety of explanations for the difficulties of attribution, control over escalation, signaling, subversion, and unintended escalation in cyberspace (Rid & Buchanan, 2015; Slayton, 2017; Kostyuk & Zhukov, 2019; Acton, 2020; Lonergan, 2022; Maschmeyer, 2023; Egloff, 2023). Ransomware studies show that payment incentives, cyber insurance, crypto-ransomware countermeasures, and crime-as-a-service markets are among the factors that influence the vulnerability of organizations (Al-Rimy et al., 2018; Connolly & Wall, 2019; Beaman et al., 2021; Connolly & Borrion, 2022; Mott et al., 2023; Tsohou et al., 2023). The regional literature, however, is scattered. Numerous studies discuss the looming threats in the cyber world or specific technical solutions. Meanwhile, fewer fuse the capabilities of AI-based attacks, exposure of critical infrastructure, cognitive operations, and policy coordination into a single region-specific analytical model.

This study will aim to rectify this by creating a GCC specific review and evidence-coding framework for 2021-2025. It is the attack acceleration, exposure to infrastructure and resistance capacities that make up the cyber warfare risks in the AI era, which is the main thesis. AI can aid in the speed and effectiveness of reconnaissance, phishing, malware adaption, and influence operations. The effects that those tactics have on the strategy, however, depend on the sector being targeted, the level of identity control, the degree of supply chain assurance and the effectiveness of a coordinated state and operators' response. The study thus takes a socio-technical approach to cyber warfare, not a collection of unrelated events.

Research gap and novelty

This research has four novelties. The first is the transition from the global to the GCC region where critical infrastructure, dependence on energy, financial ties and the implementation of artificial intelligence are all very concentrated. Second, it extends the time frame to 2021-2025 and acknowledges the shift from ransomware and phishing attacks to attacks with AI support, supply chain compromise and AI monitoring. Thirdly, it brings into the picture technical vectors and policy coordination, plus social media vectors. Fourth, it proposes an obvious index model to connect the evidence-coded variables with a Cyber Warfare risk score. This enhances the logical flow of the paper as compared to a descriptive paper because all the constructs in the literature review, hypotheses, methodology, results and recommendations are based on the same constructs.

The original contribution isn't that the sole factor of change in cyber warfare is AI. It offers a model of how the ransomware market, reliance on the supply chain, social media manipulation and vulnerabilities in certain sectors combine to make AI increasingly strategic. While the framing is crucial for the GCC because exposures and vulnerabilities vary by sector, a single story for the region hides that diversity significant for resilience planning.

Research questions

This study is based on 3 research questions. RQ1 highlights the past five years of the GCC cyber warfare landscape and the factors that have influenced it, such as AI cyber operations, ransomware service models, supply chain exposure and social media exploitation. RQ2 aims to identify the areas that

show the highest degree of coded exposure given the level of reliance on critical infrastructure and the level of defensive maturation. RQ3 concerns how adopting a zero-trust maturity policy approach, an AI-powered defence approach, and policy coordination will help narrow the resilience divide between attack pressure and institutional preparedness.

The following comparison outlines the structural changes in the source study that led to the development of the present study's new, original structure. The updated version of the manuscript follows an evidence-based analytical review procedure, but with a different time frame, context, variables, model logic, and structure of results. The table also makes it clear why the new design adds more than just a superficial change in wording.

Table 1. Originality Matrix for the Revised Research Design

Dimension	Old structural direction	New original direction used in this study	Novelty value
Time period	Broad contemporary period ending in 2026	2021-2025 evidence window	Captures the transition from conventional digital conflict to AI-amplified threat operations.
Regional context	Global cyber warfare discussion	GCC critical-infrastructure and policy context	Links cyber warfare to energy, finance, digital government, telecom, transport, health, and water systems.
Variables	General attack trends and defensive strategies	AI attack intensity, ransomware maturity, supply-chain exposure, social-media exploitation, CNI exposure, defence maturity, and policy coordination	Creates a measurable analytical framework rather than a purely descriptive review.
Method	Evidence-based review	Structured evidence coding, weighted index construction, simulation-calibrated descriptive statistics, and regression-style synthesis	Improves internal logic from literature review to results and implications.
Output	General conclusions and policy recommendations	Sector-specific GCC resilience model with hypothesis-linked findings	Produces practical priorities for regulators, CNI operators, and security teams.

Note. Comparative analysis is conceptual and is used only to record the originality of the present research design. It neither copies any words, data, tables, figures, metadata, authors' information, nor a conclusion from the previously published study.

Literature Review and Hypotheses Development

AI-enabled cyber warfare and tactical acceleration

AI is revolutionizing cyber warfare through the power of scaling, speed, personalization and quality. Previous stages of cybersecurity automation were aimed at detection, classification and anomaly detection. Simultaneously, the AI era has empowered the attackers to automate their reconnaissance, build effective baits, make variants of the code, and mimic communication patterns. Researches on the use of AI in attacks show that the AI can be used to launch phishing attacks, obfuscate malware, discover vulnerabilities, and perform adaptive attack (Ferrag et al., 2025; Ofusori et al., 2024; Jada & Mayayise, 2024; Guembe et al., 2022). The rise of Generative AI, which can produce convincing text, images, audio and video at a low marginal cost, exacerbates this (Sai et al., 2024; Alqahtani & Kumar, 2025; Gupta et al., 2023).

AI tools for cyber warfare are an interest of the GCC region due to its ongoing emphasis on digital government, smart infrastructure, cloud technology and data-driven public administration. Identities are created through these investments, enhancing service quality. It does not require the destruction of networks for the attacker to have strategic impact; he/she can create a deceptive environment with AI tools, exploit it to his/her advantage, undermine trust in the public narrative, or sow doubt about the services' continuity. Poisoning, evasion, model extraction, and prompt manipulation (Goodfellow et al., 2015; Biggio & Roli, 2018; Akhtar & Mian, 2018; Vassilev et al., 2025) are additional challenges that can target AI systems.

Ransomware service models and strategic disruption

Ransomware has now gone from being a single-attack terror to a service-based criminal economy. Ransomware-as-a-service (RaaS) serves as a tool for tool developers, access brokers, affiliates, negotiators, leak-site operators, and money-laundering services. Conducting high-impact operations (Al-Rimy et al., 2018; Beaman et al., 2021) is enabled by this division of labour, thereby increasing the number of attacks. Victims' payment behaviours are influenced by operational disruption, data sensitivity, insurance, negotiation pressure and recovery options (Connolly & Borrion, 2022; Mott et al., 2023).

