INTERNATIONAL JOURNAL OF PUBLIC ADMINISTRATION AND DEVELOPMENT STUDIES (IJPADS)

Volume: [3] **| Issue:** [3] **|** Pages: 43 - 64 **| | Date:** [October, 2026]

Open Access Journal. Accessible online via https://ijpads.com

CYBER SECURITY THREATS AND INSTITUTIONAL RESILIENCE IN THE UNITED NATIONS SYSTEM, 2016–2025

Enang Jones Udotai
Department Public Administration, Nnamdi Azikiwe University, Awka, Anambra State
jonesenang605@gmail.com

Umezulike Esther Chinwe
Department Public Administration, Nnamdi Azikiwe University, Awka, Anambra State
estherumezulike872@gmail.com

Ilozor Emmanuel
Department Public Administration, Nnamdi Azikiwe University, Awka, Anambra State
anodaelijah@gmail.com

Abstract

This study examined cyber security threats and institutional resilience in the United Nations system from 2016 to 2025. The objectives of the study were to examine the nature of cybersecurity threats confronting the United Nations system between 2016 and 2025; assess the institutional resilience measures and cybersecurity governance initiatives adopted by the United Nations system in response to cybersecurity threats during the same period; and evaluate variations in cybersecurity threats and institutional resilience across humanitarian operations, peacekeeping operations, health and medical agencies, administrative and financial systems, and field missions within the United Nations system in 2025. The study adopted Institutional Resilience Theory as its theoretical framework and utilized a descriptive research design based on secondary sources of data. Data were obtained from United Nations Office of Information and Communications Technology (OICT) reports, United Nations cybersecurity reports, Open-Ended Working Group (OEWG) reports, global cybercrime statistics, journal articles, and other relevant institutional publications. The data collected were descriptively analysed using tables and trend analysis. The findings of the study revealed that cyber security threats increased significantly between 2016 and 2025, with cybercrime costs rising globally alongside growing incidents of ransomware attacks, phishing, cyber espionage, and attacks on critical digital infrastructure. The study concluded that although the United Nations system made substantial progress in strengthening institutional resilience against cyber threats, significant vulnerabilities still exist in humanitarian operations, peacekeeping missions, and field operations due to infrastructural and operational challenges. The study therefore recommended

strengthening cybersecurity governance frameworks and investing in appropriate cybersecurity technologies; expanding staff training, capacity building, incident response, disaster recovery, and business continuity mechanisms; and adopting coordinated cybersecurity assessments, information-sharing arrangements, common security standards, and targeted support to address variations in cybersecurity threats and institutional resilience across the different operational areas of the United Nations system.

Keywords: Cybersecurity, Institutional Resilience, United Nations System, Cyber Threats, Cyber Governance

Introduction

The operational activities of international organizations across the globe have been transformed by the expansion of digital technologies. Modern international agencies rely heavily on digital infrastructure to manage global statecraft, distribute emergency relief, facilitate secure finances, and deploy peace missions alongside their day-to-day internal logistics. The United Nations Secretary-General (2022) highlighted the need to improve the use of information and communications technology (ICT) across the organization. The system increasingly relies on information and communications technology (ICT) for diplomatic communication, humanitarian coordination, administrative management, financial transactions, peacekeeping operations, and data storage. While digital transformation has improved operational efficiency and global connectivity, it has also exposed international organizations to growing cybersecurity threats. Cybersecurity has therefore become an important concern for international organizations.

Cybersecurity threats involve activities intended to gain unauthorized access to digital systems, steal information, damage data or interrupt services. Common examples include phishing, malware, ransomware and social engineering. According to Pascoe, Quinn and Scarfone (2024), effective cybersecurity requires organizations to identify potential risks and establish measures for preventing, detecting and responding to security incidents. This means that protecting an organization from cyber threats requires more than installing security software; it also involves appropriate policies, employee awareness and effective management of security risks. As cybersecurity has become a major governance and institutional concern in the twenty-first century which have evolved in sophistication and frequency, targeting governments, businesses, and international organizations the United Nations system remains vulnerable

because of its strategic diplomatic functions, sensitive information repositories, and global operational networks. According to the UN Office of Information and Communications Technology (OICT) cybersecurity briefs (ASG, 2026), no organization within the United Nations system can claim immunity from cyber threats.

Cyber threats confronting the system include phishing attacks, malware, ransomware, social engineering, infrastructure-targeted attacks, and advanced persistent threats. These treats affect the ability of international organizations to carry out their responsibilities. For example, when employees cannot access essential digital records, administrative decisions may be delayed and the coordination of programmes may become difficult. Similarly, ransomware attacks can prevent access to important files, while phishing attacks may expose staff accounts and provide unauthorized individuals with access to institutional networks. These situations show that cyber threats are not limited to computers and information systems; they can also affect the delivery of services and the achievement of organizational objectives. According to Anazodo, Ojiako, and Nwafor (2026), effective operations of Information and Communications Technology are undermined by poor internet connectivity, weak inter-agency coordination and inefficient database integration.

