The American Journal of Applied Sciences
ISSN 2689-0992 Volume 08 - 2026

Enterprise Secure Messaging for Critical Infrastructure: From Signal-Class Cryptography to National Cybersecurity Strategy

Artur Valiulin
Independent PhD Researcher Tashkent University of Information Technologies named after Muhammad al-Khwarizmi Tashkent, Uzbekistan

Received: 08 Apr 2026 | Received Revised Version: 30 Apr 2026 | Accepted: 24 May 2026 | Published: 05 June 2026

Volume 08 Issue 06 2026 | Crossref DOI: 10.37547/tajas/Volume08Issue06-18

Abstract

The rapid digital transformation of critical information infrastructure has significantly increased the strategic importance of secure enterprise communications. While public messaging platforms provide effective end-to-end encryption, they generally lack the governance, infrastructure sovereignty, and regulatory capabilities required by banking institutions, government agencies, and operators of critical information infrastructure. Consequently, secure communications should be considered not only as a cryptographic challenge but also as an essential component of organizational resilience and national cybersecurity.

This paper proposes the Enterprise Secure Communication Architecture (ESCA), a conceptual framework that extends modern Signal-class cryptography by integrating X3DH key agreement and the Double Ratchet protocol with enterprise governance, device-centric security, infrastructure sovereignty, operational resilience, and regulatory compliance. As a practical implementation of the proposed approach, the study examines the architecture of the PRIVATGRAM secure corporate messenger developed for highly regulated environments. The results demonstrate that enterprise secure messaging can evolve beyond encrypted communication into a strategic cybersecurity capability supporting organizational governance, protection of critical information infrastructure, digital sovereignty, and national cybersecurity objectives.

Keywords: Enterprise secure messaging, critical information infrastructure, cybersecurity strategy, Signal Protocol, X3DH, Double Ratchet, digital sovereignty, cyber resilience, enterprise security architecture, PRIVATGRAM.

Cite This Article: Artur Valiulin. (2026). Enterprise Secure Messaging for Critical Infrastructure: From Signal-Class Cryptography to National Cybersecurity Strategy. The American Journal of Applied Sciences, 8(06), 339–349. https://doi.org/10.37547/tajas/Volume08Issue06-18

1. Introduction

The rapid digital transformation of governments, financial institutions, healthcare organizations, industrial enterprises, telecommunications providers, transportation systems, and other operators of critical information infrastructure has fundamentally changed the role of enterprise communications. Instant messaging platforms have evolved from consumer applications into essential tools supporting operational coordination, incident response, distributed teamwork, and organizational decision-making. Consequently, communication systems have become an integral component of modern information infrastructure.

This transformation has simultaneously expanded the cybersecurity attack surface. Confidential operational information-including financial data, customer records, authentication credentials, engineering documentation, and emergency notifications-is routinely exchanged

through enterprise messaging platforms, making them attractive targets for cybercriminals, insider threats, advanced persistent threats (APTs), and state-sponsored actors. Compromise of communication channels may disrupt organizational resilience, operational continuity, and the delivery of critical services.

Although modern public messaging platforms implement strong end-to-end encryption, they are primarily designed for consumer use and generally lack the governance, device lifecycle management, infrastructure sovereignty, auditability, and regulatory capabilities required by banking institutions and operators of critical information infrastructure. Recent cybersecurity strategies adopted by the United States, the European Union, and the Republic of Uzbekistan increasingly emphasize resilience, secure-by-design principles, protection of critical infrastructure, and digital sovereignty, highlighting the strategic role of trusted enterprise communications.

To address these challenges, this research proposes the Enterprise Secure Communication Architecture (ESCA), a conceptual framework integrating Signal-class cryptography with enterprise governance, device-centric security, infrastructure sovereignty, operational resilience, and regulatory compliance. As a practical implementation of the proposed approach, the study examines the architecture of the PRIVATGRAM secure corporate messenger developed for banking institutions and critical information infrastructure. The objective of the research is to demonstrate that enterprise secure messaging can evolve from an encrypted communication service into a strategic component of modern cybersecurity architecture.