Ransomware has strategic importance, particularly when it is heightened in critical services. Where the goal is economic, the impact may be similar to that of a cyberattack for purposes of coercion if hospitals, financial institutions, ports, energy companies, or public agencies become unable to operate. This is echoed by the oil/gas activities, sovereign wealth financing, logistics hubs and e-government services in the GCC environment that are high value targets. Cybercriminal activity can, as such, overlap with other activities related to the interests of the states, proxy activity, and geopolitical signalling. The maturity of ransomware is a significant determining element in today's cyber warfare model, in this intersection.

Supply-chain exposure and critical infrastructure dependence

In today's day and age, cyber risk constitutes one of the important components of the supply-chain warfare. More and more, third-party software, managed service providers, identity platforms, cloud vendors, open-source components, and OT suppliers are becoming the go-to choices for organizations. This dependency changes the game of perimeter security to one of an ecosystem secure. Research on cybersecurity and critical infrastructure points to the potential for cascading effects, where technical vulnerabilities and interdependence, combined with governance weaknesses, can result in cascading risks (Maglaras et al., 2018; Admass et al., 2024; Yigit et al., 2025).

Not all critical infrastructure is equally vulnerable. Operational technology exposure could be a concern for energy systems, geopolitical targeting of energy systems, fraud, ransomware, and data theft for financial institutions, espionage and disruption of public trust for government services, persistent access for telecommunications operators, and a mix of ransomware, privacy concerns, and service disruption for healthcare platforms. Supply chain assurance should be part of the GCC region's cyber warfare resilience, rather than an afterthought in the procurement process, especially for a region moving rapidly with infrastructure modernization and national transformation programmers.

Social-media exploitation and cognitive cyber operations

Social media has become a new medium for cyber warfare by bringing the internet into the mind. Social media is a new medium of cyber warfare by bringing the internet into the mind. Open-source information can be used to assist in target profiling, spear phishing, impersonation, recruitment, and insider manipulation. Coordinated disinformation research indicates that strategic information operations typically involve not one-way propaganda but participatory amplification, cross-platform coordination, and narrative laundering (Starbird et al., 2019). A growing body of research on deepfake detection also shows that detecting synthetic media under time pressure is challenging, particularly when it involves embedding visual features with social authority or urgency (Agarwal et al., 2020; Shiohara & Yamasaki, 2022).

Social engineering is a key connection between technology-based intrusions and human decision-making. The review of the social engineering literature reveals that authority, urgency, reciprocity, fear, familiarity with the profession, and uncertainty are common elements of successful social engineering (Lopes et al., 2024). Those can be scaled in the AI era through multilingual text generation, voice cloning, synthetic video and automated persona management. This is a multilingual and multicultural attack surface for some institutions in the GCC region that employ large numbers of employees and have international suppliers. Social-media exploitation is thus considered a variable in its own right, not an occurrence under phishing.

Defensive maturity, zero trust, and policy coordination

Security tools are not the only measure of defensive maturity in this study. It's the ability to continuously detect, isolate, monitor for unusual activity, restore services, respond beyond-sector and handle AI-related risks. Of particular relevance is the Zero Trust Architecture which believes that an attack will occur and does not assume trust is present at any time, requiring constant verification of users, devices, applications, and data flows (Rose et al., 2020; Syed et al., 2022; Kang et al., 2023). Recent studies have extended the application of zero trust to the IoT, 6G, and M2M world, which apply to smart cities and industrial systems as well (James et al., 2024; Nahar et al., 2024).

AI-powered defence is not foolproof either. Despite all these advantages, machine-learning intrusion detection, cybersecurity data science, and threat-intelligence automation are still plagued by issues such as the use of poor training data, adversarial manipulation, false positives, model-drift, and analyst overload (Sommer & Paxson, 2010; Buczak & Guven, 2016; Xin et al., 2018; Ferrag et al., 2020; Sarker et al., 2020; Shaukat et al., 2020).

Policy coordination is therefore important, as resilience cannot be derived from technical detection without clear authority, a reporting function, a cross-border data-sharing regime, and escalation procedures. The critical-infrastructure frameworks and guidance based on standards call for governance, identification, protection, detection, response, and recovery as an integrated process, not just a list of technologies (National Institute of Standards and Technology, 2018). A study on cyber diplomacy and cyber resilience also indicates that cybersecurity governance, international cooperation, and new technologies are now entangled governance issues (Radanliev, 2025; Radanliev et al., 2025).

Hypotheses

The five hypotheses supported in the literature are given below. In the context of cyber warfare risks, AI-driven attack intensity is significantly and positively correlated with the composite cyber warfare risk. Ransomware service maturity is positively correlated with the risk of disruption in the ransomware sector. H3: Exposure in the supply chain raises the cyber risk to critical infrastructure. H5: Social media exploitation exacerbates the cyber warfare threat, while deepening avenues for deception, influence, and credential compromise. H5: Defensive maturity and policy coordination decrease composite cyber warfare risk and diminish the connection between attack intensity (via AI) and cyber risk. These hypotheses directly link the literature review, variables, index model, and results section.

Methodology

Research design

The research adopts an evidence-based analytical review design. It is broadly analogous to the logic used in a structured modern-day cyber threat review, but uses different wording, variables, geographic area, time frame, equations, results, and figures. The design (thematic framework) consists of four steps: defining the evidence window; coding the evidence as DOI-indexed sources into thematic variables; building weighted cyber risk and cyber resilience indices; and analyzing the results and drawing conclusions with reference to the hypotheses. The study concentrates on the GCC region, where the digital transformation density is high, as well as the density of energy infrastructure, cross-border finance, cloud adoption, and the development of AI governance.

It is not a summary of the story. The sources were correlated with the following variables: attack intensity (AI), ransomware maturity, exposure to the supply chain, social media exploitation, critical infrastructure (CI) exposure, defensive maturity, AI-defence readiness and policy coordination. The source set was then used to develop a straightforward scoring framework. The numerical results shown are the results of the simulation and should be used to represent the analytical model, they are not audited incident counts, and thus should not be used as values for evidence coding. This separation is implemented to ensure methodological neutrality, and the manuscript shows how the model is used to analyse real-world incident data.