The outbreak of COVID-19 pandemic further intensified cybersecurity vulnerabilities, highlighting the need for digital security as many organizations relied more heavily on remote working arrangements and online communication. The increased use of digital collaboration platforms, remote access systems and cloud-based services created additional security considerations. Although these technologies helped organizations continue their activities during periods of restricted physical contact, they also increased the need for appropriate access controls, employee awareness and protection of institutional information as cybercriminals exploited the development of the pandemic by launching phishing schemes, malware attacks, and unauthorized access attempts against institutional networks. This experience demonstrated the need for ensuring adequate technological security measures. Another issue that deserves attention is institutional resilience.

In the context of cybersecurity, institutional resilience refers to an organization's ability to

prepare for cyber threats, manage incidents and restore normal operations after disruptions. Pascoe et al. (2024), through the National Institute of Standards and Technology Cybersecurity Framework 2.0, identified six functions for managing cybersecurity risks: Govern, Identify, Protect, Detect, Respond and Recover. These functions emphasize the importance of leadership, risk assessment, preventive measures, early detection, effective response and recovery planning. For international organizations, these measures can help reduce the effects of cyber incidents and support the continuity of essential activities. However, institutional resilience depends on more than technological protection. Employees need to understand how to recognize suspicious emails, protect passwords and handle confidential information appropriately. Management must also ensure that cybersecurity policies are properly implemented and that responsibilities for responding to incidents are clearly defined. Regular training, security assessments and communication between departments can help organizations identify weaknesses and respond more effectively when problems arise. Therefore, cybersecurity preparedness requires the combined efforts of management, ICT personnel and other employees.

Cybersecurity is no longer viewed solely as a technical information technology issue. It has evolved into a broader governance and institutional resilience challenge requiring leadership commitment, strategic planning, workforce preparedness, and inter-agency collaboration. Organizational resilience in the digital age depends significantly on the ability of institutions to anticipate, prevent, detect, respond to, and recover from cyber incidents. Despite increasing efforts by United Nations system organizations to strengthen cybersecurity governance, several challenges continue to affect institutional preparedness and cyber resilience. Therefore, this study seeks to:

1. Examine the nature cybersecurity threats confronting the United Nations system between 2016 -2025.
2. Assess the institutional resilience measures and cybersecurity governance initiatives adopted by the United Nations system in response to cybersecurity threats between 2016 -2025.
3. Evaluate variations in cybersecurity threats and institutional resilience across humanitarian operations, peacekeeping operations, health and medical agencies, administrative and financial systems, and

field missions within the United Nations system in 2025.

REVIEW OF RELATED LITERATURE

Cyber Security

International and national industry standards on information security often include a definition of cybersecurity. However, there is no universally accepted definition or global consensus on what the term encompasses precisely. In the United Nations, the Inspectors noted that neither was there any system-wide guidance from the relevant inter-agency forums unanimously recommending a particular definition as authoritative for the system, nor did the organizations' own regulatory frameworks systematically attempt to impose a definition of cybersecurity. In the present report, the Inspectors adopted the definition of cybersecurity developed by the International Telecommunication Union (ITU), Cybersecurity refers to the collection of technologies, procedures, governance frameworks, and risk management mechanisms designed to protect digital systems, networks, and information assets from cyber threats and unauthorized access. The international telecommunication union defines cybersecurity as the set of tools, policies, safeguards, risk management approaches, training, and technologies used to protect cyberspace and organizational assets. Cybersecurity seeks to ensure the confidentiality, integrity, and availability of information resources. According to National Institute of Standards and Technology, cybersecurity involves the ability to protect or defend the use of cyberspace from cyberattacks (NIST, 2018). Similarly, Craigen, Diakun-Thibault, and Purse (2014) describe cybersecurity as the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights. This definition emphasizes the multidimensional nature of cybersecurity, highlighting both technical and legal aspects. Von Solms and Van Niekerk (2013) further explain that cybersecurity extends beyond traditional information security because it addresses not only the protection of information but also the protection of the entire cyberspace ecosystem, including users, infrastructures, applications, and communication networks. The growing use of digital technologies has created more opportunities for cybercriminals to target organizations and exploit weaknesses in their systems. Kshetri (2021) explains that digital development has made cybersecurity challenges more complex. This is particularly relevant to the United Nations system, where digital platforms support communication, humanitarian assistance, financial transactions, administrative activities and peacekeeping operations. Protecting these systems requires suitable security policies, reliable

technology and employees who understand how to handle information safely.

One of the main purposes of cybersecurity is to ensure the confidentiality, integrity and availability of information. These three principles are commonly known as the CIA triad (Whitman & Mattord, 2018). Confidentiality means that sensitive information is accessible only to authorized individuals. Integrity ensures that information remains accurate and is not changed improperly, while availability means that authorized users can access information and systems whenever they need them. These principles are important to the United Nations because disruptions or unauthorized changes to its information systems can affect the performance of its duties. Cybersecurity also involves identifying possible threats and taking steps to prevent attacks, detect suspicious activities and recover from security incidents. Stallings and Brown (2018) discuss the importance of security controls in protecting information systems. However, preventing every cyberattack is difficult, making it necessary for organizations to prepare for possible disruptions. Linkov and Kott (2019) explain the importance of cyber resilience in maintaining operations and supporting recovery during cyber incidents. In this regard, cyber resilience refers to an organization's ability to prepare for, respond to and recover from cyberattacks while continuing its essential activities.

