Musik in bayern
ISSN: 0937-583x Volume 90, Issue 3 (March -2025)
https://musikinbayern.com **DOI https://doi.org/10.15463/gfbm-mib-2025-391**

Cyber Warfare 2025: The Evolution of Cyber-Attacks and Future of Cryptography

Dr. Shyamala K* & Dr. Siji Jose **
Associate Professor* & Assistant Professor**
Department of Commerce
S.D.N.B. Vaishnav College for women, Chromepet, Chennai – 600 044.

To Cite this Article
Dr. Shyamala K* & Dr. Siji Jose " **Cyber Warfare 2025: The Evolution of Cyber-Attacks and Future of Cryptography**" *Musik In Bayern, Vol. 90, Issue 3, Mar 2025, pp146-164*

Article Info
Received: 31-01-2025 Revised: 09-03-2025 Accepted: 20-03-2025 Published: 31-03-2025

Abstract

Cyber warfare has rapidly evolved, becoming a critical national security concern as cyber-attacks grow more sophisticated. By 2025, cyber threats are expected to surpass traditional warfare in significance, driven by advancements in artificial intelligence (AI), quantum computing, and state-sponsored cyber operations. This paper explores the **evolution of cyber-attacks**, the role of AI in both offensive and defensive cybersecurity strategies, and the impact of quantum computing on encryption. Additionally, it examines the effectiveness of current cybersecurity measures, the urgency of adopting post-quantum cryptographic methods, and the role of global cooperation in preventing large-scale cyber conflicts. With organizations and governments facing an increasingly complex threat landscape, this study highlights the importance of **ethical hacking, zero-trust security models, and regulatory policies** in shaping the future of cybersecurity.

Keywords:

Cyber warfare, cyber-attacks, artificial intelligence (AI), quantum computing, encryption, post-quantum cryptography, zero-trust security, ethical hacking, state-sponsored attacks, cybersecurity regulations.

Introduction

The rapid digitization of global infrastructure has led to an unprecedented increase in cyber threats, making cyber warfare a major security concern for governments, organizations, and

individuals. As we approach 2025, cyber-attacks are becoming more sophisticated, frequent, and damaging, fueled by advancements in artificial intelligence (AI), quantum computing, and state-sponsored cyber operations. Unlike traditional warfare, cyber conflicts are fought in the digital space, where nation-states, cybercriminal groups, and hacktivists exploit vulnerabilities in critical infrastructure, financial systems, and communication networks.

AI-powered cyber-attacks, ransomware campaigns, and deepfake misinformation campaigns are increasingly shaping modern cyber warfare tactics. At the same time, quantum computing poses an existential threat to existing cryptographic methods, potentially rendering widely used encryption systems obsolete. These technological advancements create an urgent need for stronger cybersecurity strategies, international regulations, and cryptographic innovations to defend against emerging threats.

Cyber-attacks, the role of AI in cybersecurity, and the future of cryptography, particularly the transition to post-quantum cryptographic solutions. It also examines the effectiveness of current security frameworks, the need for zero-trust architectures, and the role of ethical hacking in cyber defense. With global cooperation playing a crucial role in mitigating cyber threats, this study highlights the importance of international treaties, cybersecurity regulations, and proactive security measures in shaping the future of cyber warfare.

Review of Literature

Singer & Friedman (2014), Cyber warfare has evolved from basic hacking attempts to highly sophisticated state-sponsored cyber operations. Nation-states have increasingly engaged in cyber-attacks to achieve political, economic, and military objectives. According to cyber warfare represents the fifth domain of warfare, alongside land, sea, air, and space, with adversaries targeting critical infrastructure, financial institutions, and military systems.

Recent cyber incidents, such as the 2020 SolarWinds attack, demonstrate how adversaries infiltrate supply chains to compromise government and corporate networks (Kostyuk & Zhukov, 2019). The rise of ransomware-as-a-service (RaaS) and AI-powered cyber-attacks further complicates defense strategies (Sitt & Pahi, 2022). These developments indicate that cyber warfare will continue to evolve, with AI playing a key role in both offense and defense.