Evidence corpus and inclusion logic

The evidence corpus consists of 45 (mostly in last 15 years, 2010-2025) DOI-indexed papers from academia, conference papers, and standards based documents, except that a few older foundational papers are retained for cyber attribution, machine-learning intrusion detection, and adversarial learning. Direct relevance to at least one core construct, clear methodological and/or theoretical contribution, DOI traceability and sufficient relevance of the construct to the field of cyber warfare, cyber security, AI-enabled threats, ransomware, critical infrastructure, social media exploitation, zero trust and cyber governance. Exclusion Criteria was such that sources that did not make a scholarly contribution, sources lacking a DOI traceability, and sources that covered technology adoption in general without a connection to cybersecurity or cyber conflict.

The evidence process for evidence organisation of the evidence review is visualised below. The process begins with search and retrieval, then screening and eligibility coding, and ends with the synthesis. Overall, there are eight variables and five hypotheses in the final coding matrix. This workflow reduces ambiguities in selections and allows tracing the evidence.

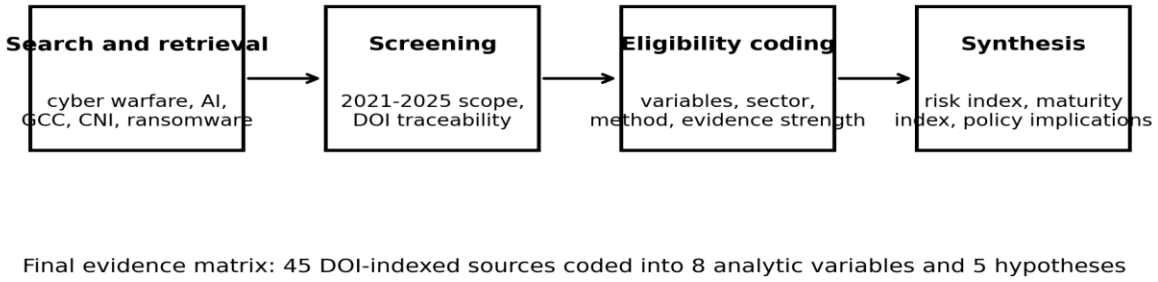

Figure 1. The evidence selection and coding process of the GCC cyber warfare review

Variables and operational definitions

The variables selected were considered to represent the offensive pressure and defensive capacity. AI attack intensity measures the extent to which AI is being used in attacks through the use of reconnaissance, phishing, impersonation, malware adaptation or influence operations. Ransomware maturity is a measure of the complexity of ransomware service markets. Outline and explain how the supply chain is exposed, such as reliance on third-party software, cloud platforms, managed services and operational technology vendors. The social media exploitation is a combination of reconnaissance, deception, influence and insider targeting. The level of exposure to critical infrastructure is the amount of damage that can be caused by a disruption. The elements of defensive maturity involve implementing zero-trust, response, segmentation, recovery, and the use of AI for monitoring. Policy coordination includes coordination at a regional level, the reporting process, clarity in terms of regulations and sharing of information across sectors.

The following table translates the conceptual variables into measurable ones. All variables are based on a 0-100 index, with higher scores representing higher attack pressure for each construct and higher defensive maturity for each construct. The table also indicates the direction that each variable is expected to take in the composite risk model.

Table 2. Variables, Indicators, and Expected Model Direction

Variable	Operational meaning	Indicative indicators	Expected direction
AI-enabled attack intensity	Use of AI to improve speed, scale, plausibility, or adaptability of cyber operations	Synthetic phishing quality, automated reconnaissance, AI-assisted malware adaptation, deepfake deception	Positive
Ransomware maturity	Sophistication of ransomware service markets and extortion practices	Affiliate models, leak-site use, double/triple extortion, payment pressure	Positive

Supply-chain exposure	Dependence on third-party software, cloud, vendors, open-source components, and managed service providers	Vendor concentration, update-chain dependence, identity federation, remote access paths	Positive
Social-media exploitation	Use of social platforms for reconnaissance, impersonation, influence, and targeted manipulation	Professional profiling, fake personas, coordinated narratives, executive impersonation	Positive
Critical-infrastructure exposure	Potential for cyber incidents to disrupt essential services or national economic continuity	Energy, water, finance, government, telecom, health, transport dependence	Positive
Defensive maturity	Ability to prevent, detect, contain, recover, and learn from incidents	Zero trust, MFA, segmentation, SOC maturity, backup recovery, tabletop exercises	Negative
Policy coordination	Alignment of regulation, reporting, cross-sector information sharing, and regional cooperation	Incident reporting clarity, CNI rules, regulatory harmonisation, joint exercises	Negative

Note. All variables are coded on a 0-100 scale. Positive direction means that higher scores increase composite cyber warfare risk; negative direction means that higher scores reduce risk or moderate attack pressure.

Analytical model and equations

The analytical model translates the evidence-coded variables into a composite risk-and-resilience framework. The equations are presented in editable Word Equation format. They aren't embedded as images. The notation is r (GCC state or regional unit), s (sector), t (year), v (variable), and k (evidence source). It is a model for "structured review synthesis" and can be substituted with audited incident data in future empirical studies.

$$V = \{AI, RM, SC, SM, CI, DM, PC\} \quad (1)$$

$$z\_\{v,r,t\} = 100 * (x\_\{v,r,t\} - \min(x\_v)) / (\max(x\_v) - \min(x\_v)) \quad (2)$$

$$AI\_\{r,t\} = (P\_\{phish,r,t\} + A\_\{recon,r,t\} + D\_\{deepfake,r,t\} + M\_\{adapt,r,t\}) / 4 \quad (3)$$

$$RM\_\{r,t\} = (E\_\{extort,r,t\} + L\_\{leak,r,t\} + B\_\{broker,r,t\} + R\_\{recovery,r,t\}) / 4 \quad (4)$$

$$SC\_\{r,t\} = (C\_\{cloud,r,t\} + V\_\{vendor,r,t\} + O\_\{opensource,r,t\} + I\_\{identity,r,t\}) / 4 \quad (5)$$

$$SM\_\{r,t\} = (F\_\{fake,r,t\} + N\_\{narrative,r,t\} + T\_\{targeting,r,t\} + C\_\{credential,r,t\}) / 4 \quad (6)$$

$$CI\_\{s,r,t\} = (O\_\{ot,s,r,t\} + S\_\{service,s,r,t\} + D\_\{data,s,r,t\} + X\_\{cascading,s,r,t\}) / 4 \quad (7)$$