Enterprise Communications as a Cybersecurity Risk Layer

Traditionally, cybersecurity research has focused on protecting servers, databases, network infrastructure, endpoints, and cloud services. However, the growing dependence of organizations on digital collaboration has transformed enterprise communications into a critical cybersecurity layer directly affecting organizational resilience.

Modern messaging platforms support operational coordination, financial approvals, incident response, customer services, executive communications, and cross-organizational collaboration. Their confidentiality, integrity, and availability therefore directly influence the continuity of essential business processes.

Unlike traditional email systems, enterprise messaging applications provide real-time communication, multimedia collaboration, persistent synchronization across multiple devices, and rapid information exchange. While these capabilities improve operational efficiency, they also increase the attack surface available to adversaries. Compromise of communication channels may facilitate phishing, credential theft, social engineering, insider attacks, lateral movement, unauthorized disclosure of sensitive information, and disruption of incident-response activities.

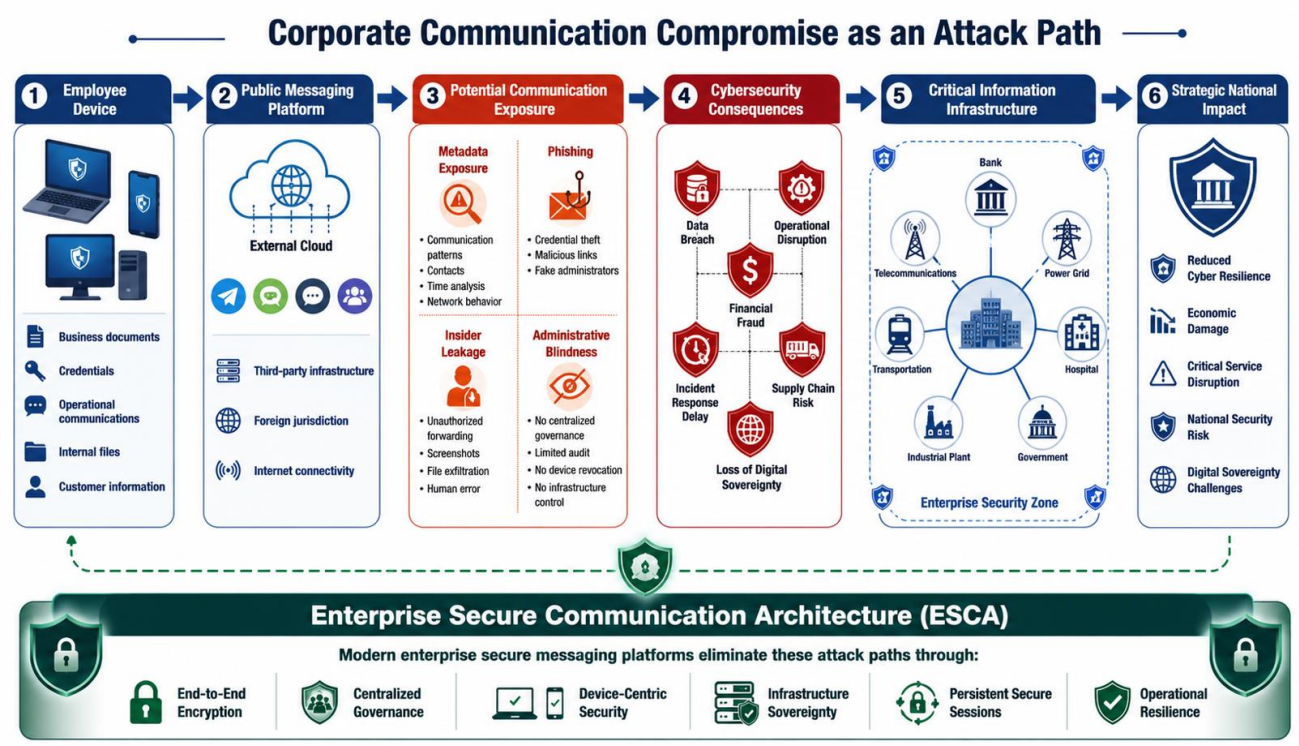
For operators of critical information infrastructure, these risks extend beyond individual organizations. Compromised communications may delay operational decision-making, interfere with coordinated incident response, prolong service recovery, and amplify the consequences of cyberattacks affecting essential public services.