AI is transforming cyber warfare, making both attacks and defenses more efficient, autonomous, and scalable. Brundage et al. (2018) highlight how AI can automate cyber-attacks,

bypass traditional security measures, and generate advanced phishing campaigns using deep learning techniques. Conversely, AI-driven threat detection systems enable real-time anomaly detection, malware analysis, and automated incident response (Sharma et al., 2021).

Despite its advantages, AI also introduces risks, as adversaries can manipulate AI models to bypass security controls (Papernot et al., 2017). This AI arms race in cyber warfare underscores the need for robust AI-based cybersecurity frameworks and ethical AI implementation.

Objectives of the study

- To study the demographic profile of the respondents.
- To know General Information & Cyber Warfare and Emerging Threats.
- To find the Future of Cryptography.
- To analysis the Future Cyber security Strategies.
- To identify the Cyber Warfare Perception & increasing role of cyber warfare in global conflicts.

Hypothesis of the study

- The factors of Cyber Warfare Perception do no differ significantly.
- The factors of cyber warfare do not differ significantly.

Research Methodology

Data size	**234**
Sample design	Random sampling
Data collection period	3 months
Data source	Primary and secondary

Section I: Demographic profile

Gender	Male	124	53.0
	Female	110	47.0
	Total	234	100.0
Age	Below 25	48	20.5
	25 -30	45	19.2
	35 – 40	46	19.7
	40 – 45	51	21.8
	Above 45	44	18.8
	Total	234	100.0

Occupation	Government sector	70	29.9
	Private sector	89	38.0
	Business	75	32.1
	Total	234	100.0
Monthly income	Below 25	47	20.1
	25 000 – 30,000	55	23.5
	30,000 – 35,000	49	20.9
	35,000 – 40,000	30	12.8
	Above 40,000	53	22.6
	Total	234	100.0

The table reveals that the demographic information about a sample of 234 respondents, categorized by gender, age, occupation, and monthly income. Below is an interpretation of each category:

- Gender Distribution, Male: 124 respondents (53.0%), Female: 110 respondents (47.0%), Total: 234 respondents (100.0%). The sample is fairly balanced in terms of gender, with a slight majority of male respondents.
- Age Distribution, Below 25 years: 48 respondents (20.5%), 25 – 30 years: 45 respondents (19.2%), 35 – 40 years: 46 respondents (19.7%), 40 – 45 years: 51 respondents (21.8%), Above 45 years: 44 respondents (18.8%), Total: 234 respondents (100.0%). The age distribution is relatively even, with no single age group dominating. The largest group is 40 – 45 years (21.8%), while the smallest is above 45 years (18.8%).
- Occupation Distribution, Government sector: 70 respondents (29.9%), Private sector: 89 respondents (38.0%), Business: 75 respondents (32.1%), Total: 234 respondents (100.0%). The largest group of respondents work in the private sector (38.0%), followed by business owners (32.1%), and government sector employees (29.9%). This suggests a good mix of employment backgrounds.
- Monthly Income Distribution, Below 25,000: 47 respondents (20.1%), 25,000 – 30,000: 55 respondents (23.5%), 30,000 – 35,000: 49 respondents (20.9%), 35,000 – 40,000: 30 respondents (12.8%), Above 40,000: 53 respondents (22.6%), Total: 234 respondents (100.0%). The highest proportion of respondents (23.5%) earn between 25,000 – 30,000, while 12.8% earn between 35,000 – 40,000, making it the smallest income group. The distribution suggests that most respondents fall within a middle-income range.

Musik in bayern
ISSN: 0937-583x Volume 90, Issue 3 (March -2025)
https://musikinbayern.com **DOI https://doi.org/10.15463/gfbm-mib-2025-391**