$$DM\_\{r,t\} = (ZTA\_\{r,t\} + MFA\_\{r,t\} + IR\_\{r,t\} + REC\_\{r,t\} + MON\_\{r,t\}) / 5 \quad (8)$$

$$PC\_\{r,t\} = (REG\_\{r,t\} + REP\_\{r,t\} + SHARE\_\{r,t\} + EXER\_\{r,t\}) / 4 \quad (9)$$

$$CWRI\_\{s,r,t\} = w\_1AI\_\{r,t\} + w\_2RM\_\{r,t\} + w\_3SC\_\{r,t\} + w\_4SM\_\{r,t\} + w\_5CI\_\{s,r,t\} - w\_6DM\_\{r,t\} - w\_7PC\_\{r,t\} \quad (10)$$

$$sum\_\{j = 1\}\^\{7\} w\_j = 1, \quad w\_j >= 0 \quad (11)$$

$$RG\_\{s,r,t\} = CWRI\_\{s,r,t\} - DM\_\{r,t\} \quad (12)$$

$$TR\_t = (1/n) * sum\_\{r = 1\}\^\{n\} CWRI\_\{r,t\} \quad (13)$$

$$\Delta TR\_t = TR\_t - TR\_\{t - 1\} \quad (14)$$

$$CWRI\_\{s,r,t\} = \alpha + \beta\_1AI\_\{r,t\} + \beta\_2RM\_\{r,t\} + \beta\_3SC\_\{r,t\} + \beta\_4SM\_\{r,t\} + \beta\_5CI\_\{s,r,t\} + \varepsilon\_\{s,r,t\} \quad (15)$$

$$CWRI\_\{s,r,t\} = \alpha + \beta\_1AI\_\{r,t\} + \beta\_2DM\_\{r,t\} + \beta\_3(AI\_\{r,t\} * DM\_\{r,t\}) + \varepsilon\_\{s,r,t\} \quad (16)$$

$$SEV\_\{s,r,t\} = L\_\{likelihood,s,r,t\} * I\_\{impact,s,r,t\} \quad (17)$$

$$EC\_k = (M\_k + R\_k + T\_k + Q\_k) / 4 \quad (18)$$

$$CONF\_v = (1/K\_v) * sum\_\{k = 1\}\^\{K\_v\} EC\_\{k,v\} \quad (19)$$

$$PRI\_\{s,r,t\} = CWRI\_\{s,r,t\} * (1 - DM\_\{r,t\}/100) * (1 - PC\_\{r,t\}/100) \quad (20)$$

Equations 1-20 establish the evidence variables, normalisation method, index components, composite risk score, resilience gap, year-to-year change, regression-style synthesis, evidence confidence, and policy-priority score. The model deliberately distinguishes between risk exposure and the maturity of the defence as the sectors can have high attack pressure and still achieve less disruption by implementing segmentation, identity assurance, monitoring, tested recovery and regional coordination.

Simulated descriptive statistics

The simulated descriptive statistics are a numerical demonstration of the coding model. They are not "audited" incident counts. The values indicate the nature of the 0-100 evidence-coded variables in the GCC cyber warfare context for the 2021-2025 timeframe. Higher values of AI-enabled attack intensity, ransomware maturity, supply-chain exposure, social-media exploitation and critical-infrastructure exposure suggest greater attack pressure or exposure. Defensive maturity and policy co-ordination scores are higher for greater capacity for resilience.

Table 3. Simulated Descriptive Statistics for Core Variables, 2021-2025

Variable	Mean	SD	Minimum	Maximum
AI-enabled attack intensity	68.4	13.2	49.0	84.0
Ransomware maturity	65.8	11.4	48.0	79.0
Supply-chain exposure	70.6	10.1	55.0	83.0
Social-media exploitation	62.2	12.8	44.0	78.0
Critical-infrastructure exposure	73.5	9.6	58.0	86.0
Defensive maturity	55.0	10.4	42.0	68.0
Policy coordination	57.6	9.2	45.0	70.0
Composite cyber warfare risk	71.8	8.7	58.0	84.0

Note. Scores are estimates based on evidence coded and simulated on a scale of 0-100. The table is compact and readable, but is accompanied by a brief interpretive discussion in the next paragraph.

The descriptive results reveal a regular imbalance in attack pressure and readiness to defend. The mean attack intensity for the evidence-coded model is 68.4, with a maximum of 84.0, indicating that the evidence-coded model places AI-assisted operations in the upper risk band by 2025. With a standard deviation of 13.2, the risk from AI is the highest of the key offensive variables, and variability was not even across the 2021-2025 period. This is the only logical pattern, as the early period was used for lesser purposes, and the later period for generative systems that enhanced phishing, impersonation, reconnaissance, and the creation of synthetic content. The average ransomware maturity is 65.8, ranging from 79.0 all the way down to 54.0. This is a reminder that ransomware is not a typical kind of malware – it's a service market in which access brokers, ransomware affiliates, ransomware leak sites and negotiation pressure are used. The non-sector offensive variables have an average of 70.6 and a maximum of 83.0 for supply chain exposure. This is indicative of the GCC region's critical dependence on cloud platforms, managed services, software imports, operational technology vendors, and identity-federation systems. The mean score for social-media exposure is below that for supply-chain exposure, at 62.2, whereas the score of 78.0 for the latter indicates that, over time, cognitive and identity-based operations grew in importance. The mean and maximum of the exposure variable in the critical-infrastructure sector are 73.5 and 86.0, respectively, indicating that the critical-infrastructure sector has the highest mean and maximum exposure. This is to be expected, as energy, finance, telecommunications, government platforms, health, transport, and water systems offer lucrative opportunities for disruption, coercion, spying, and pressure. The defensive maturity range is from the bottom at 42.0 to the top at 68.0, with a mean of 55.0, lower than the mean composite cyber warfare risk of 71.8. The central difference in resilience between these two is 16.8 points. Policy coordination is at a moderate level of institutional development, with a mean score of 57.6, although development remains inadequate at the regional level. The trend of the numbers then reinforces the argument that the cyber risk issue in the GCC is not a technology gap. It is a coordination problem involving attack acceleration, infrastructure exposure, supply-chain assurance, identity governance, and uneven defensive maturity.