These observations demonstrate that secure communications require more than cryptographic protection alone. Effective enterprise communication security must additionally incorporate administrative governance, device lifecycle management, infrastructure control, auditability, secure deployment models, and organizational policies supporting operational resilience.

Accordingly, enterprise secure messaging should be recognized as a dedicated cybersecurity layer within modern critical infrastructure protection architectures rather than simply another communication application.

Figure 1 illustrates how compromise of public messaging platforms may propagate cybersecurity risks from individual employee devices through organizational communication ecosystems to critical information infrastructure and ultimately influence national cyber resilience. The lower section introduces the proposed Enterprise Secure Communication Architecture (ESCA) as a conceptual approach for mitigating these risks through enterprise governance, infrastructure sovereignty, and secure communications.

Figure 1. Corporate Communication Compromise as an Attack Path



The cascading attack model presented in Figure 1 explains why recent national cybersecurity strategies increasingly recognize secure enterprise communications as an essential element of organizational resilience and critical infrastructure protection. The following section therefore examines the regulatory approaches adopted in the United States, the European Union, and the Republic of Uzbekistan.

LEGAL AND STRATEGIC CYBERSECURITY FRAMEWORKS FOR SECURE ENTERPRISE COMMUNICATIONS

The growing dependence of critical information infrastructure on digital communications has fundamentally changed national approaches to cybersecurity. Secure communication platforms are increasingly recognized not merely as technical tools but as strategic assets supporting operational resilience, continuity of essential services, digital sovereignty, and national security. Although enterprise messaging systems are rarely regulated directly, modern cybersecurity legislation increasingly incorporates communication security through broader requirements for critical infrastructure protection, organizational governance, and cyber resilience.

1. United States

The United States promotes a resilience-oriented cybersecurity model through the National Cybersecurity Strategy (2023), Executive Order 14028, and the NIST Cybersecurity Framework (CSF) 2.0. These documents emphasize secure-by-design principles, organizational governance, software supply-chain security, operational continuity, and protection of critical infrastructure. The introduction of the Govern function in NIST CSF 2.0 further highlights that enterprise communications should support centralized administration, policy enforcement, auditability, and device lifecycle management rather than encryption alone.

2. European Union

The European Union has adopted a similar approach through the NIS2 Directive and the Digital Operational Resilience Act (DORA). These regulatory frameworks require operators of essential services and financial institutions to implement comprehensive cyber risk management, operational resilience, incident reporting, governance mechanisms, and secure ICT operations. Consequently, secure enterprise communications are increasingly regarded as an integral component of organizational resilience and regulatory compliance.

3. Republic of Uzbekistan

Uzbekistan has significantly strengthened its national cybersecurity framework through the Law "On Cybersecurity", Presidential Resolution No. PP-167 on the protection of critical information infrastructure, and the recently approved Cybersecurity Strategy of the Republic of Uzbekistan, which establishes long-term priorities for strengthening cyber resilience, protecting critical infrastructure, reducing cyber risks, developing domestic cybersecurity technologies, and enhancing digital sovereignty. These strategic priorities demonstrate that secure enterprise communications are becoming an important element of the national cybersecurity architecture rather than simply communication software.