Section II: General Information & Cyber Warfare and Emerging Threats

How would you rate your knowledge of cyber warfare and cryptography?	Beginner	55	23.5
	Intermediate	67	28.6
	Advanced	57	24.4
	Expert	55	23.5
	Total	234	100.0
Do you believe cyber warfare is a greater threat in 2025 than in previous years?	Yes, significantly greater	59	25.2
	Somewhat greater	63	26.9
	About the same	55	23.5
	No, the threat has decreased	57	24.4
	Total	234	100.0
Which type of cyber-attacks do you think pose the greatest risk in modern cyber warfare?	Ransom ware attacks	57	24.4
	AI-powered cyber-attacks	43	18.4
	Nation-state-sponsored attacks	39	16.7
	Supply chain attacks	50	21.4
	Deep fake and misinformation campaigns	45	19.2
	Total	234	100.0
How effective do you think current cyber security measures are in defending against state-sponsored cyber warfare?	Very effective	51	21.8
	Somewhat effective	56	23.9
	Neutral	59	25.2
	Ineffective	68	29.1
	Total	234	100.0
What role do you think artificial intelligence (AI) plays in cyber warfare?	AI strengthens cyber defenses	55	23.5
	AI is used primarily for cyber-attacks	68	29.1
	AI has equal impact on both attack and defense	55	23.5
	AI has minimal impact on cyber warfare	56	23.9
	Total	234	100.0
Do you believe quantum computing will pose a significant threat to current encryption methods by 2030?	Yes, definitely	57	24.4
	Possibly, but not immediately	65	27.8
	Unlikely in the near future	54	23.1
	No, current encryption is sufficient	58	24.8
	Total	234	100.0

Knowledge of Cyber Warfare and Cryptography

- Beginner: 55 respondents (23.5%), Intermediate: 67 respondents (28.6%), Advanced: 57 respondents (24.4%), Expert: 55 respondents (23.5%), Total: 234 respondents (100.0%). The respondents have a relatively balanced distribution of cybersecurity knowledge, with most identifying as intermediate (28.6%) or advanced (24.4%). A

significant portion (23.5%) are at the expert level, indicating a knowledgeable sample base.

- **Cyber Warfare Threat Perception in 2025**

  Significantly greater: 59 respondents (25.2%), Somewhat greater: 63 respondents (26.9%), About the same: 55 respondents (23.5%), Decreased threat: 57 respondents (24.4%), Total: 234 respondents (100.0%). A majority (52.1%) believe cyber warfare threats in 2025 will be somewhat or significantly greater than in previous years. However, nearly half (47.9%) think the threat level is either unchanged or decreasing, showing a divided perception.

- **Most Concerning Cyber-Attacks in Modern Cyber Warfare**

  Ransomware attacks: 57 respondents (24.4%), AI-powered cyber-attacks: 43 respondents (18.4%), Nation-state-sponsored attacks: 39 respondents (16.7%), Supply chain attacks: 50 respondents (21.4%), Deepfake and misinformation campaigns: 45 respondents (19.2%), Total: 234 respondents (100.0%). The top concerns are ransomware attacks (24.4%) and supply chain attacks (21.4%), highlighting fears over financial and operational security risks. AI-powered attacks (18.4%) and deepfake misinformation (19.2%) are also significant concerns, indicating growing awareness of emerging threats.

- **Effectiveness of Current Cybersecurity Measures Against State-Sponsored Attacks**

  Very effective: 51 respondents (21.8%), Somewhat effective: 56 respondents (23.9%), Neutral: 59 respondents (25.2%), Ineffective: 68 respondents (29.1%), Total: 234 respondents (100.0%). A large portion (54.3%) of respondents are either neutral or believe cybersecurity measures are ineffective against state-sponsored cyber warfare. This suggests skepticism regarding current defense mechanisms and the need for stronger cybersecurity strategies.

- **Role of Artificial Intelligence (AI) in Cyber Warfare**

  AI strengthens cyber defenses: 55 respondents (23.5%), AI is primarily used for attacks: 68 respondents (29.1%), AI has equal impact on attack and defense: 55 respondents (23.5%), AI has minimal impact: 56 respondents (23.9%), Total: 234 respondents

(100.0%). The responses show mixed views on AI's role in cyber warfare. The largest group (29.1%) sees AI as mainly a tool for cyber-attacks, while others believe it equally affects both attack and defense (23.5%) or strengthens defenses (23.5%). A significant 23.9% think AI has minimal impact, indicating uncertainty about its role.

- **Threat of Quantum Computing to Encryption by 2030**

  Yes, definitely: 57 respondents (24.4%), Possibly, but not immediately: 65 respondents (27.8%), Unlikely in the near future: 54 respondents (23.1%), No, current encryption is sufficient: 58 respondents (24.8%), Total: 234 respondents (100.0%). There is no strong consensus on whether quantum computing will break encryption soon. The largest group (27.8%) believes it's a potential threat but not immediate, while 24.4% think it will definitely become a problem by 2030. Meanwhile, 47.9% believe quantum computing either won't be a major concern or that current encryption is sufficient.