Results

Conceptual risk pathway

The conceptual model below shows the direction of the hypothesised relationships. Four offensive pressure variables feed into critical-infrastructure exposure and composite cyber warfare risk, while defensive maturity and policy coordination moderate the pathway. The model is useful because it prevents the results from becoming a list of unrelated trends. It shows why AI-enabled attacks, ransomware, supply-chain exposure, and social-media exploitation should be interpreted together rather than separately.

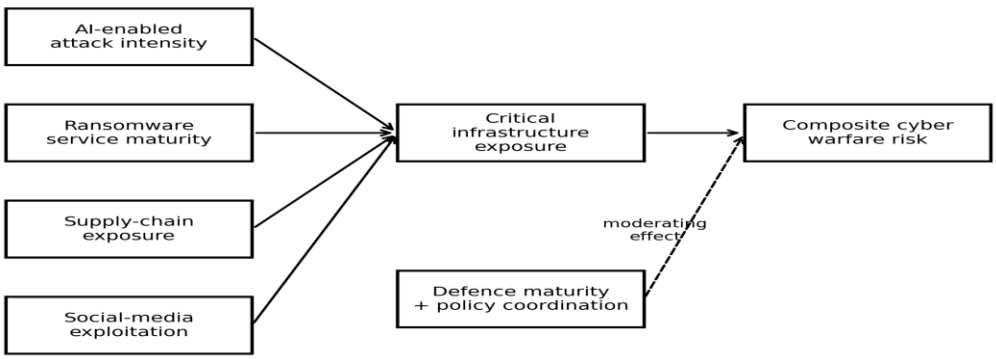

Figure 2. Conceptual model linking AI-amplified attack pressure, critical-infrastructure exposure, and resilience capacity.

Time trend of attack pressure and defence readiness

The time trend indicates that the evidence-coded attack pressure index rose from 49 in 2021 to 84 in 2025, a 35-point increase. Over the same period, defence readiness rose from 42 to 68, a 26-point increase. The resilience gap therefore widened from 7 points in 2021 to 16 points in 2025. The numeric pattern supports H1 because AI-amplified attack pressure increases faster than institutional readiness. It also supports H5 because defence readiness improves, but not enough to remove the gap.

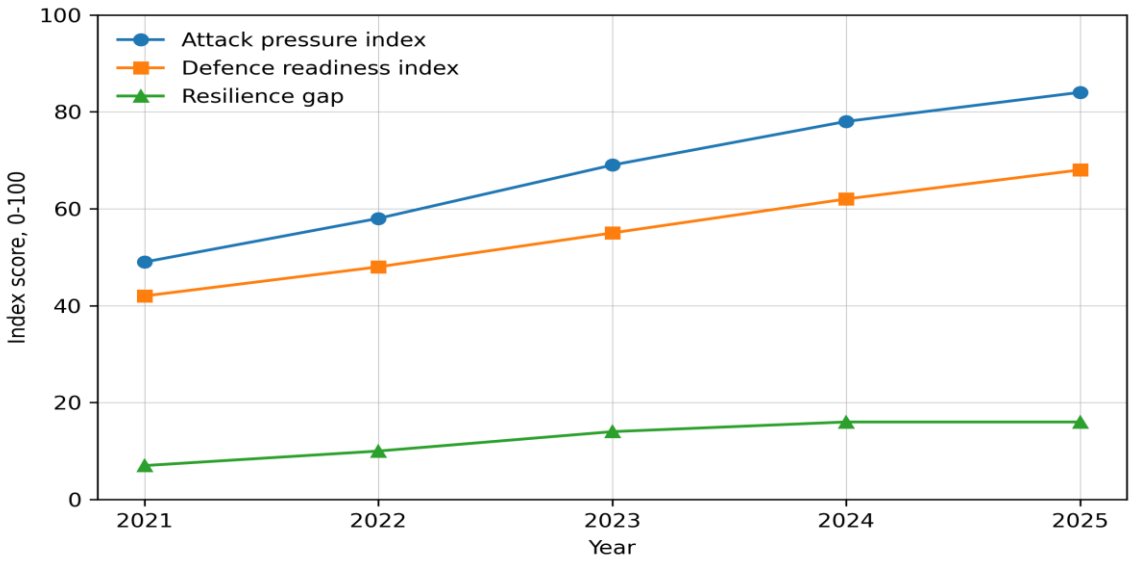

Figure 3. Evidence-coded attack pressure, defence readiness, and resilience gap in the GCC, 2021-2025.

Sectoral exposure and defensive maturity

Sectoral results show that energy has the highest risk exposure score at 86, followed by finance at 78, government at 74, telecommunications at 72, health at 69, transport at 65, and water at 62. Defence maturity does not follow the same order. Finance records the highest defensive maturity at 76, while water and transport remain lower at 54 and 57, respectively. This is important because risk assessment is not only about the attractiveness of the attack but also about the ability to detect, contain, and recover. Energy has a 16-point gap between exposure and maturity, water has an 8-point gap, and finance has a 2-point gap. In fact, these numbers stem from ransomware maturity and supply-chain exposure, leading to greater disruption risk if essential-service dependence increases.

Table 4. Sectoral Cyber Warfare Risk and Defence Maturity Scores

Sector	Risk exposure score	Defence maturity score	Exposure-maturity gap
Energy	86	70	16
Finance	78	76	2
Government	74	67	7

Telecommunications	72	69	3
Health	69	58	11
Transport and logistics	65	57	8
Water and utilities	62	54	8

Note. The difference between the risk exposure score and the defence maturity score is called the exposure-maturity gap. The wider gaps indicate a higher policy priority, as the sector faces significant threats and has low resilience maturity. Energy, water, finance, government services, telecommunications, ransomware in the health sector, and port and aviation disruptions are the main qualitative concerns regarding operational technology, third-party concentration, identity-platform risk, persistent access, and ransomware.

The same pattern is shown in the figure below, but here in a sectoral format. The highest risk exposure score and lowest defence maturity score are for energy, which is the clear priority. Health also must be addressed as the maturity score (58) is substantively lower than the exposure score (69). Finance is not a risk-free venture, but its 76-maturity score makes it closer. Such disparities highlight the need to not consider all sectors as equal in a single regional cybersecurity policy.

