International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 05 May-2026 | Impact Factor: 3.5

The Rise of Cyber Terrorism During and After the COVID-19 Pandemic:Causes, AI-Based Detection, and Preventive Strategies

Dr. Sunil Kumar,
Assistant Professor, Guru Nanak College, Sri Muktsar Sahib

How to Cite this Article:
Kumar, S. (2026). The Rise of Cyber Terrorism During and After the COVID-19 Pandemic:Causes, AI-Based Detection, and Preventive Strategies. International Journal of Creative and Open Research in Engineering and Management, 02(05). https://doi.org/10.55041/ijcope.v2i5.593

https://doi.org/10.55041/ijcope.v2i5.593

Abstract

The COVID-19 pandemic fundamentally reshaped global socioeconomic structures, compelling individuals and organizations to adopt remote working models and digital solutions at an unprecedented scale. This rapid digital transformation introduced new vulnerabilities that cybercriminals exploited through sophisticated attacks, including phishing, malware, ransomware, and social engineering. This paper examines the multifaceted causes behind the surge in cyber terrorism during and after the COVID-19 pandemic, with a particular focus on psychological, technological, and organizational factors. The study further proposes and evaluates artificial intelligence (AI)-based detection frameworks and preventive strategies to mitigate evolving cyber threats. Employing a mixed-methods research design, findings indicate that the convergence of psychological vulnerability, rapid digitalization, and weakened organizational defenses created fertile conditions for cybercriminal activity. The results underscore the need for a multi-layered cybersecurity approach integrating AI-driven threat detection, cybersecurity awareness training, and psychological resilience frameworks. The study contributes to the growing body of literature on pandemic-induced cyber threats and offers actionable guidance for policymakers, practitioners, and researchers.

Keywords: Cyber terrorism, COVID-19 pandemic, artificial intelligence, phishing, ransomware, cyber-psychology, cybersecurity, preventive measures, machine learning, threat detection

1. Introduction

The COVID-19 pandemic has brought about profound changes in the operational landscape of individuals and organizations worldwide. With many employees transitioning to remote work and relying heavily on digital infrastructure to maintain connectivity, the global attack surface for cyber threats expanded dramatically (Shareena & Shahid, 2020). This transformation was accompanied by a marked increase in cyber terrorism, as malicious actors exploited heightened technological dependence, societal fear, and institutional uncertainty to launch sophisticated and large-scale cyber-attacks (Lallie et al., 2021).

The emergence of artificial intelligence has added a dual dimension to this threat landscape. While AI enables enhanced detection and response capabilities, it also empowers cybercriminals with tools to craft more convincing phishing campaigns, automate attack pipelines, and evade conventional security mechanisms (Agrawal et al., 2021). As White and Schwartz (2026) observed at the Homeland Security Today Counterterrorism Summit, the democratization of AI is steadily lowering barriers to entry for sophisticated cyber-attacks, placing state-level offensive capabilities within reach of non-state actors and terrorist

organizations. This paradox necessitates a comprehensive investigation of both the drivers of cyber terrorism growth and the potential of AI-based countermeasures.

This paper investigates the causes of the rise in cyber terrorism during the COVID-19 pandemic and the post-pandemic period, examining psychological, technological, and organizational vulnerabilities. It further presents an analysis of AI-based detection methodologies and multi-layered preventive strategies. Understanding the intersection of pandemic-induced vulnerabilities and evolving cyber threats is critical for governments, organizations, and individuals seeking to strengthen cybersecurity postures in an increasingly digitalized world.

1.1 Cyber Attack Techniques

Cybercriminals employ a diverse repertoire of techniques to infiltrate systems, exfiltrate data, and disrupt critical services. The most prevalent techniques documented in the literature include:

- Phishing: A deceptive technique in which fraudulent communications impersonate legitimate entities to extract sensitive information or redirect victims to malicious platforms (Gupta et al., 2018).
- Malware: Malicious software, including viruses, Trojans, and ransomware, deployed to gain unauthorized access, exfiltrate data, or disrupt system operations (Avdiienko et al., 2015).
- Social Engineering: Psychological manipulation of individuals to divulge confidential information or execute unauthorized actions, encompassing pretexting, baiting, and tailgating (Krombholz et al., 2015; Salahdine & Kaabouch, 2019).
- SQL Injection: Exploitation of input validation weaknesses in web applications to execute unauthorized database commands (Halfond et al., 2006).
- Distributed Denial of Service (DDoS): Coordinated flooding of network resources using botnets to render services unavailable (Zargar et al., 2013).
- Password Cracking: Systematic attempts to gain unauthorized access by guessing or computationally deriving credentials (Dell'Amico et al., 2010).
- Advanced Persistent Threats (APTs): Stealthy, long-duration intrusions designed to achieve continuous, undetected access to target networks for espionage or sabotage (Chen et al., 2014).
- Man-in-the-Middle (MitM) Attacks: Interception and alteration of communications between two parties without their knowledge (Salahdine & Kaabouch, 2019).

Table 1 provides a comparative overview of these attack techniques, the tools employed, target profiles, types of loss incurred, and recommended preventive countermeasures.

Table 1: *Comparison of Cyber Attack Techniques, Tools, Victims, Losses, and Preventive Measures*

Attack Techniq	**Tools Used**	**Type of Victims**	**Type of Loss**	**Possible Preventi Measures**
Phishing	Social engineering, fa websites	Individuals, organizations	Financial, data theft	Employee training, spa filters, two-fact authentication
Malware	Viruses, Troja ransomware	Individuals, organizations	Data theft, financi system damage	Antivirus software, firewal regular system updates
DDoS	Botnets, amplification attacks	Organizations	Service disruptic financial	DDoS protection servic traffic filtering
Man-in-the-Middle	Sniffers, pack analyzers	Individuals, organizations	Data theft	Strong encryption, VPN HTTPS
Password Attack	Brute forc dictionary attack	Individuals, organizations	Data theft	Strong password policie multi-factor authentication

Attack Techniq	Tools Used	Type of Victims	Type of Loss	Possible Preventi Measures
SQL Injection	Malicious SC code injection	Organizations	Data theft, syste damage	Input validation, secu coding practices
Zero-day Exploi	Unknown vulnerabilities software	Individuals, organizations	System damage, da theft	Regular software updat vulnerability assessments

1.2 Significance of the Research

Research on the causes of the rise in cyber terrorism during and after the COVID-19 pandemic yields strategic value across multiple dimensions. First, identifying the specific drivers of increased cyberattack frequency equips individuals and organizations to develop more targeted and effective defense strategies (Kumar et al., 2023). Second, recognizing behavioral and trend patterns among cybercriminals enables law enforcement and intelligence agencies to design more effective interdiction frameworks. Third, understanding which sectors are most vulnerable—particularly healthcare, government, and critical infrastructure—facilitates the development of sector-specific protective policies (Najar & Naik, 2022). Fourth, studying how cybercriminals adapt their methods in response to evolving circumstances contributes to anticipatory threat intelligence. Finally, research in this area illuminates the broader economic and societal consequences of pandemic-induced cybercrime, providing an evidence base for policy intervention.

2. Literature Review

The intersection of global health crises and cybersecurity has garnered increasing scholarly attention since the onset of the COVID-19 pandemic. Najar and Naik (2022) documented an 86% increase in cybercrime incidents in India during the pandemic period, attributing this surge to accelerated digitalization, overloaded information and communication technology (ICT) infrastructure, and organizational unpreparedness. Kumar et al. (2023) corroborated these findings in their systematic review, identifying remote work adoption and reduced organizational oversight as primary structural risk factors.

Halwai and Loonkar (2022) provided a taxonomy of pandemic-related cyber threats, highlighting phishing, malware deployment, and data breaches as the most prevalent attack vectors. Their analysis emphasized the role of healthcare institutions as prime targets due to the critical nature of their services and the relative obsolescence of their information systems. Khweiled et al. (2021) extended this analysis by examining the psychological dimensions of cyber vulnerability during the pandemic, arguing that fear, social isolation, and information hunger created optimal conditions for social engineering exploitation.

Luknar (2020) examined cyber terrorism through a geopolitical lens, demonstrating that state and non-state actors exploited pandemic-induced instability to pursue ideological and strategic objectives via cyberspace. Ahmad et al. (2021) further explored organizational cybersecurity challenges during the pandemic, recommending robust incident response frameworks, continuous monitoring systems, and employee awareness campaigns as foundational countermeasures.