4. Comparative Analysis

Despite differences in legal systems, the cybersecurity policies of the United States, the European Union, and the Republic of Uzbekistan demonstrate a clear convergence around several strategic priorities: protection of critical information infrastructure; cyber resilience and operational continuity; organizational governance and accountability; digital sovereignty; secure digital transformation.

These common objectives provide a strong foundation for developing enterprise communication architectures that integrate advanced cryptography with centralized governance, infrastructure sovereignty, operational resilience, and regulatory compliance.

Table 1. Strategic Cybersecurity Priorities Relevant to Enterprise Secure Communications

Jurisdiction	Legal / Strategic Source	Main Requirement	Relevance to Secure Communications
United States	National Cybersecurity Strategy (2023); Executive Order 14028; NIST Cybersecurity Framework (CSF 2.0)	Cyber resilience; secure-by-design; organizational governance; critical infrastructure protection	Secure communications integrated with centralized governance, strong authentication, incident response, and operational resilience
European Union	NIS2 Directive (EU 2022/2555); Digital Operational Resilience Act (DORA, EU 2022/2554)	Cyber risk management; operational resilience; ICT governance; protection of essential entities	Enterprise communication platforms supporting encrypted communications, auditability, business continuity, and regulatory compliance
Republic of Uzbekistan	Law "On Cybersecurity"; Cybersecurity Strategy of the Republic of Uzbekistan; Presidential Resolution № PP-167	Protection of critical information infrastructure; cyber resilience; digital sovereignty; development of national cybersecurity capabilities	Sovereign enterprise communication platforms supporting secure communications, infrastructure control, regulatory compliance, and reduced dependence on foreign ecosystems

As summarized in Table 1, modern cybersecurity strategies increasingly treat secure enterprise communications as a strategic capability supporting organizational resilience and protection of critical information infrastructure. These international trends provide the conceptual basis for the Enterprise Secure Communication Architecture (ESCA) proposed in this research.

FROM SIGNAL-CLASS CRYPTOGRAPHY TO ENTERPRISE SECURITY ARCHITECTURE

Modern Signal-class cryptographic protocols provide a high level of protection for digital communications through X3DH asynchronous key agreement and the Double Ratchet algorithm, ensuring end-to-end encryption, forward secrecy, post-compromise security,

and continuous key evolution. However, organizations operating critical information infrastructure require substantially more than cryptographic protection, including governance, infrastructure control, operational resilience, and regulatory compliance.

To address these requirements, this research proposes the Enterprise Secure Communication Architecture (ESCA), a conceptual framework integrating cryptographic assurance with enterprise governance, infrastructure sovereignty, operational resilience, and strategic cybersecurity alignment. Unlike conventional secure messaging applications focused primarily on confidentiality, ESCA positions secure communications as a strategic organizational capability supporting enterprise cybersecurity and national cyber resilience.

Figure 2. Enterprise Secure Communication Architecture (ESCA)