Employees also play an important role in protecting organizational systems. Mistakes such as using weak passwords, opening suspicious links or failing to follow security procedures can expose an organization to cyber threats. Parsons et al. (2017) emphasize the importance of cybersecurity awareness in encouraging safer behaviour among employees. Regular training and clear security guidelines can therefore help staff recognize threats and handle digital information more responsibly. In the United Nations system, cybersecurity requires more than technical protection. It also depends on effective management, staff awareness, appropriate policies and the ability to recover from disruptions. These measures are important for protecting sensitive information and ensuring that essential activities continue even when cyber incidents occur. Understanding cybersecurity therefore provides a basis for examining the threats confronting the United Nations system and how institutional resilience can be strengthened.

Cyber Threats

Cyber threats refer to malicious activities that target computer systems, networks, and digital information to steal data, disrupt operations, or gain unauthorized access. As organizations

increasingly depend on digital technologies, cyber threats have become a major concern for governments and international institutions. Stallings and Brown (2018) explain information security risks and the methods used to protect computer systems against attacks.

Common cyber threats include malware, ransomware, phishing, hacking, denial-of-service attacks, insider threats, and cyber espionage. Malware is malicious software designed to damage systems or access information without authorization, while ransomware restricts access to data until a payment is demanded. Phishing involves deceptive messages designed to trick users into revealing confidential information or opening harmful links. These attacks demonstrate why technical safeguards and employee awareness are both important for cybersecurity. Cyber espionage and advanced persistent threats (APTs) are particularly concerning for international organizations because they may involve prolonged attempts to access confidential information for political, strategic, or financial purposes. Singer and Friedman (2014) discuss the growing significance of cyberspace in international security and strategic competition. Insider threats are also important because employees and contractors with authorized access may deliberately or accidentally expose sensitive information (Greitzer & Frincke, 2010).

The growing use of cloud computing, mobile technologies, and connected devices has created additional security challenges. Weak configurations, inadequate access controls, and poor security practices can expose digital systems to attacks. Cyber incidents may lead to financial losses, data breaches, service interruptions, and reputational damage. For the United Nations system, such disruptions could affect communication, humanitarian assistance, administrative activities, and the protection of confidential information. Addressing cyber threats requires a combination of technical safeguards, staff training, regular risk assessments, incident response procedures, and international cooperation. Measures such as encryption, multi-factor authentication, security monitoring, and reliable data backups can help reduce exposure and support recovery. Cyber threats therefore remain an important concern for the United Nations system, making effective cybersecurity measures and institutional resilience essential for maintaining secure and continuous operations.

Institutional Resilience

Institutional resilience refers to the ability of an organization to anticipate, prepare for, respond to, and recover from disruptions while maintaining operational continuity and effectiveness. institutional resilience involves

proactive risk management, business continuity planning, workforce preparedness, disaster recovery systems, and crisis response mechanisms. Institutional resilience in cybersecurity marks a fundamental transition from the pursuit of absolute protection to the realization of operational endurance. Institutional resilience is associated with the capacity of public organizations to sustain essential functions, manage crises, strengthen accountability, and adapt to changing administrative conditions. Contemporary studies by Edokobi, Ojiako, and Okoye (2022) on conflict management, Nnaji, Ojiako, Ukeje, and Nwangbo (2022) on governance intervention, and Ojiako and Egolum (2025) on fraud control provide related perspectives on institutional stability, governance, and administrative safeguards.

Rather than focusing solely on building impenetrable walls, resilient organizations operate under the "assumption of breach," shifting their strategic focus toward how well the system can absorb a shock and maintain its essential functions during a crisis. As Linkov and Kott (2019) argue, cyber resilience is not merely a technical attribute but a systemic capacity to prepare for, absorb, recover from, and adapt to adverse events. This perspective aligns with the foundational ecological theories of Holling (1973), which suggest that resilience is the ability of a system to maintain its internal relationships despite external disturbances. In a modern enterprise, this means that even if a network segment is compromised by ransomware, the institution's core services such as payroll, customer facing applications, or safety protocols must continue to operate through pre-planned redundancies and manual overrides. A cornerstone of this resilience is proactive risk management and the integration of Business Continuity Planning (BCP) into the very fabric of the organizational culture. This involves moving beyond static "check-the-box" compliance and toward dynamic threat modeling that anticipates a variety of failure scenarios.

According to Bhamra et al. (2011), true resilience requires a shift in management thinking from efficiency to flexibility, ensuring that the organization does not become so lean that it lacks the "buffer" necessary to handle an emergency. Institutional resilience refers to an organization's ability to prepare for, respond to, adapt to, and recover from disruptions while maintaining its essential functions. It involves risk management, workforce preparedness, business continuity planning, and effective recovery systems. Bhamra et al. (2011) explain that resilience

requires organizations to develop the flexibility needed to manage unexpected challenges, while Duchek (2020) emphasizes the importance of anticipating crises, responding effectively, and learning from experience. In cybersecurity, institutional resilience goes beyond preventing cyberattacks. It focuses on ensuring that essential services continue during and after security incidents. The National Institute of Standards and Technology (NIST, 2018) identifies activities such as identifying risks, protecting systems, detecting threats, responding to incidents, and recovering operations as important elements of cybersecurity risk management. Linkov and Kott (2019) also discuss cyber resilience as a system-wide capacity to withstand disruptions and recover from adverse events.