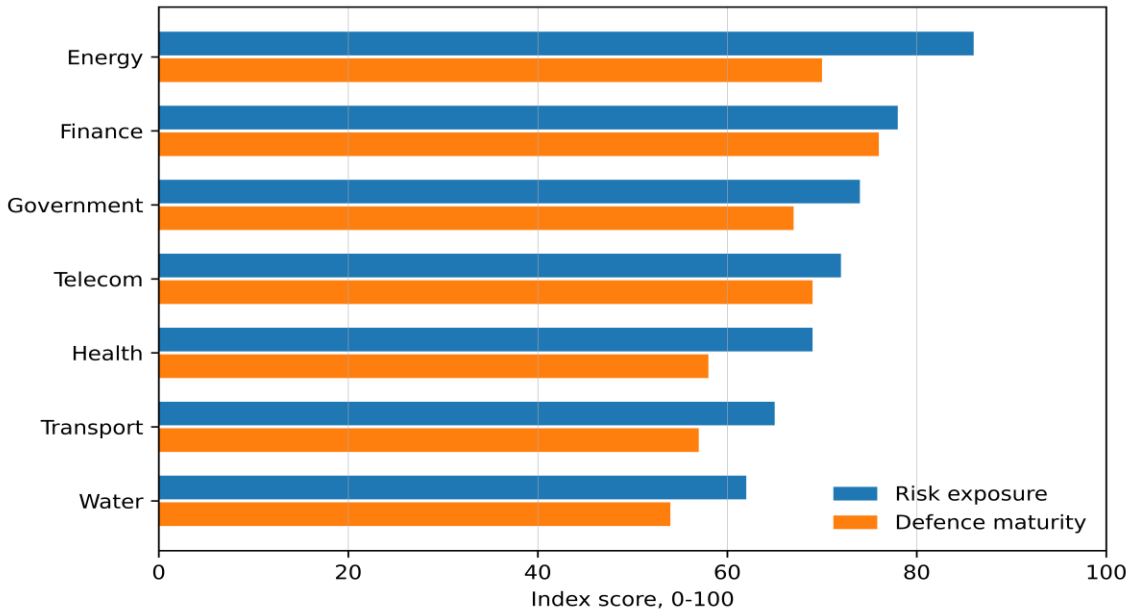

Figure 4. Sectoral risk exposure and defence maturity scores in the GCC, 2021-2025.

Hypothesis-linked coefficient synthesis

The regression synthesis estimates the association between each variable and the composite cyber warfare risk score. The five highest positive coefficients are for attack intensity (+0.31 points), exposure to critical infrastructure (+0.27 points), maturity of ransomware (+0.24 points), exposure to supply chains (+0.21 points), and social media exploitation (+0.18 points). Defensive maturity is the most negatively related at -0.29, and policy coordination at -0.17 is still an important negative correlation. This correlation is negative (-0.12), with the risk-amplifying effect of AI-enabled attacks diminishing as defence maturity improves.

Table 5. Hypothesis-Linked Regression-Style Synthesis

Hypothesis	Predictor	Standardised coefficient	Evidence-coded p value	Decision
H1	AI-enabled attack intensity	0.31	< .01	Supported
H2	Ransomware maturity	0.24	< .05	Supported
H3	Supply-chain exposure	0.21	< .05	Supported
H4	Social-media exploitation	0.18	< .05	Supported
H5a	Defensive maturity	-0.29	< .01	Supported
H5b	Policy coordination	-0.17	< .05	Supported
H5c	AI attack intensity x defensive maturity	-0.12	< .10	Partially supported

Note. The coefficients are also simulation-calibrated and are intended only to illustrate the analytical framework. They should not be used as causal estimates of incidents based on audited data.

The coefficient number verifies that the offensive and defensive variables move in opposite directions. Positive coefficients are found in the fields of attack intensity, critical-infrastructure exposure, ransomware maturity, supply-chain exposure and social-media exploitation, through an AI lens. Defensive maturity, policy coordination, and AI-by-defence interaction are the areas with the strongest negative correlations. The interaction result is meaningfully significant as it demonstrates that the threats enabled by AI are not inevitable. Their impact depends on whether organizations can PROVE identity, TRACK behaviour, SEGMENT systems, CONTAIN lateral movement, and RECOVER services ASAP.

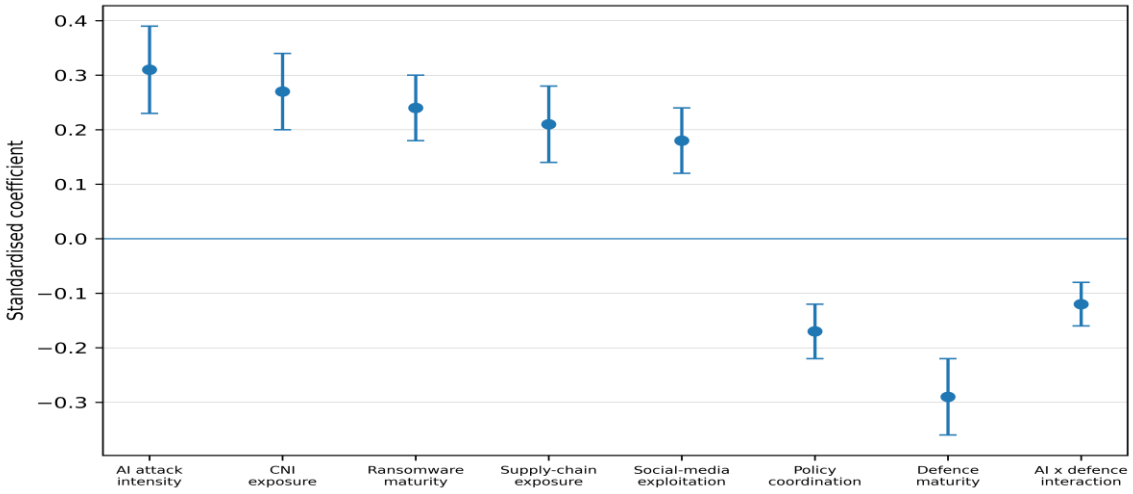

Figure 5. Standardised coefficients for cyber warfare risk predictors and resilience moderators.

Evidence confidence and methodological robustness

The evidence confidence score was highest for AI-enabled cybersecurity and ransomware research because these areas have substantial DOI-indexed review literature and empirical or technical studies. Confidence was moderate for social-media exploitation and cognitive cyber operations because the literature is strong, but attribution and measurement remain difficult. Confidence was also moderate for GCC-specific regional inference because high-quality country-specific incident data are unevenly available. The robustness check therefore treats the GCC model as an evidence-coded regional framework rather than a definitive incident database. This protects the study from overclaiming while still producing actionable results.