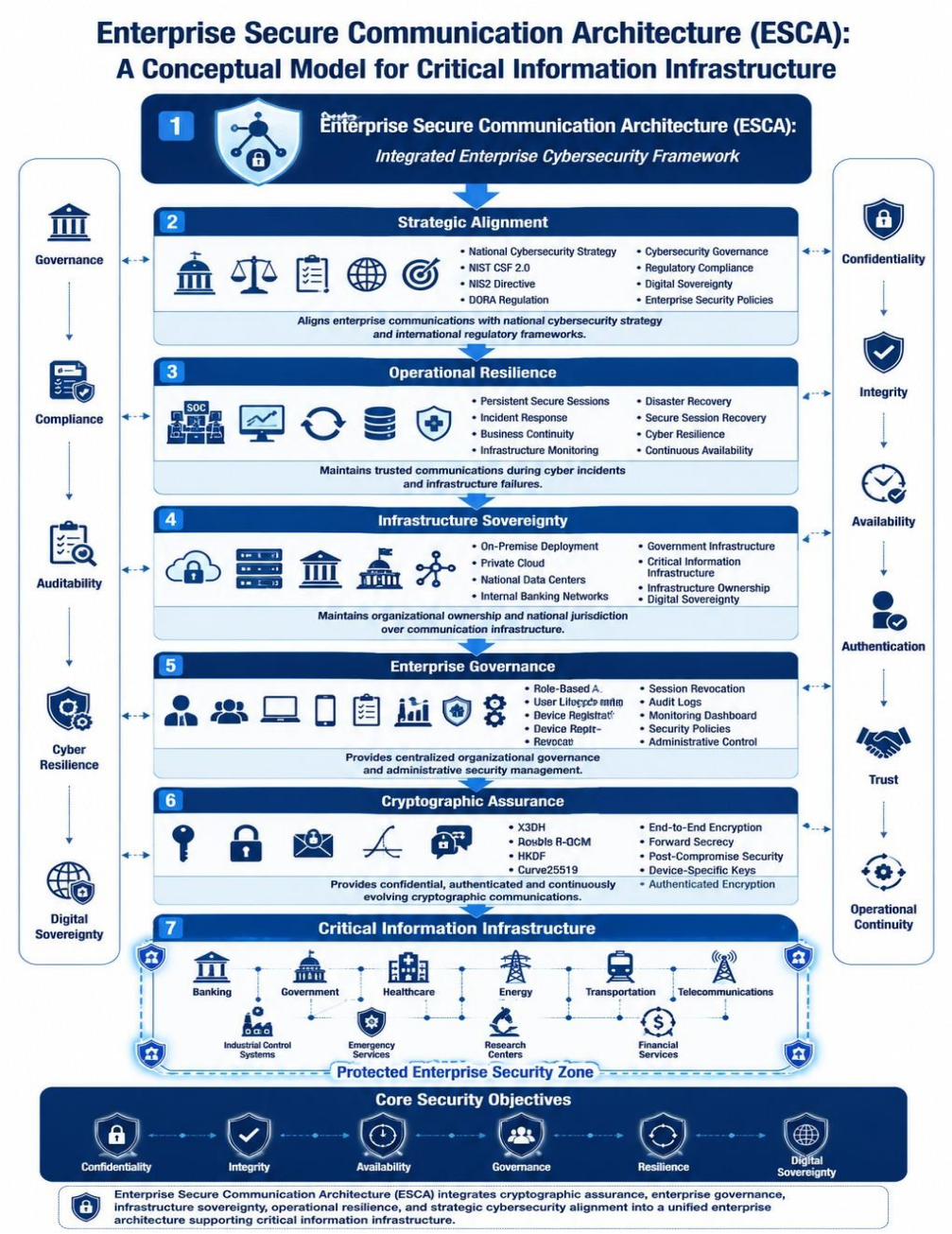


Figure 2 illustrates the proposed ESCA model, extending traditional Signal-class secure messaging into a unified enterprise cybersecurity architecture.

1. Enterprise Requirements Beyond Consumer Messaging

Consumer messaging platforms primarily protect communication confidentiality between individual users, whereas enterprise environments additionally require centralized governance, user and device lifecycle management, role-based access control, auditability, policy enforcement, infrastructure ownership, and operational continuity. Operators of critical information infrastructure also require selective device revocation, secure recovery procedures, and resilient communications capable of supporting incident response and business continuity.

2. Enterprise Secure Communication Architecture (ESCA)

The proposed ESCA framework consists of four complementary domains:

Cryptographic Assurance - X3DH, Double Ratchet, AES-256-GCM, HKDF, and Curve25519.

Enterprise Governance - centralized administration, role-based access control, device and session management, security policies, and audit logging.

Infrastructure Sovereignty - secure deployment within organizational data centers, private clouds, and sovereign infrastructures.

Operational Resilience - secure recovery, continuous monitoring, incident response, and communication continuity.