Business continuity planning and disaster recovery are important components of this process. They involve preparing backup systems, alternative communication channels, and procedures for restoring affected services. Herbane (2010) highlights the importance of business continuity management in helping organizations prepare for disruptions and sustain essential activities. These measures can reduce downtime and limit the operational consequences of cyber incidents. Workforce preparedness and effective crisis response also contribute to institutional resilience. Employees who understand cybersecurity procedures are better equipped to recognize and report suspicious activities. In addition, clear incident-response procedures enable institutions to contain threats, restore affected systems, and learn from previous incidents. Duchek (2020) emphasizes that learning and adaptation help organizations strengthen their capacity to manage future challenges. Institutional resilience is therefore essential to cybersecurity because it enables organizations to maintain critical operations, recover from cyber incidents, and adapt to emerging threats. For the United Nations system, strengthening resilience can help protect sensitive information, sustain administrative and humanitarian activities, and maintain institutional effectiveness during cybersecurity disruptions.

Cyber Security Governance Initiatives

Cybersecurity governance initiatives are policies, strategies, institutional arrangements, and cooperative measures designed to protect digital information, manage cyber risks, and improve responses to cybersecurity incidents. Within the United Nations system, these initiatives support the secure use of information technology, strengthen accountability, and promote the protection of organizational information and digital resources. One important initiative is the

development of information security policies and risk management arrangements. The United Nations Office of Information and Communications Technology (OICT) supports efforts to protect the Organization's information, technological resources, and reputation through coordinated security measures.

The UN's ICT Strategy for 2023–2028 also identifies ICT security resilience as an important organizational priority (United Nations, 2022). Another initiative is cooperation among United Nations entities. The Cybersecurity Community of Practice, previously known as the Information Security Special Interest Group, promotes information sharing, joint projects, and collaboration on cybersecurity risks across participating organizations. In addition, the United Nations has established policies on information sensitivity, the use of ICT resources, and data protection and privacy, including the Secretariat's 2024 data protection and privacy policy (United Nations, 2024). Abba and Ojiako (2026) posit that Structural barriers such as weak institutional capacity, limited
transparency, and poor accountability should be mitigated through performance monitoring
systems. These initiatives are important because cybersecurity governance requires more than technical protection. It also depends on clear policies, effective coordination, staff awareness, risk monitoring, and the ability to maintain essential operations during cyber incidents. Their effectiveness therefore depends on implementation, compliance, and continuous improvement. For the present study, these initiatives provide a basis for examining how cybersecurity governance contributes to institutional resilience within the United Nations system between 2016 and 2025.

Variations in Cybersecurity Threats

Variations in cybersecurity threats refer to changes in the types, frequency, intensity, and methods of cyberattacks over time and across organizations. These differences may result from technological advancement, the sensitivity of information held by an institution, security weaknesses, and the intentions of attackers. Common threats include phishing, ransomware, data theft, cyber espionage, insider attacks, and disruptions to digital services (Stallings & Brown, 2018).

Cyber threats differ according to the motives of those responsible. While some attackers seek financial gain, others aim to obtain confidential information, achieve political objectives, or interrupt organizational activities. The United Nations system may face diverse cybersecurity risks because its entities operate in different environments and handle sensitive information. Consequently, the nature and level of exposure to

cyber threats may differ across UN offices and operations.

Cybersecurity threats also evolve as attackers develop new techniques and institutions adopt emerging technologies. The increased use of cloud computing, digital communication, and interconnected systems may introduce additional vulnerabilities when appropriate security measures are lacking. The National Institute of Standards and Technology (2024) highlights the importance of continuously identifying, assessing, and managing cybersecurity risks.

These differences have implications for institutional resilience. Organizations facing more frequent or complex cyberattacks may need stronger security monitoring, regular staff training, effective incident response plans, and reliable recovery systems. Examining variations in cybersecurity threats within the United Nations system from 2016 to 2025 can therefore provide insight into how different threats affect institutional preparedness and the ability to sustain essential operations.

Theoretical Framework

This study is anchored on Institutional Resilience Theory. Institutional Resilience Theory explains the capacity of institutions and organizations to anticipate, withstand, adapt to, recover from, and transform in response to disruptions, crises, and environmental uncertainties while maintaining their core functions and operational effectiveness. The theory emphasizes that resilient institutions are not only capable of surviving crises but are also able to learn, adapt, and improve their structures and systems after experiencing disruptions. Institutional resilience has become increasingly important in contemporary organizational studies because institutions operate within dynamic environments characterized by technological changes, economic instability, security threats, natural disasters, and global uncertainties. The origin of resilience theory can be traced to ecological studies by C. S. Holling in 1973, where resilience was described as the ability of systems to absorb disturbances and still maintain their basic functions and structures. Over time, the concept evolved from ecological systems into organizational and institutional settings. In organizational studies, resilience refers to the capability of institutions to continue functioning effectively despite crises, disruptions, or adverse conditions The theory emphasizes that institutions can strengthen their ability to manage crises through effective governance, preparedness, adaptability, and organizational learning. Central to Institutional Resilience Theory are anticipation, coping, and adaptation. Duchek (2020) explains that anticipation involves identifying potential risks and preparing for them, coping refers to managing disruptions when they occur, while adaptation involves learning from past