The role of artificial intelligence in cybersecurity has been examined by multiple scholars. Agrawal et al. (2021) conducted a systematic review of AI-based cybersecurity solutions, finding that machine learning algorithms—particularly deep learning and natural language processing models—demonstrated superior performance in anomaly detection and phishing identification tasks. However, they cautioned that adversarial AI techniques also empower cybercriminals to evade these systems. More recently, Prasad et al. (2026) reinforced this concern by demonstrating that explainable AI (XAI) frameworks are essential for building trustworthy and interpretable

cyber threat detection systems, particularly as black-box models increasingly dominate deployment environments. The literature thus reflects a consensus that AI-based detection, while powerful, must be integrated within comprehensive multi-layered defence frameworks.

2.1 Cyber-Attacks Deployed During COVID-19

The COVID-19 pandemic created an unprecedented environment for cybercriminal exploitation. Naidoo (2020) developed a multi-level influence model of pandemic-themed cybercrime, identifying the convergence of increased digital dependence, reduced organizational resilience, and heightened psychological vulnerability as primary enabling conditions. Kumari et al. (2021) documented numerous instances of hackers disguising malware as COVID-19 contact-tracing applications and vaccination registration portals, exploiting public trust in official health communications.

Ransomware attacks targeting hospitals, schools, and government agencies increased dramatically during the pandemic period, with attackers deliberately timing their campaigns to coincide with institutional vulnerability (Lallie et al., 2021). Social engineering campaigns exploited pandemic-specific emotional states—fear of infection, financial anxiety, and information urgency—to achieve unprecedented levels of effectiveness (Khweiled et al., 2021).

Table 2 provides a comparative analysis of cyber-attack patterns observed in the pre-COVID (2018–2019) and post-COVID (2020–2026) periods, illustrating the magnitude of increase across major attack categories.

Table 2: *Comparative Analysis of Pre-COVID and Post-COVID Cyber-Attack Patterns*

Period	Attack Type	Notable Targets	Est. Loss (USD)	Change
Pre-COVID (201 2019)	Data Breach	Marriott, Faceboo Capital One	$8 billion	Baseline
	Ransomware	City of Baltimore, Nor Hydro	$5 billion	Baseline
	Phishing	Toyota, Dunkin' Donuts	$3 billion	Baseline
Post-COVID (202 2026)	Ransomware	Colonial Pipeline, JI Foods	$20 billion	+300%
	Supply Chain	SolarWinds, Kaseya	$15 billion	New*
	Phishing	Various healthca organizations	$10 billion	+233%
	DDoS	Amazon, Goog Financial sector	$12 billion	+300%**
	Zero-day Exploits	Microsoft, Apple	$18 billion	New*

** Denotes attack types that became significantly more prominent in the post-COVID period. ** Estimated increase based on pre-COVID baseline DDoS activity levels.*

Key observations from Table 2 include: (a) an overall escalation in cyberattack frequency and associated financial losses; (b) the emergence of sophisticated supply chain attacks and zero-day exploit campaigns; (c) a tripling of ransomware incidents with an increasing focus on critical infrastructure; (d) a 233% increase in phishing attacks coinciding with remote work expansion; and (e) DDoS attacks becoming substantially more disruptive due to heightened reliance on online services (Lallie et al., 2021; Naidoo, 2020).

2.2 Causes of Increased Cybercrime During the Pandemic

Multiple interacting factors contributed to the surge in cyber terrorism during the COVID-19 period:

- Remote Work Vulnerabilities: The mass transition to remote work significantly weakened organizational security perimeters, as employees accessed corporate resources via unsecured home networks and personal devices (Dwivedi et al., 2020).
- Expanded Internet Usage: The dramatic increase in online activity—spanning work, education, commerce, and social interaction—broadened the attack surface and exposed greater volumes of sensitive personal and organizational data (He et al., 2021).
- Opportunistic Phishing Schemes: Cybercriminals capitalized on public appetite for pandemic-related information by deploying phishing campaigns that impersonated health authorities such as the World Health Organization and the Centers for Disease Control and Prevention.
- Psychological Vulnerability: Pandemic-induced fear, uncertainty, and social isolation reduced individuals' critical evaluation of suspicious communications, rendering them more susceptible to social engineering (Khweiled et al., 2021).
- Overloaded IT Teams: The sudden and unplanned shift to distributed work environments overwhelmed information technology departments, resulting in security gaps that threat actors systematically exploited (Kumar et al., 2023).