Together, these domains transform secure messaging into an integrated enterprise cybersecurity architecture.

3. Enterprise Security Requirements for Critical Information Infrastructure

Operators of critical information infrastructure require communication platforms capable of ensuring confidentiality, integrity, availability, auditability, infrastructure sovereignty, protected metadata management, secure recovery, and operational resilience. Extending Signal-class cryptography with enterprise governance mechanisms therefore provides a practical foundation for secure communication platforms supporting both organizational cybersecurity and national cyber resilience.

Table 3. Consumer Messenger vs. Enterprise Secure Messenger

Criterion	Consumer Messenger	Enterprise Secure Messenger	Strategic Cybersecurity Relevance
Primary Purpose	Personal communi-cation	Secure organizational communications	Supports mission-critical operations
Deployment Model	Public cloud infrastructure	On-premise, private cloud, sovereign infrastructure	Reduces dependency on external service providers
Administrative Governance	Limited	Centralized administration	Enables organizational control and accountability
User Lifecycle Management	Minimal	Centralized registration, modification and revocation	Supports secure personnel management
Device Management	Basic multi-device support	Device registration, authorization and revocation	Limits compromise to individual endpoints
Cryptographic Protection	End-to-end encryption	End-to-end encryption with enterprise governance	Preserves confidentiality while supporting operational control
Session Management	User-oriented	Device-aware secure session management	Improves resilience against compromised devices
Auditability	Limited	Comprehensive audit logs and security monitoring	Supports regulatory compliance and incident investigation

Metadata Management	Provider controlled	Organization controlled	Reduces information exposure and improves privacy
Infrastructure Ownership	Foreign or third-party providers	Organization-owned infrastructure	Strengthens digital sovereignty
Regulatory Compliance	General consumer privacy standards	Banking, governmental and critical infrastructure requirements	Facilitates compliance with sector-specific regulations
Operational Resilience	Service availability depends on provider	Controlled continuity and recovery mechanisms	Supports uninterrupted operation of critical services
Incident Response	User-driven	Centralized administrative response	Enables coordinated cybersecurity operations
Strategic Role	Communica-tion service	Component of enterprise cybersecurity architecture	Contributes to national cyber resilience
Scientific Concept	Not defined	ESCA	Provides a conceptual architecture for enterprise cybersecurity

Table 3 summarizes the principal differences between consumer and enterprise messaging platforms, demonstrating that enterprise secure messaging extends conventional end-to-end encryption through governance, operational resilience, infrastructure sovereignty, and regulatory compliance, as represented by the proposed Enterprise Secure Communication Architecture (ESCA).

PRIVATGRAM as a Practical Implementation of Enterprise Secure Messaging

The proposed Enterprise Secure Communication Architecture (ESCA) has been practically implemented through the development of the PRIVATGRAM secure corporate messenger intended for banking institutions and operators of critical information infrastructure. Rather than representing a conventional enterprise messaging application, PRIVATGRAM demonstrates how the conceptual principles of ESCA can be translated into a deployable communication platform integrating cryptographic protection, enterprise governance, and operational resilience.

Unlike consumer-oriented messaging platforms, PRIVATGRAM was designed according to enterprise security principles where secure communications constitute one component of a broader organizational cybersecurity architecture. The platform combines modern Signal-class cryptography with centralized administration, device-centric security, infrastructure sovereignty, and operational governance.

1. Enterprise-Oriented Architecture

The platform follows a multilayer architecture consisting of client applications, administrative services, secure communication servers, and protected infrastructure components.

Administrative functions-including user registration, role management, device authorization, policy enforcement, audit logging, and session revocation—operate independently from encrypted message processing, improving organizational governance while reducing the attack surface associated with privileged operations.

All cryptographic operations are performed locally on client devices. Private keys never leave endpoint devices, while the server infrastructure is limited to authenticated user management, encrypted message routing, temporary ciphertext storage, file delivery, notification services, and synchronization of public cryptographic material. Consequently, server compromise does not expose plaintext communications.