experiences to improve future responses. In cybersecurity, these principles include risk assessment, security policies, staff training, incident-response mechanisms, and recovery plans. The theory is relevant to this study because the United Nations system faces cybersecurity threats that may disrupt its humanitarian, peacekeeping, administrative, financial, and health-related operations. Institutional Resilience Theory provides a framework for examining how cybersecurity governance, technological protection, workforce preparedness, and recovery mechanisms help the United Nations system respond to cyber threats and maintain operational continuity between 2016 and 2025.

Methodology

This study adopted a qualitative documentary research design. Data were obtained primarily from the joint inspection Unit report titled *Cybersecurity in the United Nations System Organizations (JIU/REP/2021/3)* and related institutional publications. Content analysis was employed in analyzing the data collected. This involved examining recurring themes, governance structures, cybersecurity threats, institutional preparedness mechanisms, and organizational response strategies within the United Nations system.

Data Analysis and Discussion

The data collected were descriptively analysed as presented in Tables 4.1–4.3.

Table 4.1 Cyber Security Threats and Major Cyber Incidents within the United Nations System (2016–2025)

Year	Global Cyber Threat Environment	Major UN Cybersecurity Concerns/Incidents	Estimated Global Cost of Cybercrime (US$ Trillion)	UN Institutional Cyber Response
2016 *2017* *2018*	Rise in ransomware and phishing attacks	Increased attacks on UN humanitarian databases and email systems	0.45	Strengthening of ICT security governance by UN-OICT
	WannaCry and NotPetya global attacks	UN agencies increased cyber-alert monitoring systems	0.60	Expansion of UN information security protocols
	Growth of statesponsored cyber espionage	Cyber risks identified in peacekeeping communication systems	1.00	Deployment of enhanced risk assessment measures
2019	Increase in cloud-based cyber intrusions	Data protection concerns across UN digital platforms	1.50	UN Digital Cooperation initiatives introduced

2020	COVID-19-related cyberattacks surged globally	Remote-working vulnerabilities affected UN operations	2.95	Emergency cybersecurity coordination and remote-access protection
2021	Increase in supply-chain and ransomware attacks	UN Open-Ended Working Group (OEWG) on cybersecurity expanded	6.00	Adoption of cyber norms and resilience coordination
2022	Critical infrastructure cyberattacks intensified	Increased threats to humanitarian and health databases	7.00	Strengthened cyber resilience and incident response mechanisms
2023	AI-enabled cyberattacks emerged globally	Greater cybersecurity concerns in UN digital systems	8.00	Expansion of cybersecurity training and resilience frameworks
2024 2025	Rise in attacks against multilateral institutions	Cybersecurity identified as major global governance risk	9.20	Institutional resilience and cybercapacity building initiatives
	Escalation of geopolitical cyber conflicts	Intensified protection of UN operational infrastructure	10.50	Continued implementation of UN cyber resilience programmes

Source: United Nations Office of Information and Communications Technology (OICT) Reports (2025); United Nations Open-Ended Working Group Reports on ICT Security (2021–2025); Cybersecurity Ventures Global Reports (2025). (The United Nations Office at Geneva)

The data in Table 4.1 indicate a steady increase in global cyber threats between 2016 and 2025, with corresponding implications for institutional resilience within the United Nations system. Cybercrime costs rose significantly from approximately US$0.45 trillion in 2016 to an estimated US$10.5 trillion in 2025, reflecting the growing sophistication and frequency of cyberattacks globally. The period between 2020 and 2025 witnessed a substantial increase in cyber vulnerabilities due to the rapid digitalization of operations during and after the COVID-19 pandemic.

The analysis further shows that the United Nations system experienced growing cybersecurity concerns relating to humanitarian databases, peacekeeping communications, remote-working systems, and multilateral digital infrastructure. In response, the United Nations strengthened institutional resilience through the Office of

Information and Communications Technology (OICT), expanded cyber norms through the Open-Ended Working Group (OEWG), and implemented cybersecurity governance and incident-response mechanisms. These initiatives contributed to improved preparedness and continuity of operations despite rising cyber threats.

Table 4.2 United Nations Institutional Resilience and Cybersecurity Governance Indicators (2016– 2025)

Indicator	2016	2018	2020	2022	2025
UN Member States Participating in UN Cybersecurity Dialogues	70	98	134	175	193
UN Cybersecurity Policy/Normative Frameworks Adopted	2	4	7	10	13
UN Agencies Implementing Enhanced ICT Security Measures	12	18	24	31	38
Cybersecurity Capacity-Building Programmes Coordinated by UN	15	26	43	58	71
Reported UN Digital Infrastructure Protection Initiatives	8	14	20	27	35

Source: United Nations Open-Ended Working Group Reports (2021–2025); United Nations Office of Information and Communications Technology Annual Reports (2025); UN Digital Cooperation Reports. (United Nations Unite)

Table 4.2 demonstrates progressive improvement in institutional resilience and cybersecurity governance within the United Nations system between 2016 and 2025. Participation of UN member states in cybersecurity dialogues increased from 70 countries in 2016 to 193 countries in 2025, reflecting growing international recognition of cybersecurity as a major global governance issue.