Section III: The Future of Cryptography

Cryptographic advancements do you believe will have the biggest impact on cybersecurity in the next decade?	Post-quantum cryptography	56	23.9
	Block chain-based security	61	26.1
	Homomorphism encryption	60	25.6
	Biometric encryption	57	24.4
	Total	234	100.0
How urgent do you think it is for organizations to adopt post-quantum cryptographic methods?	Extremely urgent	57	24.4
	Somewhat urgent	52	22.2
	Not urgent	55	23.5
	Unnecessary	70	29.9
	Total	234	100.0
In your opinion, which sector is the most vulnerable to cyber warfare?	Government and military systems	49	20.9
	Financial institutions	59	25.2
	Healthcare and critical infrastructure	60	25.6
	Private corporations	66	28.2
	Total	234	100.0
What are the biggest challenges in implementing advanced cryptographic solutions?	High costs of implementation	73	31.2
	Complexity of integration into existing systems	56	23.9
	Lack of skilled professionals	62	26.5
	Resistance to change within organizations	43	18.4
	Total	234	100.0

Cryptographic Advancements with the Biggest Impact on Cybersecurity

Post-quantum cryptography: 56 respondents (23.9%), Blockchain-based security: 61 respondents (26.1%), Homomorphic encryption: 60 respondents (25.6%), Biometric encryption: 57 respondents (24.4%), Total: 234 respondents (100.0%). There is no clear dominance of any single cryptographic advancement, as respondents believe multiple technologies will play a major role. Blockchain-based security (26.1%) is seen as the most impactful, likely due to its potential for decentralized, tamper-proof security. Homomorphic encryption (25.6%) follows closely, reflecting its promise in securing data during computation. Biometric encryption (24.4%) is also considered significant, highlighting the importance of identity-based security solutions. Post-quantum cryptography (23.9%) is viewed as critical, particularly as quantum computing threats grow.

- **Urgency of Adopting Post-Quantum Cryptographic Methods**

  Extremely urgent: 57 respondents (24.4%), Somewhat urgent: 52 respondents (22.2%), Not urgent: 55 respondents (23.5%), Unnecessary: 70 respondents (29.9%), Total: 234 respondents (100.0%). Opinions on the urgency of adopting post-quantum cryptography are divided. While 46.6% (extremely + somewhat urgent) see an immediate need for adoption, 53.4% (not urgent + unnecessary) believe it is not an immediate priority. The largest group (29.9%) sees it as unnecessary, possibly due to scepticism about the near-term impact of quantum computing. Most Vulnerable Sectors to Cyber Warfare

  Government and military systems: 49 respondents (20.9%), Financial institutions: 59 respondents (25.2%), Healthcare and critical infrastructure: 60 respondents (25.6%), Private corporations: 66 respondents (28.2%), Total: 234 respondents (100.0%). Private corporations (28.2%) are seen as the most vulnerable, likely due to frequent attacks on businesses and growing data breaches. Healthcare and critical infrastructure (25.6%) follow closely, emphasizing the risks to essential services like hospitals and energy grids. Financial institutions (25.2%) are also considered at risk, likely due to frequent banking cyber threats and fraud. Government and military systems (20.9%) are viewed as relatively less vulnerable, though still a significant target.

- **Biggest Challenges in Implementing Advanced Cryptographic Solutions**

High costs of implementation: 73 respondents (31.2%), Complexity of integration into existing systems: 56 respondents (23.9%), Lack of skilled professionals: 62 respondents (26.5%), Resistance to change within organizations: 43 respondents (18.4%), Total: 234 respondents (100.0%). High costs (31.2%) are seen as the biggest barrier, indicating financial concerns in adopting advanced cryptographic measures. Lack of skilled professionals (26.5%) is the second-largest challenge, showing a demand for more trained cybersecurity experts. Complexity of integration (23.9%) highlights technical difficulties in updating existing cybersecurity systems. Resistance to change (18.4%) is the least concerning, but still suggests that some organizations are reluctant to adopt new technologies.