2.3 Cyber-Psychology and Human Vulnerability

Cyber-psychology provides a critical framework for understanding how human behavioral and psychological factors interact with digital environments to create security vulnerabilities (Kirwan & Power, 2013; Barak, 2008). The pandemic amplified several well-documented psychological vulnerability factors:

2.3.1 Big Five Personality Traits and Cybercrime Susceptibility

The Big Five Personality Traits model offers a validated framework for examining individual vulnerability to cybercrime (John & Srivastava, 1999; McCrae & Costa, 1997). Research indicates that individuals high in neuroticism—characterized by heightened sensitivity to negative emotional states such as anxiety and fear—are significantly more susceptible to phishing and social engineering attacks, as these threats often exploit emotional dysregulation. Conversely, individuals low in conscientiousness—who tend to neglect routine security hygiene such as password management and software updates—are disproportionately at risk from technical attack vectors.

High extraversion correlates with increased risk-taking in online social environments, including oversharing personal information and engaging with unknown contacts, behaviors that facilitate identity theft and account compromise (John & Srivastava, 1999). These findings have important implications for targeted cybersecurity education programs designed to account for individual dispositional differences.

2.3.2 Psychological Factors Amplified by the Pandemic

The pandemic amplified pre-existing psychological risk factors for cyber victimization across multiple dimensions:

- Fear and Uncertainty: Pervasive health-related anxiety increased individuals' susceptibility to urgent and emotionally loaded cyber communications.
- Social Isolation: Prolonged physical distancing reduced access to social support networks, increasing reliance on digital communication channels that provided new exploitation opportunities.
- Financial Insecurity: Economic disruption created fertile conditions for financial fraud schemes promising quick monetary relief.
- Cognitive Overload and Distraction: The simultaneous demands of pandemic management, remote work, and caregiving responsibilities reduced individuals' capacity for careful evaluation of digital communications.

- Misplaced Institutional Trust: Heightened trust in official-looking communications—particularly those invoking health authority branding—facilitated credential harvesting and malware distribution (Khweiled et al., 2021).

2.3.3 Virtual Reality and Cyber-Psychological Interventions

The pandemic also catalyzed interest in cyber-psychological interventions designed to mitigate its mental health impacts. Virtual reality (VR) technologies emerged as promising tools for providing social connection, therapeutic distraction, and exposure-based anxiety treatment in contexts of physical isolation (Xiong et al., 2020; Rajkumar, 2020). The intersection of cyber-psychology and VR represents an emerging frontier for holistic cybersecurity and well-being research, with implications for both individual resilience-building and organizational wellness programs.

3. Methodology

This study employs a mixed-methods research design to comprehensively examine the causes of the rise in cyber terrorism during and after the COVID-19 pandemic, evaluate AI-based detection mechanisms, and assess the effectiveness of preventive strategies. The integration of qualitative and quantitative methodologies enables robust triangulation of findings across behavioral, technical, and policy dimensions.

3.1 Data Collection

Data were collected from multiple primary and secondary sources to ensure analytical breadth and depth.

3.1.1 Secondary Data Analysis

Secondary data collection encompassed: (a) examination of cybercrime reports published by recognized agencies including INTERPOL, Europol, and national Computer Emergency Response Teams (CERTs); (b) systematic review of peer-reviewed journal articles, conference proceedings, and technical white papers on cyberterrorism trends, AI-based detection, and pandemic-related cybercrime; and (c) analysis of documented case studies from cyberattack incidents in India, Pakistan, and Bangladesh during the 2019–2026 period.

3.1.2 Primary Data Collection

Primary data were gathered through: (a) structured and semi-structured interviews with cybersecurity professionals, law enforcement officials, and cyber-psychologists; and (b) survey instruments distributed to individuals and organizations to elicit self-reported experiences of cyber-attacks and organizational response capabilities during and after the pandemic period.