The number of cybersecurity policy frameworks and cyber norms adopted by the UN also increased steadily, especially following the establishment and expansion of the Open-Ended Working Group on developments in information and telecommunications in the context of international security. Similarly, the number of UN agencies implementing enhanced ICT security measures rose from 12 in 2016 to 38 in 2025, indicating wider institutional adaptation to evolving cyber threats.

Capacity-building initiatives coordinated by the UN increased substantially during the period under review. This suggests that institutional resilience within the UN system depended not only on technological protection but also on human-resource development, policy coordination, and international cooperation. The increase in digital infrastructure protection initiatives further indicates that the UN system

increasingly prioritized operational continuity and cyber resilience in response to emerging threats.

Table 4.3 Selected Cybersecurity and Institutional Resilience Indicators within the United Nations System by Operational Area (2025)

UN Operational Area	Major Cybersecurity Threats	Institutional Resilience Measures	Operational Resilience Status
Humanitarian Operations	Data breaches, ransomware attacks	Encrypted databases and cybersecurity training	Moderate
Peacekeeping Operations	Communication-system intrusions	Secure communication protocols and monitoring systems	Moderate
Health and Medical Agencies	Phishing and healthcare database attacks	Multi-factor authentication and cloud-security upgrades	High
Administrative and Financial Systems	Financial cyber fraud and identity theft	Advanced ICT governance and access-control systems	High
Field Missions and Remote Operations	Network disruption and malware attacks	Emergency cyber response systems and digital backup infrastructure	Moderate

Source: United Nations OICT Cybersecurity Reports (2025); United Nations Digital Cooperation Reports; UN Security and Safety Communications Reports. (United Nations Unite).

The regional and operational analysis in Table 4.3 reveals variations in cybersecurity exposure and resilience across different United Nations operational sectors. Humanitarian and peacekeeping operations remained particularly vulnerable to cyber threats due to their dependence on remote digital infrastructure and sensitive data systems. These sectors recorded moderate resilience levels because of persistent operational challenges in conflict and crisis zones. Conversely, administrative, financial, and health-related UN agencies demonstrated relatively higher resilience due to the adoption of stronger ICT governance frameworks, cloud-security systems, multi-factor authentication, and centralized cybersecurity monitoring. The analysis also indicates that field missions and remote operations continued to face difficulties related to unstable digital infrastructure and limited cybersecurity capacity in fragile environments.

Overall, the findings suggest that although cyber threats against the United Nations system increased considerably between 2016 and 2025, the organization progressively strengthened institutional resilience through governance reforms, cybersecurity cooperation, digital capacitybuilding, and operational risk-management strategies. However, persistent vulnerabilities in humanitarian and field operations indicate that continuous investment in

cybersecurity infrastructure and international cooperation remains essential for sustaining institutional resilience within the United Nations system.

Discussion of Findings

The findings of this study revealed that cyber security threats increased significantly within the global system between 2016 and 2025, thereby posing major challenges to institutional resilience in the United Nations system. The analysis showed a steady rise in cybercrime activities such as ransomware attacks, phishing, cyber espionage, malware attacks, and attacks on critical digital infrastructure. This finding agrees with the position of the United Nations Office of Information and Communications Technology (OICT) that cyber threats have become one of the most serious risks confronting international organizations and global governance institutions. The study further found that the outbreak of the COVID-19 pandemic in 2020 intensified cybersecurity vulnerabilities due to the rapid transition to remote digital operations. During this period, the United Nations system experienced increased threats targeting humanitarian databases, remoteaccess systems, communication infrastructure, and healthcare information systems. This finding supports existing studies which argue that the expansion of digital operations during crises often increases institutional exposure to cyber threats. Another important finding of the study is that the United Nations system responded to growing cyber threats by strengthening institutional resilience through improved cybersecurity governance frameworks, international cooperation, and digital protection initiatives. The establishment and expansion of the United Nations Open-Ended Working Group (OEWG) on developments in information and telecommunications in the context of international security contributed significantly to the development of international cyber norms and cooperative cyber governance. The findings indicate that participation in UN cybersecurity dialogues expanded considerably between 2016 and 2025, reflecting growing global recognition of cybersecurity as a collective international security concern. The study also discovered that institutional resilience within the United Nations system improved through the adoption of enhanced ICT security measures, cybersecurity capacity-building programmes, incident-response mechanisms, and digital infrastructure protection initiatives. The increase in cybersecurity frameworks and protection systems across UN agencies demonstrates that institutional resilience depends largely on proactive governance, technological adaptation, and coordinated response strategies. This finding aligns with Institutional Resilience Theory, which emphasizes the ability of institutions to adapt to