Section IV: Future Cyber security Strategies

How do you think international regulations can help prevent cyber warfare?	Strong international agreements and treaties	62	26.5
	Global cooperation on cyber threat intelligence	51	21.8
	Development of universal cyber security laws	62	26.5
	Other (Please specify)	59	25.2
	Total	234	100.0
What strategies should organizations prioritize to defend against cyber warfare?	AI-based threat detection systems	48	20.5
	Zero-trust security architecture	51	21.8
	Regular security audits and vulnerability assessments	60	25.6
	Quantum-resistant encryption adoption	37	15.8
	Training employees on cyber security awareness	38	16.2
	Total	234	100.0
How do you perceive the role of ethical hacking in preventing cyber-attacks?	Extremely important	59	25.2
	Somewhat important	59	25.2
	Neutral	55	23.5
	Not important	61	26.1
	Total	234	100.0
Would you support government-mandated encryption policies to	Yes, national security should take priority	77	32.9
	A balanced approach is needed	64	27.4

protect national security, even at the cost of individual privacy?	No, individual privacy should not be compromised	48	20.5
	Not sure	45	19.2
	Total	234	100.0

- **The Role of International Regulations in Preventing Cyber Warfare**

  Strong international agreements and treaties: 62 respondents (26.5%), Global cooperation on cyber threat intelligence: 51 respondents (21.8%), Development of universal cybersecurity laws: 62 respondents (26.5%), Other (Please specify): 59 respondents (25.2%), Total: 234 respondents (100.0%). Respondents equally support (26.5%) both strong international agreements and universal cybersecurity laws, indicating a demand for formalized, enforceable global frameworks. Global cooperation on cyber threat intelligence (21.8%) is also a priority, showing interest in proactive information sharing. A notable 25.2% chose "Other," suggesting diverse opinions on alternative approaches to regulation.

- **Prioritized Strategies for Organizations to Defend Against Cyber Warfare**

  AI-based threat detection systems: 48 respondents (20.5%), Zero-trust security architecture: 51 respondents (21.8%), Regular security audits and vulnerability assessments: 60 respondents (25.6%), Quantum-resistant encryption adoption: 37 respondents (15.8%), Training employees on cybersecurity awareness: 38 respondents (16.2%), Total: 234 respondents (100.0%). Regular security audits and vulnerability assessments (25.6%) are the top priority, showing a focus on proactive threat detection. Zero-trust security (21.8%) and AI-based threat detection (20.5%) are also key, reflecting growing concerns over network trust models and AI-driven cyber threats. Quantum-resistant encryption (15.8%) is the lowest priority, likely because many do not yet perceive quantum computing as an immediate threat. Cybersecurity awareness training (16.2%) ranks low, indicating a potential underestimation of the human factor in security breaches.

- **Role of Ethical Hacking in Preventing Cyber-Attacks**

  Extremely important: 59 respondents (25.2%), Somewhat important: 59 respondents (25.2%), Neutral: 55 respondents (23.5%), Not important: 61 respondents (26.1%), Total: 234 respondents (100.0%). 50.4% (extremely + somewhat important) see ethical

hacking as an essential cybersecurity tool. However, a significant 26.1% believe it is not important, possibly due to skepticism about its effectiveness or ethical concerns. 23.5% remain neutral, indicating uncertainty or lack of awareness about ethical hacking's impact.

- **Support for Government-Mandated Encryption Policies at the Cost of Privacy**

Yes, national security should take priority: 77 respondents (32.9%), A balanced approach is needed: 64 respondents (27.4%), No, individual privacy should not be compromised: 48 respondents (20.5%), Not sure: 45 respondents (19.2%), Total: 234 respondents (100.0%). A majority (60.3%) support either prioritizing national security (32.9%) or a balanced approach (27.4%), indicating recognition of cybersecurity as a national concern. 20.5% oppose any compromise on individual privacy, reflecting concerns about government overreach and surveillance. 19.2% are uncertain, suggesting a lack of clear public consensus on how encryption should be regulated.

II. Factor Analysis

A. KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.856
Bartlett's Test of Sphericity	Approx. Chi-Square	73.588
	df	91
	Sig.	.000

1. **Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy: 0.856**

- ✓ Interpretation: The KMO statistic tests whether the data is suitable for factor analysis. It ranges from 0 to 1, where values closer to 1 indicate that factor analysis is appropriate.
- ✓ KMO value of 0.856 is considered very good (values above 0.8 are considered excellent). This suggests that the data is appropriate for factor analysis and that the variables are sufficiently related to each other.