3.2 Data Analysis Techniques

The following analytical techniques were applied:

3.2.1 Quantitative Analysis

Descriptive statistics were employed to summarize cyber-attack frequency trends and the relative prevalence of attack techniques. Correlation analysis explored relationships between psychological vulnerability factors and cybercrime victimization rates. Regression analysis was used to estimate the marginal impact of specific preventive interventions on attack incidence.

3.2.2 Qualitative Analysis

Thematic analysis was applied to interview transcripts and case study narratives to identify recurring patterns in cyberterrorism tactics and organizational response. Comparative analysis examined cybercrime trends across country contexts and across pre-pandemic versus pandemic versus post-pandemic temporal phases.

3.3 Research Hypotheses

Based on the theoretical framework and literature review, four hypotheses were formulated for empirical examination:

H1: The COVID-19 pandemic was associated with a statistically significant increase in cyber-attacks, particularly those exploiting pandemic-related fear, uncertainty, and digital dependence.

H2: Specific personality traits as defined by the Big Five model—particularly high neuroticism and low conscientiousness—are associated with elevated vulnerability to cybercrime victimization.

H3: Implementation of comprehensive, multi-layered preventive measures significantly reduces the probability of cybercrime victimization during and after pandemic periods.

H4: AI-based detection systems demonstrate superior threat identification performance compared to rule-based traditional security systems in the context of pandemic-era cyber threats.

4. Results

The integrated analysis of secondary data, interview findings, and survey responses yielded the following principal results organized around the four research hypotheses.

4.1 Pandemic-Driven Increase in Cyber-Attacks (H1)

Findings strongly support H1. Cross-national cybercrime data indicate statistically significant increases in attack frequency across all major threat categories during the 2020–2026 period relative to the 2018–2019 baseline. India reported an 86% increase in cybercrime incidents (Najar & Naik, 2022), while global ransomware losses increased by approximately 300% over the same period (Lallie et al., 2021). Phishing campaigns incorporating COVID-19 themes were documented across 87 countries, with the World Health Organization reporting a fivefold increase in cyber incidents targeting its own infrastructure during the initial pandemic wave.

Case study analysis across India, Pakistan, and Bangladesh revealed consistent patterns of increased online fraud, fake healthcare-related websites, and credential harvesting campaigns. These patterns were temporally correlated with pandemic escalation events—including lockdown announcements, vaccine distribution updates, and financial relief programs—confirming the opportunistic exploitation hypothesis embedded in H1.

4.2 Personality Traits and Cybercrime Vulnerability (H2)

Survey and interview data provide qualified support for H2. Respondents reporting high anxiety sensitivity—a characteristic aligned with the neuroticism dimension of the Big Five—were significantly more likely to report clicking on suspicious links or disclosing credentials in response to phishing communications. Respondents reporting lower self-reported conscientiousness demonstrated significantly higher rates of neglecting software updates and utilizing weak or repeated passwords across accounts (John & Srivastava, 1999; McCrae & Costa, 1997).

Importantly, personality traits functioned as moderating rather than deterministic risk factors. Cybersecurity awareness training was found to substantially attenuate the relationship between high neuroticism and phishing susceptibility, underscoring the intervention potential of targeted education programs.

4.3 Effectiveness of Preventive Measures (H3)

Evidence supports H3, with multi-layered preventive interventions demonstrating significant protective effects. Organizations implementing Zero Trust Architecture reported substantially lower rates of unauthorized access incidents. Multi-Factor Authentication deployment reduced account compromise rates by an estimated 99.9% in organizational contexts, consistent with findings by Kumar et al. (2023). Employee cybersecurity training programs reduced successful phishing rates by 60–70% in organizations with sustained, simulation-based training protocols.

Table 3 presents AI-based detection methods evaluated in the study, including their applications, strengths, and limitations. Table 4 summarizes preventive measures and their assessed effectiveness based on the synthesized evidence base.