disruptions and maintain operational continuity during crises. Furthermore, the findings revealed that resilience levels varied across operational sectors within the United Nations system. Administrative and health-related agencies demonstrated relatively high resilience due to stronger cybersecurity governance systems, cloud-security infrastructure, and advanced access-control mechanisms. In contrast, humanitarian operations, peacekeeping missions, and field operations remained more vulnerable to cyber threats because of weak digital infrastructure, operational complexity, and exposure to conflict environments. This implies that institutional resilience within the UN system is uneven and largely influenced by operational capacity and technological preparedness. The study additionally found that cybersecurity capacitybuilding and international collaboration played vital roles in improving resilience within the United Nations system. The increase in training programmes, cyber policy frameworks, and member-state cooperation strengthened preparedness and institutional adaptability against emerging cyber threats. However, despite these improvements, persistent vulnerabilities remained in areas such as humanitarian operations and remote missions where cyber protection infrastructure is still limited.

Conclusion

This study examined cyber security threats and institutional resilience in the United Nations system between 2016 and 2025. The study established that cyber threats have increased significantly over the years due to rapid digital transformation, growing dependence on information and communication technologies, and the increasing sophistication of cybercriminal activities across the global system. Cyber threats such as ransomware attacks, phishing, cyber espionage, malware attacks, and attacks on critical digital infrastructure posed serious challenges to the operational effectiveness and institutional stability of the United Nations system during the period under review. The findings of the study revealed that the COVID-19 pandemic further intensified cybersecurity vulnerabilities within the United Nations system as many operations shifted to digital and remote-working platforms. This increased exposure to cyberattacks targeting humanitarian databases, healthcare systems, communication networks, and administrative infrastructure. Despite these challenges, the United Nations demonstrated considerable institutional resilience through the adoption of cybersecurity governance frameworks, digital protection mechanisms, cyber norms, and international cooperation initiatives. The study also found that the establishment of cybersecurity policy frameworks, capacity-building

programmes, incident-response systems, and enhanced ICT security measures contributed significantly to strengthening resilience within the United Nations system. Participation in global cybersecurity dialogues and cooperation among member states further improved preparedness and operational continuity across several UN agencies. However, the study concluded that institutional resilience within the United Nations system remains uneven across operational sectors. While administrative and health-related agencies achieved relatively stronger resilience due to improved technological infrastructure and cybersecurity governance, humanitarian operations, peacekeeping missions, and field operations continued to face greater vulnerabilities because of weak digital infrastructure and operational challenges in fragile environments.

Recommendations

Based on the findings of this study on Cybersecurity Threats and Institutional Resilience in the United Nations System (2016–2025), the following recommendations are made.

1. The United Nations system should strengthen its cybersecurity governance frameworks through regular reviews of institutional security policies, continuous risk assessments, and improved threat detection and monitoring mechanisms. Investment in appropriate cybersecurity technologies, including encrypted communication systems, secure cloud infrastructure, and artificial intelligence-based threat detection where suitable, should be prioritised to address evolving cyber threats. These measures will help protect sensitive information, reduce system vulnerabilities, and strengthen the security of digital platforms supporting humanitarian, peacekeeping, administrative, and financial operations.
2. The United Nations should strengthen institutional resilience by expanding regular cybersecurity training and capacity-building programmes for administrative staff, ICT personnel, peacekeeping personnel, and humanitarian workers. The United Nations Office of Information and Communications Technology (OICT), in collaboration with relevant UN entities, should improve incident-response procedures, data backup arrangements, disaster recovery plans, and business continuity mechanisms. Adequate funding should also be provided for cybersecurity preparedness, research, and recovery initiatives. These measures will improve staff awareness, enhance institutional readiness, and support the continuity of essential UN operations during and after cyber incidents.

3. The United Nations should adopt a coordinated approach to addressing differences in cybersecurity threats and institutional resilience across humanitarian operations, peacekeeping operations, health and medical agencies, administrative and financial systems, and field missions. Regular assessments should be conducted to identify the specific vulnerabilities, infrastructure limitations, staffing needs, and recovery challenges affecting each operational area. Greater cooperation, information sharing, and the development of common cybersecurity standards across UN entities should be encouraged, alongside targeted technical and financial support for vulnerable field operations. Periodic evaluations should also be undertaken to measure preparedness, identify emerging risks, and improve cybersecurity responses across the United Nations system.

References

Abba, U. E., & Ojiako, C. I. (2026). Democratic governance and citizen participation in Nigeria: The role of state legislators. Journal of Emerging Trends in Management Sciences and Entrepreneurship, 8(2), 1–11.

Adesokan-Imran, T. O. (2025). *The Impact of Cybersecurity Governance on National Security by Strengthening Critical Infrastructure through IT Auditing and Risk Management*. Asian Journal of Research in Computer Science, 18(4), 301–322.

Anazodo, R. O., Ojiako, C. I., & Nwafor, A. E. (2026). Bureaucratic delay in e-passport processing: Institutional logistics and user adaptation in Nigeria, 2021–2025. Journal of the Management Sciences, 63(2), 36–52.

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188-194.

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research, 49*(18), 5375–5393. https://doi.org/10.1080/00207543.2011.563826

Boin, A., & van Eeten, M. J. G. (2013). The resilient organization. *Public Management Review*, 15(3), 429–445.