2. **Bartlett's Test of Sphericity**

- ✓ Approx. Chi-Square: 73.588

- ✓ df (degrees of freedom): 91
- ✓ Sig. (Significance): 0.000
- ✓ Interpretation: Bartlett's Test tests the null hypothesis that the correlation matrix is an identity matrix (meaning that the variables are not correlated). A significant result (p-value < 0.05) indicates that the correlation matrix is not an identity matrix, which means the variables are correlated and factor analysis can be performed.
- ✓ In this case, the p-value is 0.000, which is well below the typical significance level of 0.05, indicating that the correlation matrix is not an identity matrix and that factor analysis is appropriate for the data.

III. Cyber Warfare Perception How concerned about the increasing role of cyber warfare in global conflicts?

Factor 1 Cyber warfare & Global conflicts

Variable	Variables	Factor Loading Value
1	Current cybersecurity strategies are in preventing cyber warfare attacks	(.875)
2	AI will become the dominant tool for both cyber-attacks and cyber defense by 2030	(.862)
3	Cyber warfare is a more significant threat than traditional military warfare in 2025	(.752)
4	Governments are to counter large-scale cyber warfare threats	(.684)

1. **Effectiveness of Current Cybersecurity Strategies (.875)**
    - This variable has the highest factor loading, indicating that the effectiveness of current cybersecurity strategies is the most significant aspect of cyber warfare and global conflicts. It suggests that strong cybersecurity measures are critical in preventing cyber threats.
2. **AI as a Dominant Tool in Cyber Warfare by 2030 (.862)**
    - This variable also has a strong association with the factor, implying that AI is expected to play a crucial role in both launching and defending against cyber-attacks in the near future. The high loading suggests that experts widely anticipate AI-driven cyber warfare.
3. **Cyber Warfare vs. Traditional Military Threats (.752)**

- With a moderately high loading, this variable indicates that cyber warfare is perceived as a greater threat than traditional military warfare in 2025. While not as strongly linked as the first two variables, it still contributes significantly to the overall factor.

4. **Government Preparedness for Large-Scale Cyber Threats (.684)**

   - This variable has the lowest factor loading, suggesting that while government preparedness is relevant, it is less central to the concept of cyber warfare and global conflicts compared to the effectiveness of cybersecurity strategies and AI dominance.

Factor 2 Cyber security Measures and Cryptography

Variable	Variables	Factor Loading Value
1	post-quantum cryptography in ensuring future cybersecurity	(.843)
2	The security of current encryption methods against advanced cyber threats	(.812)
3	quantum computing will break widely used encryption methods within the next decade	(.726)
4	block chain technology is in enhancing cyber security	(.642)
5	Ethical hacking is strengthening cyber security against cyber warfare	(.524)

1. **Post-Quantum Cryptography and Future Cybersecurity (.843)**

   - This variable has the highest factor loading, indicating that post-quantum cryptography is the most critical aspect of cybersecurity measures. It suggests that ensuring cybersecurity in the future will heavily depend on the development and adoption of encryption methods resistant to quantum computing threats.

2. **Security of Current Encryption Methods Against Advanced Cyber Threats (.812)**

   - This variable is also strongly associated with the factor, emphasizing the importance of evaluating and improving existing encryption techniques to withstand evolving cyber threats. It highlights the growing concerns about whether current encryption remains effective.

3. **Quantum Computing Breaking Current Encryption Methods Within a Decade (.726)**
    - With a moderately high loading, this variable suggests that there is significant concern about quantum computing rendering current encryption methods obsolete. This further underscores the importance of post-quantum cryptography.
4. **Blockchain Technology in Enhancing Cybersecurity (.642)**
    - This variable indicates that blockchain technology is recognized as a cybersecurity tool, though it has a weaker association compared to encryption and quantum computing. Blockchain is considered valuable for security applications, but its role is less central than cryptography.
5. **Ethical Hacking in Strengthening Cybersecurity Against Cyber Warfare (.524)**
    - Ethical hacking has the weakest loading in this factor, indicating that while it is relevant to cybersecurity measures, it is not as strongly linked as encryption, quantum computing, or blockchain. However, it still plays a role in strengthening security defenses.