Table 3: *AI and Machine Learning Methods for Cyber Threat Detection*

AI/ML Method	Application in Cyb Threat Detection	Strengths	Limitations
Deep Learni (CNN/RNN)	Malware classificatic network intrusion detectio	High accuracy on lar datasets	Computationally intensiv requires labeled data
Natural Langua Processing (NLP)	Phishing email detectic social engineeri identification	Effective on text-bas threats	May miss novel phrasir language-dependent
Random Forest Ensemble Methods	Anomaly detection, insic threat identification	Robust, interpretable	Less effective on high imbalanced datasets
Federated Learning	Privacy-preserving thre intelligence sharing	Protects data priva across organizations	Communication overhea model poisoning risk
Generative Adversar Networks (GANs)	Synthetic attack simulatic adversarial testing	Enables proactive defer testing	Can also be misused generate deepfakes

Table 4: *Summary of Preventive Measures and Their Assessed Effectiveness*

Preventive Measure	Description	Effectiveness
Zero Trust Architecture	Implements 'never trust, always veri principles for all network access	High when fully deployed; challengi implementation
Multi-Factor Authenticati (MFA)	Requires multiple verification forms f system access	Very effective; user adoption remains challenge
Employee Cybersecur Training	Educating staff on risks, phishi simulation, and best practices	Crucial for social engineeri prevention; requires reinforcement
AI-Based Threat Detection	Using ML algorithms to identify a respond to threats in real time	Promising and evolving; may circumvented by sophisticated actors
Regular Patch Management	Timely software updates to addre known vulnerabilities	Highly effective; often neglected due operational pressures
Incident Response Planning	Developing and testing plans for cyb incident containment	Critical for damage minimizatic frequently deprioritized
International Cybersecur Cooperation	Sharing threat intelligence a coordinating cross-border responses	Potentially high impact; hampered geopolitical tensions

4.4 AI-Based Detection Performance (H4)

Comparative analysis of detection systems provides support for H4. Deep learning-based intrusion detection systems demonstrated classification accuracy exceeding 97% on benchmark network traffic datasets, compared to 78–82% accuracy rates achieved by signature-based detection systems on equivalent datasets (Agrawal et al., 2021). Natural language processing models trained for phishing detection achieved precision rates above 94% in identifying COVID-themed phishing emails that evaded conventional spam filters.

Federated learning frameworks demonstrated particular promise in enabling collaborative threat intelligence sharing across organizations without exposing sensitive proprietary data, addressing a significant barrier to cross-organizational cybersecurity cooperation. However, adversarial AI techniques—including the use of generative adversarial networks to craft evasive phishing content—represent a persistent and evolving challenge to AI-based detection systems.

5. Discussion

The findings of this study illuminate several critical dimensions of the pandemic-era cyber threat landscape and carry significant implications for cybersecurity policy, practice, and research.

5.1 Structural and Contextual Drivers of Cyber Terrorism

The pandemic created a unique convergence of structural vulnerabilities that cybercriminals systematically exploited. The rapid, unplanned nature of digital transformation—particularly the mass transition to remote work—meant that organizations prioritized operational continuity over security hardening (Dwivedi et al., 2020). Reduced cybersecurity budgets, overextended IT teams, and the expansion of the attack surface to encompass home networks and personal devices collectively created conditions highly favorable to exploitation (He et al., 2021).

The emergence of sophisticated attack vectors—including AI-powered spear-phishing, supply chain compromise, and double-extortion ransomware—reflects the adaptive capability of cybercriminal organizations. These actors demonstrated rapid innovation in response to changing environmental conditions, underscoring the need for equally adaptive and anticipatory defensive frameworks (Kumar et al., 2023; Luknar, 2020).

5.2 Sectors Most Severely Affected

The healthcare sector emerged as the most severely targeted, reflecting both the critical value of medical data and the sector's historically underinvested cybersecurity infrastructure. The education sector faced acute vulnerabilities stemming from the precipitous shift to online learning platforms, often implemented without adequate security review. Financial services institutions experienced significant increases in online fraud and account takeover attempts coinciding with increased online transaction volumes. Government agencies, serving as repositories of high-value personal data and pandemic response coordinators, were targeted by both financially motivated and state-sponsored actors (Halwai & Loonkar, 2022; Najar & Naik, 2022).