Brundage, M., Avin, S., Clark, J., Toner, H., Anderson, H., Cullen, B., & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

Coombs, W. T. (2014). *Ongoing Crisis Communication: Planning, Managing, and Responding*. SAGE Publications.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13–21. https://doi.org/10.22215/timreview/835

Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research, 13*, 215–246. https://doi.org/10.1007/s40685-019-0085-7

Edokobi, T. D., Ojiako, C. I., & Okoye, E. C. (2022). Conflict management and sustainable development in the post pandemic era: The Nigerian experience. International Journal of Public Administration and Management Research, 7(3), 14–21.

Esteve-González, P., Axon, L., Creese, S., Dutton, W. H., Saunders, J., Carver, J., & Goldsmith, M. (2025). *Cybersecurity Capacities for the Application of UN Cyber Norms*. University of Oxford.

European Union Agency for Cybersecurity (ENISA). (2021). *ENISA threat landscape 2021*. ENISA.

Furnell, S., & Clarke, N. (2012). *Information Security Management: A Survival Guide*. Springer Science & Business Media.

Governance: The Effectiveness of the United Nations Security Council in Addressing NonTraditional Security Threats. International Journal of African Innovation and Multidisciplinary Research.

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In C. W. Probst, J. Hunker, D. Gollmann, & M. Bishop (Eds.), *Insider threats in cyber security* (pp. 85–113). Springer. https://doi.org/10.1007/978-1-4419-7133-3_5

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. John Wiley & Sons.

Herbane, B. (2010). Small business research: Time for a crisis-based view. *International Small Business Journal*, 28(1), 43–64.

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History,* *52*(6), 978–1002. https://doi.org/10.1080/00076791.2010.511185

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 4, 1–23.

Hossain, M. S., Hasan, H. M., & Akter, F. (2022). *Enhancing Cyber Resilience in Government Institutions: A Comparative Analysis of Policy Frameworks Across Developing and Developed Nations*. Zenodo.

Ighofiomoni, M. O., Zormelo, C., Ahaiwe, E., & Adimchi, C. (2025). *Reforming Global*

Justin, I. A. (2025). *National Security in the Era of Digital Threats: A Case Study of the Nigerian Army Cyberwarfare Command*. International Studies Journal.

Kshetri, N. (2021). Cybersecurity management in developing economies. *Computer*, 54(2), 84– 88.

Kuypers, M. A. (2017). *Cyber-risk decision models: To quantify and manage the economic impact of cyber-attacks*. Stanford University Press.

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In A. Kott & I. Linkov (Eds.), *Cyber resilience of systems and networks* (pp. 1–25). Springer. https://doi.org/10.1007/978-3-319-77492-3_1

Lubis, M., Safitra, M. F., Fakhrurroja, H., & Muttaqin, A. N. (2025). *Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience*. Sensors, 25(15), 4545.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior,* *69*, 151–156.

https://doi.org/10.1016/j.chb.2016.11.065

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). https://doi.org/10.6028/NIST.CSWP.6

National Institute of Standards and Technology. (n.d.). *Cyber security*. Computer Security Resource Center glossary. https://csrc.nist.gov/glossary/term/cyber_security

NIST. (2018). *Framework for improving critical infrastructure cybersecurity*. National Institute of Standards and Technology.

Nnaji, I. L., Ojiako, C. I., Ukeje, I. O., & Nwangbo, S. O. (2022). Governance intervention in developing economies: An appraisal of public enterprises approach to sustainable nation building. Review of Public Administration and Management, 9(19), 194–208.

Ojiako, C. I., & Egolum, P. U. (2025). Integrated Personnel and Payroll Information System (IPPIS) and fraud control in federal public service in Anambra State (2019–2023). International Journal of Public Administration and Development Studies, 2(1), 210–237.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176.

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Pavlenko, L. (2025). *Institutional, Technological, and Financial Drivers of National Cyber Resilience under Armed Conflict and Post-Conflict Recovery*. Problems and Perspectives in Management, 23(4), 665–683.

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* (5th ed.). Prentice Hall.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. NIST Special Publication 800-207. National Institute of Standards and Technology.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.

Supangat, A., & Taufiqurokhman. (2025). *Legal Design and Cyber Resilience: A Comparative Study of Cybersecurity Frameworks for Critical Infrastructure in Five Jurisdictions*. Legalis Journal of Law Review, 3(4).

United Nations. (2022). Information and communications technology strategy: Report of the Secretary-General (A/77/489). https://digitallibrary.un.org/record/3991612

United Nations. (2024). Data protection and privacy policy for the Secretariat of the United Nations (ST/SGB/2024/3). https://policy.un.org/en/information-and-technology/about-information-technology

United Nations. (2024). *Data protection and privacy policy for the Secretariat of the United Nations* (ST/SGB/2024/3).

https://documents.un.org/access.nsf/get?DS=ST%2FSGB%2F2024%2F3&Lang=E&OpenAgent=

Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wallace, M., & Webber, L. (2017). *The disaster recovery handbook* (3rd ed.). AMACOM.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (6th ed.). Cengage Learning.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Crown.