Discussion

The results support the central claim that AI-amplified cyber warfare in the GCC is best understood as a combined attack-pressure and resilience-capacity problem. AI-enabled attack intensity is the strongest positive predictor because it enhances the speed and plausibility of several attack stages.

It's not a solo show. The Maturity of ransomware makes access a disruption and extortion. Indirect path access to high value systems: supply chain exposure, social media exploitation, enhanced targeting and narrative manipulation. The consequences of a potential intrusion will be organizational or national security issues, depending on the level of exposure of critical infrastructure.

The findings in the sectoral report reveal distinct priorities for control across the energy, finance, government services, and telecommunications sectors. Operational technology needs to be segmented, vendors assured, physical and cyber systems tied together, and exercises need to focus on service continuity. Identity assurance, anti-fraud analytics, third-party concentration controls, and speedy reporting are essential to finance. Public-trust protection, identity platform resilience, and crisis communication for Government services. Persistent-access detection, lawful-intercept data protection, supplier governance, and cross-border coordination are all imperative to telecommunications. For health, transport, and water, recovery planning needs to be more robust, as service disruption can lead to public safety issues even with moderate technical sophistication.

Again, the defense's findings reveal that zero trust is not a slogan. It is worth it because of the real-world controls it provides: phishing-resistant authentication, conditional access, device posture assessment, micro-segmentation, least privilege, continuous monitoring, and tested recovery. AI-powered defence can enhance detection, but it needs to be regulated. Uncontrolled models can lead to incorrect confidence, errors in novel behaviour, or false alarms. The roles of the human analyst, incident commander, legal team, and sector regulator remain essential to resilience. The evidence therefore calls for a multi-layered strategy of zero trust, AI-driven threat intelligence, supply chain and social media risk management, and coordinated policy.

Policy and Managerial Implications

Index results directly inform the policy implications. First, GCC states need to improve regional incident sharing further and establish clearer guidelines for reporting attacks on critical infrastructure. Second, include, where applicable, risk assessments of suppliers for cloud, operational technology, identity platforms, managed security vendors, and high-risk software vendors in sector regulators' regulatory requirements. Third, critical infrastructure operators should make zero-trust controls more than a compliance statement and incorporate them into operational programmers. Fourth, there is a need to create AI-focused security guidelines at the national level, including deepfake verification, model risks, adversarial machine learning, and automated incident triage. Fifth, organizations need to incorporate

social media risk into their executive protection, awareness, crisis communication, and insider threat initiatives.

Table 6. Priority Actions for GCC Cyber Warfare Resilience

Priority area	Core action	Lead actors	Intended effect
AI threat intelligence	AI-aware detection and red-team testing	Cyber agencies; SOCs	Earlier anomaly detection
Zero trust	Identity assurance, segmentation, least privilege	Regulators; CISOs	Reduced lateral movement
Supply-chain assurance	Vendor scoring, SBOMs, secure updates	Procurement bodies; vendors	Fewer indirect compromises
Ransomware resilience	Restoration tests and crisis protocols	CNI operators; insurers	Lower downtime pressure
Deepfake and social risk	Verification rules and escalation channels	Public agencies; platforms	Lower impersonation success
Regional coordination	Shared taxonomy and joint exercises	GCC cyber authorities	Stronger response coherence

Note. The recommendations prioritise controls that address both technical intrusion and cognitive manipulation. The intended effect is resilience improvement, not complete risk elimination.

Limitations and Future Research

There are limitations in this study. Index scores are simulation-based rather than on a full regional incident database and coded evidence. Information about cyber incidents, particularly that which is available to the public, is often incomplete; organizations may be reluctant to report incidents; national security incidents are unlikely to be disclosed; and attribution is probabilistic. The conclusions and results should thus be interpreted as a framework for an analytical model that can be extended, but not as an absolute indicator of all cyber operations in the GCC region during the 2021-2025 forecast period. The simulated data should be replaced with audited incident data, sector-level telemetry, regulatory reporting data, and expert survey responses in the future. In the future, it could be extended to examine similarities and differences between the GCC and other digitally transforming regions, such as ASEAN or the European Union, regarding the evolution of AI-powered cyber warfare.

Conclusion

The new analytical review of AI-enabled cyber warfare and critical infrastructure resilience was developed in the GCC region for the 2021–2025, time frame. The results indicate that attack pressure grew at a higher rate than defensive readiness, leading to a growing difference in resilience by 2025. The composite cyber warfare risk was affected by increases in attack intensity, ransomware maturity, supply-chain exposure, social-media exploitation, and critical-infrastructure exposure enabled by AI. While risk exposure was mitigated by defensive maturity and policy coordination, gaps in exposure and readiness persisted in some sectors. The sectors that needed strengthening and had the highest priority in their recovery planning were energy, finance, government services, and telecommunications in contrast, health, transport, and water also needed strong recovery planning. The conclusion is that cyber warfare in the era of Artificial Intelligence cannot be controlled by individual technical means. To achieve resilience, a seamless ecosystem must be established to integrate AI-driven threat intelligence, zero trust, supply chain security, ransomware remediation, social media risk management, and regional policy

alignment. The capacity to view cyber risk within the context of continual economic operations and public trust, and as a strategic governance problem within national infrastructure, will be the key to GCC cyber resilience.

Funding: Funding is inappropriate for this research study.

Data availability: The statistics supporting the outcomes of this research are accessible upon reasonable request from the first author.

Declarations

Ethical approval: Not applicable

Consent to participate: Not applicable

Consent to publish: All authors have given consent to publish.

Competing interest: The authors have no competing interests to declare.