5.3 Implications for AI-Based Cybersecurity

The dual-use nature of AI represents one of the most consequential cybersecurity challenges of the current era. While AI-based detection systems demonstrate superior performance on established threat categories, the adversarial application of AI—including deepfakes, automated vulnerability discovery, and evasive malware generation—demands continuous advancement of defensive AI capabilities. Policymakers and organizations must invest in the development, validation, and ethical deployment of AI-based security systems that can adapt to novel threat modalities while preserving privacy and minimizing false positive rates (Agrawal et al., 2021).

Federated learning represents a particularly promising avenue for advancing collaborative cyber defence without sacrificing data sovereignty—a framework with especially high relevance for healthcare, government, and critical infrastructure sectors that possess sensitive data but face regulatory restrictions on data sharing.

5.4 Psychological Dimensions of Cyber Defence

The psychological dimensions of cyber vulnerability—consistently underrepresented in technical cybersecurity literature—emerge from this study as central to effective defence design. Cybersecurity interventions that address the emotional and cognitive dimensions of decision-making under threat—rather than relying solely on technical controls—are likely to achieve substantially greater protective effects (Kirwan & Power, 2013; Barak, 2008). Organizations should integrate psychological resilience training, stress management support, and cognitively accessible security communications into their broader cybersecurity programs.

6. Conclusion

This study demonstrates that the COVID-19 pandemic fundamentally transformed the cyber threat landscape by creating a convergence of structural vulnerabilities, psychological risk factors, and opportunistic criminal adaptation. The dramatic increase in cyber terrorism during and after the pandemic reflects not only the tactical adaptability of malicious actors but also the systemic underinvestment in cybersecurity resilience across critical sectors.

The integration of AI-based detection systems—including deep learning, natural language processing, and federated learning frameworks—offers substantial promise for enhancing threat identification speed and accuracy. However, the adversarial application of AI by cybercriminals necessitates ongoing investment in adaptive, robust, and ethically designed defensive AI systems.

Effective cyber defence in the post-pandemic era requires a genuinely multi-layered approach encompassing technical controls, behavioral interventions, and policy frameworks. Particular priority should be accorded to Zero Trust Architecture implementation, sustained and simulation-based employee training, multi-factor authentication adoption, and international cybersecurity cooperation frameworks.

Future research should prioritize the collection and analysis of large-scale longitudinal data on pandemic-related cybercrime to enable more precise causal inference. Additionally, the development of personality-informed and culturally adapted cybersecurity education programs represents a high-value research frontier with significant practical implications. The exploration of AI governance frameworks that balance defensive capability with ethical constraints constitutes another critical area for scholarly and policy attention.

References

Agrawal, M., Tapaswi, S., & Sandhu, R. (2021). A systematic review on cyber security trends. Materials Today: Proceedings, 37(Part 2), 2333–2339. https://doi.org/10.1016/j.matpr.2020.07.728

Ahmad, S. U., Kashyap, S., Shetty, S., & Sood, N. (2021). Cybersecurity during COVID-19. In Italian Conference on Theoretical Computer Science (pp. 1–15). Springer.

Avdiienko, V., Kuznetsov, K., Gorla, A., Zeller, A., Arzt, S., Rasthofer, S., & Bodden, E. (2015, August). Mining apps for abnormal usage of sensitive data. In Proceedings of the 37th IEEE International Conference on Software Engineering (Vol. 1, pp. 426–436). IEEE. https://doi.org/10.1109/ICSE.2015.58

Barak, A. (Ed.). (2008). Psychological aspects of cyberspace: Theory, research, applications. Cambridge University Press. https://doi.org/10.1017/CBO9780511813740

Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In B. De Decker & A. Zúquete (Eds.), Communications and Multimedia Security (pp. 63–72). Springer. https://doi.org/10.1007/978-3-662-44885-4_5

Dell'Amico, M., Michiardi, P., & Roudier, Y. (2010, March). Password strength: An empirical analysis. In 2010 Proceedings IEEE INFOCOM (pp. 1–9). IEEE. https://doi.org/10.1109/INFCOM.2010.5461951

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., Gupta, B., Lal, B., Misra, S., Prashant, P., Raman, R., Rana, N. P., Sharma, S. K., & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. International Journal of Information Management, 55, 102211. https://doi.org/10.1016/j.ijinfomgt.2020.102211

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. Telecommunication Systems, 67(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z

Halfond, W. G. J., Viegas, J., & Orso, A. (2006, March). A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE International Symposium on Secure Software Engineering (Vol. 1, pp. 13–15). IEEE.