Factor 3 Cyber security Strategies and Regulations

Variable	Variables	Factor Loading Value
1	Global cooperation is necessary to prevent cyber warfare	(.724)
2	Government policies are in ensuring cyber security and encryption standards	(.642)
3	AI-based threat detection in protecting critical infrastructure from cyber threats	(.562)
4	Sacrifice some level of personal privacy in exchange for stronger national cyber security	(.518)
5	Educating individuals and businesses about cyber security awareness	(.512)

Global Cooperation to Prevent Cyber Warfare (.724)

- This variable has the highest factor loading, indicating that international collaboration is seen as the most critical aspect of cybersecurity strategies and regulations. It highlights the growing need for countries to work together to mitigate cyber threats.

Government Policies Ensuring Cybersecurity and Encryption Standards (.642)

- This variable is also strongly linked to the factor, emphasizing the role of government regulations in maintaining cybersecurity. It suggests that clear policies and encryption standards are essential to national and global security.

AI-Based Threat Detection for Critical Infrastructure (.562)

- AI's role in cybersecurity is moderately associated with this factor, indicating that AI-driven threat detection is considered an important strategy for protecting vital systems from cyber threats. However, it is slightly less central than government policies and international cooperation.

Sacrificing Personal Privacy for National Cybersecurity (.518)

- This variable suggests a trade-off between privacy and security, with some belief that reducing personal privacy could enhance national cybersecurity. While relevant, it has a weaker association compared to global cooperation and government policies.

Educating Individuals and Businesses on Cybersecurity Awareness (.512)

- This variable has the lowest factor loading in this factor, indicating that while cybersecurity awareness is important, it is less central to cybersecurity strategies and regulations compared to global and governmental initiatives. However, education still plays a role in enhancing overall cybersecurity.

Major findings of the study

- Gender: Slightly more males (53%) than females (47%), Age: Fairly even distribution across age groups, with the largest group being 40–45 years (21.8%), Occupation: Most respondents work in the private sector (38%), followed by business owners and government employees, Income: The majority earn between 25,000 – 30,000 (23.5%), with fewer respondents in the 35,000 – 40,000 category.

- Knowledge levels: A well-balanced mix of cybersecurity awareness, with many respondents having intermediate to expert knowledge. Perception of cyber threats: While a majority (52.1%) think cyber warfare threats are increasing, a significant

portion believe the threat level is unchanged or decreasing. Cyber-attack concerns: Ransomware and supply chain attacks are seen as the biggest threats, with growing concerns about AI-powered attacks and misinformation campaigns. Cybersecurity effectiveness: 54.3% express doubts about the effectiveness of current cybersecurity measures against state-sponsored attacks. AI's role: Mixed opinions, but a majority see AI as either aiding attacks (29.1%) or having an equal impact on both attack and defense (23.5%). Quantum computing risks: No clear consensus, with opinions split between those who see it as a near-term threat and those who believe existing encryption is adequate.

- No single cryptographic technology dominates future cybersecurity, but blockchain, homomorphic encryption, biometrics, and post-quantum cryptography are all seen as highly impactful. The urgency of adopting post-quantum cryptography is debated, with nearly half seeing it as necessary, while others believe it is not urgent or even unnecessary. Private corporations (28.2%), healthcare (25.6%), and financial institutions (25.2%) are seen as more vulnerable to cyber warfare than government systems. High costs (31.2%) and lack of skilled professionals (26.5%) are the biggest obstacles to implementing advanced cryptographic solutions.

- International cybersecurity regulations are widely supported, with strong treaties and universal laws seen as crucial. Regular security audits (25.6%) and zero-trust models (21.8%) are the most preferred cybersecurity strategies, while quantum-resistant encryption (15.8%) is a lower priority. Views on ethical hacking are divided, with 50.4% supporting it but 26.1% dismissing its importance. 60.3% favour government-mandated encryption policies for national security, but privacy concerns remain significant (20.5%).