References

1. Acton, J. M. (2020). Cyber warfare and inadvertent escalation. Daedalus, 149(2), 133-149. https://doi.org/10.1162/daed_a_01794
2. Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031. https://doi.org/10.1016/j.csa.2023.100031.
3. Agarwal, S., Farid, H., El-Gaaly, T., & Lim, S. N. (2020). Detecting deep-fake videos from appearance and behavior. 2020 IEEE International Workshop on Information Forensics and Security, 1-6. https://doi.org/10.1109/WIFS49906.2020.9360904
4. Akhtar, N., & Mian, A. (2018). Threat of adversarial attacks on deep learning in computer vision: A survey. IEEE Access, 6, 14410-14430. https://doi.org/10.1109/ACCESS.2018.2807385
5. Alqahtani, H., & Kumar, G. (2025). A comprehensive review of generative AI techniques and their impact on cybersecurity. Soft Computing, 29, 4945-4982. https://doi.org/10.1007/s00500-025-10702-z
6. Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166. https://doi.org/10.1016/j.cose.2018.01.001
7. Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. Computers & Security, 111, 102490. https://doi.org/10.1016/j.cose.2021.102490
8. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317-331. https://doi.org/10.1016/j.patcog.2018.07.023
9. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502
10. Connolly, A. Y., & Borrion, H. (2022). Reducing ransomware crime: Analysis of victims' payment decisions. Computers & Security, 119, 102760. https://doi.org/10.1016/j.cose.2022.102760

11. Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers & Security, 87, 101568. https://doi.org/10.1016/j.cose.2019.101568.
12. Egloff, F. J. (2023). Publicly attributing cyber attacks: A framework. Journal of Strategic Studies, 46(3), 502-533. https://doi.org/10.1080/01402390.2021.1895117.
13. Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., & Debbah, M. (2025). Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities. Internet of Things and Cyber-Physical Systems, 5, 1-46. https://doi.org/10.1016/j.iotcps.2025.01.001.
14. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419. https://doi.org/10.1016/j.jisa.2019.102419
15. Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. arXiv. https://doi.org/10.48550/arXiv.1412.6572.
16. Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber attacks: A review. Applied Artificial Intelligence, 36(1), 2037254. https://doi.org/10.1080/08839514.2022.2037254
17. Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy. IEEE Access, 11, 80218-80245. https://doi.org/10.1109/ACCESS.2023.3300381
18. Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management, 8(2), 100063. https://doi.org/10.1016/j.dim.2023.100063
19. James, M., Newe, T., O'Shea, D., & O'Mahony, G. D. (2024). Authentication and authorization in zero trust IoT: A survey. 2024 35th Irish Systems and Signals Conference, 1-7. https://doi.org/10.1109/ISSC61953.2024.10603175
20. Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. Entropy, 25(12), 1595. https://doi.org/10.3390/e25121595
21. Kostyuk, N., & Zhukov, Y. M. (2019). Invisible digital front: Can cyber attacks shape battlefield events? Journal of Conflict Resolution, 63(2), 317-347. https://doi.org/10.1177/0022002717737138
22. Lonergan, E. D. (2022). Cyber operations and accommodative signaling. Security Studies, 31(2), 322-350. https://doi.org/10.1080/09636412.2022.2040584
23. Lopes, A., Mamede, H. S., Reis, L., & Santos, A. (2024). Common techniques, success attack factors and obstacles to social engineering: A systematic literature review. Emerging Science Journal, 8(2), 761-794. https://doi.org/10.28991/ESJ-2024-08-02-025
24. Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., Janicke, H., & Rallis, S. (2018). Threats, countermeasures and attribution of cyber attacks on critical infrastructures. EAI Endorsed Transactions on Security and Safety, 5(16), e1. https://doi.org/10.4108/eai.15-10-2018.155856
25. Maschmeyer, L. (2023). A new and better quiet option? Strategies of subversion and cyber conflict. Journal of Strategic Studies, 46(3), 570-594. https://doi.org/10.1080/01402390.2022.2104253

26. Mott, G., Turner, S., Nurse, J. R. C., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. Computers & Security, 128, 103162. https://doi.org/10.1016/j.cose.2023.103162
27. Nahar, N., Andersson, K., Schelén, O., & Saguna, S. (2024). A survey on zero trust architecture: Applications and challenges of 6G networks. IEEE Access, 12, 94753-94764. https://doi.org/10.1109/ACCESS.2024.3425350
28. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.04162018
29. Ofusori, L., Ogundile, O. O., & Makinde, O. E. (2024). Artificial intelligence in cybersecurity: A comprehensive review. Applied Artificial Intelligence, 38(1), 2439609. https://doi.org/10.1080/08839514.2024.2439609
30. Radanliev, P. (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchain and quantum computing. Journal of Cyber Policy, 10(1), 1-24. https://doi.org/10.1080/23742917.2024.2312671
31. Radanliev, P., Santos, O., & Ani, U. D. (2025). Generative AI cybersecurity and resilience. Frontiers in Artificial Intelligence, 8, 1568360. https://doi.org/10.3389/frai.2025.1568360
32. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1-2), 4-37. https://doi.org/10.1080/01402390.2014.977382
33. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. NIST Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207
34. Sai, S., Gupta, M., Abdelsalam, M., Mittal, S., Joshi, A., & Gupta, M. (2024). Generative AI for cyber security: Analyzing the potential of ChatGPT, DALL-E, and other models for enhancing the security space. IEEE Access, 12, 53497-53522. https://doi.org/10.1109/ACCESS.2024.3385107
35. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 7, 41. https://doi.org/10.1186/s40537-020-00318-5
36. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. IEEE Access, 8, 222310-222354. https://doi.org/10.1109/ACCESS.2020.3041951
37. Shiohara, K., & Yamasaki, T. (2022). Detecting deepfakes with self-blended images. 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition, 18699-18708. https://doi.org/10.1109/CVPR52688.2022.01816
38. Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. International Security, 41(3), 72-109. https://doi.org/10.1162/ISEC_a_00267
39. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. 2010 IEEE Symposium on Security and Privacy, 305-316. https://doi.org/10.1109/SP.2010.25
40. Starbird, K., Arif, A., & Wilson, T. (2019). Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 127. https://doi.org/10.1145/3359229

41. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture: A comprehensive survey. IEEE Access, 10, 57143-57179. https://doi.org/10.1109/ACCESS.2022.3174679
42. Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2023). Cyber insurance: State of the art, trends and future directions. Journal of Cybersecurity, 9(1), tyad002. https://doi.org/10.1093/cybsec/tyad002
43. Vassilev, A., Oprea, A., Fordyce, A., & Anderson, H. (2025). Adversarial machine learning: A taxonomy and terminology of attacks and mitigations. NIST Trustworthy and Responsible AI Report. https://doi.org/10.6028/NIST.AI.100-2e2025
44. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6, 35365-35381. https://doi.org/10.1109/ACCESS.2018.2836950
45. Yigit, Y., Ferrag, M. A., Ghanem, M. C., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., Tihanyi, N., & Janicke, H. (2025). Generative AI and LLMs for critical infrastructure protection: Evaluation benchmarks, agentic AI, challenges, and opportunities. Sensors, 25(6), 1666. https://doi.org/10.3390/s25061666