Halwai, S., & Loonkar, S. (2022). Overview of key cyber security threats amid COVID-19 pandemic. International Journal for Research in Applied Science and Engineering Technology, 10(3), 1234–1241. https://doi.org/10.22214/ijraset.2022.40765

He, W., Zhang, Z., & Li, W. (2021). Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. International Journal of Information Management, 57, 102287. https://doi.org/10.1016/j.ijinfomgt.2020.102287

John, O. P., & Srivastava, S. (1999). The Big Five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), Handbook of personality: Theory and research (2nd ed., pp. 102–138). Guilford Press.

Khweiled, R., Jazzar, M., & Eleyan, D. (2021). Cybercrimes during COVID-19 pandemic. International Journal of Information Engineering and Electronic Business, 13(2), 1–10. https://doi.org/10.5815/ijieeb.2021.02.01

Kirwan, G., & Power, A. (2013). Cybercrime: The psychology of online offenders. Cambridge University Press. https://doi.org/10.1017/CBO9781139177290

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Kumar, S., Sharma, M. G., Sharma, P. S., & Sagar, V. (2023). Post pandemic cyber attacks impacts and countermeasures: A systematic review. Artificial Intelligence and Symbolic Computation, 14, 1–22. https://doi.org/10.1007/978-3-031-39387-5

Kumari, A., Kumar, A., Behera, R. K., & Shukla, S. K. (2021). Cybersecurity concerns in the era of COVID-19 pandemic. Materials Today: Proceedings, 46(Part 11), 10338–10342. https://doi.org/10.1016/j.matpr.2021.01.290

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248

Luknar, I. (2020). Cyber terrorism threat and the pandemic. In The Euro-Atlantic Values in the Balkan Countries (pp. 1–12). Faculty of Security Studies, University of Belgrade.

McCrae, R. R., & Costa, P. T., Jr. (1997). Personality trait structure as a human universal. American Psychologist, 52(5), 509–516. https://doi.org/10.1037/0003-066X.52.5.509

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems, 29(3), 306–321. https://doi.org/10.1080/0960085X.2020.1771222

Najar, A. A., & Naik, S. M. (2022). COVID-19 impact on cyber crimes in India: A systematic study. In 2022 IEEE India Council International Subsections Conference (INDISCON) (pp. 1–6). IEEE. https://doi.org/10.1109/INDISCON54605.2022.9862882

Prasad, P. W. C., et al. (2026). Explainable AI: Enhancing decision-making in the detection of cyber threats. *Frontiers in Computer Science, 8*, Article 1762332. https://doi.org/10.3389/fcomp.2026.1762332.

Rajkumar, R. P. (2020). COVID-19 and mental health: A review of the existing literature. Asian Journal of Psychiatry, 52, 102066. https://doi.org/10.1016/j.ajp.2020.102066

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89. https://doi.org/10.3390/fi11040089

Shareena, P., & Shahid, M. (2020). Work from home during COVID-19: Employees perception and experiences. Global Journal for Research Analysis, 9(5), 1–3.

White, S. J., & Schwartz, T. (2026, May). *Cyber & AI in the terrorism battlespace* [Panel presentation]. Homeland Security Today 2026 Counterterrorism Summit, Washington, DC, United States. https://www.hstoday.us/subject-matter-areas/counterterrorism/counterterrorism-2026-cyber-and-ai-in-the-terrorism-battlespace/

Xiong, J., Lipsitz, O., Nasri, F., Lui, L. M. W., Gill, H., Phan, L., Chen-Li, D., Iacobucci, M., Ho, R., Majeed, A., & McIntyre, R. S. (2020). Impact of COVID-19 pandemic on mental health in the general population: A systematic review. Journal of Affective Disorders, 277, 55–64. https://doi.org/10.1016/j.jad.2020.08.001

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials, 15(4), 2046–2069. https://doi.org/10.1109/SURV.2013.031413.00127