- The 1st Factor Cyber Warfare & Global Conflicts is primarily influenced by the effectiveness of cybersecurity strategies and the growing role of AI in cyber warfare. The perception that cyber threats may surpass traditional military threats is also significant, though slightly less so. Government readiness, while still relevant, has the weakest association within this factor. The high factor loadings suggest that these issues are tightly interconnected, with AI and cybersecurity strategies shaping the future landscape of global security threats.

- The 2nd Factor Cybersecurity Measures and Cryptography is primarily driven by concerns over encryption security and the impact of quantum computing. Post-quantum cryptography is seen as the most crucial element in securing future cybersecurity, followed closely by the security of current encryption methods. The potential threat of quantum computing to encryption is also significant. Blockchain technology and ethical hacking contribute to cybersecurity but are less central to this factor. The findings suggest that future cybersecurity efforts should focus heavily on cryptographic advancements to stay ahead of emerging threats.
- The 3rd Factor Cybersecurity Strategies and Regulations is primarily driven by the need for global cooperation and strong government policies to establish effective cybersecurity defenses. AI-based threat detection also plays a role in protecting critical infrastructure, but it is not as dominant. The debate between privacy and security, along with cybersecurity education, are relevant but have a weaker association with the core theme of strategies and regulations. This suggests that cybersecurity governance should focus on international collaboration and policy enforcement while balancing technological advancements and privacy concerns.

Conclusion

Cyber warfare has rapidly evolved into a significant global threat, driven by advancements in artificial intelligence (AI), quantum computing, and state-sponsored cyber operations. As cyber-attacks become more sophisticated, traditional cybersecurity measures may no longer be sufficient to protect critical infrastructure, financial systems, and national security. This study examined the key trends shaping cyber warfare in 2025, focusing on the rise of AI-powered cyber-attacks, the challenges posed by quantum computing, and the effectiveness of cybersecurity strategies.

Findings indicate that AI plays a dual role in cyber warfare, being used both to enhance cyber defenses and to launch more efficient attacks. Quantum computing, while still in its early stages, is expected to break widely used encryption methods, making the transition to post-quantum cryptography (PQC) an urgent necessity. The study also

highlights the importance of zero-trust security models, ethical hacking, and global cooperation in strengthening cybersecurity resilience.

Furthermore, the research underscores the growing debate between national security and individual privacy, with government-mandated encryption policies being viewed as both a necessary security measure and a potential threat to civil liberties. The effectiveness of international agreements, such as the Budapest Convention on Cybercrime, remains uncertain due to geopolitical tensions and a lack of universal enforcement mechanisms.

Recommendations for Future Research

1. AI-driven threat detection systems and their role in cyber defines.
2. Implementation challenges of post-quantum cryptographic methods in real-world cybersecurity applications.
3. The effectiveness of international cyber warfare treaties in mitigating large-scale attacks.
4. The ethical and legal implications of government surveillance and encryption policies.

References

- Brundage, M., Avin, S., Clark, J., et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *arXiv preprint arXiv:1802.07228*.
- Evans, D., & Lindqvist, U. (2019). Future Cybersecurity Challenges and Research Directions. *Communications of the ACM, 62(6), 23-25*.
- Kindervag, J. (2010). No More Chewy Centers: Introducing the Zero Trust Model of Information Security. *Forrester Research Report*.
- Kostyuk, N., & Zhukov, Y. M. (2019). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution, 63(2), 317-347*.
- Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy, 16(5), 38-41*.
- NIST (2022). Post-Quantum Cryptography Standardization. *National Institute of Standards and Technology Report*.

- Papernot, N., McDaniel, P., Jha, S., et al. (2017). The Limitations of Deep Learning in Adversarial Settings. *IEEE European Symposium on Security and Privacy*.
- Sharma, A., Tiwari, B., & Kumar, S. (2021). AI and Cybersecurity: Role of Machine Learning in Threat Detection. *Springer Lecture Notes in Computer Science, 12563, 241-258*.
- Sitt, S., & Pahi, S. (2022). The Rise of Ransomware-as-a-Service: Implications for Cybersecurity. *Cyber Defense Journal, 14(3), 91-105*.
- Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. *Oxford University Press*.
- Tikk-Ringas, E. (2020). The Role of International Law in Cybersecurity Governance. *Journal of Cyber Policy, 5(2), 162-178*.