2. Enterprise Extension of Signal-Class Cryptography

The cryptographic subsystem extends the classical Signal architecture using X3DH asynchronous key agreement, Double Ratchet session evolution, AES-256-GCM authenticated encryption, HKDF-based key derivation, and Curve25519 elliptic-curve cryptography.

Beyond conventional Signal implementations, the proposed platform incorporates several enterprise-oriented mechanisms, including persistent storage of Double Ratchet session state, device-centric session management, selective device revocation, and device-specific ciphertext isolation. These mechanisms strengthen operational continuity, administrative control, and cyber resilience while preserving the security guarantees of modern end-to-end encryption.

3. Enterprise Governance and Operational Resilience

The conducted research demonstrates that secure enterprise communications cannot rely exclusively on cryptographic protection. Effective communication security additionally requires centralized governance, user and device lifecycle management, auditability, infrastructure control, secure deployment, and coordinated incident response.

Within the proposed architecture, these organizational mechanisms complement modern Signal-class cryptography, transforming secure messaging from a communication application into an enterprise cybersecurity capability supporting operational resilience, regulatory compliance, and protection of critical information infrastructure.

The PRIVATGRAM platform therefore represents a practical implementation of the proposed Enterprise Secure Communication Architecture (ESCA), demonstrating how secure communications can simultaneously satisfy advanced cryptographic requirements, enterprise governance, infrastructure sovereignty, and resilience objectives.

ENTERPRISE SECURE MESSAGING AS A COMPONENT OF NATIONAL CYBERSECURITY STRATEGY

The conducted research demonstrates that enterprise secure messaging should be regarded not only as an organizational communication platform but also as a strategic component of national cybersecurity architecture. Modern cyberattacks increasingly target communication and coordination processes rather than isolated information systems. Consequently, protecting enterprise communications directly contributes to organizational resilience, continuity of essential services, and national cybersecurity.

The proposed Enterprise Secure Communication Architecture (ESCA) provides a conceptual framework linking modern cryptographic protection with enterprise governance, operational resilience, infrastructure sovereignty, and regulatory compliance. Within this model, secure communications evolve from encrypted messaging applications into enterprise cybersecurity capabilities supporting organizational and national resilience.

1. Alignment with International Cybersecurity Strategies

Despite differences in legal systems and implementation approaches, the cybersecurity strategies of the United States, the European Union, and the Republic of Uzbekistan demonstrate a common transition toward resilience-oriented cybersecurity models. Modern regulatory frameworks consistently emphasize critical infrastructure protection, organizational governance, operational continuity, digital sovereignty, and secure-by-design principles.

Within this strategic context, enterprise secure messaging supports trusted operational coordination, secure incident response, administrative governance, and resilient communication infrastructure, directly contributing to national cybersecurity objectives.

2. Integration with the NIST Cybersecurity Framework

The proposed ESCA model naturally aligns with the governance-oriented approach introduced by NIST Cybersecurity Framework (CSF) 2.0. Through centralized administration, cryptographic protection, device lifecycle management, auditability, and secure recovery mechanisms, enterprise secure messaging supports all six core NIST cybersecurity functions.

Table 2. Mapping Secure Messaging Functions to NIST CSF 2.0

NIST Function	Required Capability	PRIVATGRAM / Enterprise Messenger Implementation
Govern	Cybersecurity governance, policy control, roles and responsibilities, risk management oversight	Centralized administration, role-based access control, security policy management, administrator accountability, organizational control over users and devices
Identify	Identification of assets, users, devices, communication channels, and organizational dependencies	User registry, device registry, session inventory, controlled user lifecycle management, classification of communication assets
Protect	Protection of data, identities, access, systems, and communication channels	End-to-end encryption, X3DH key agreement, Double Ratchet session evolution, TLS transport protection, device-level session isolation, authenticated access
Detect	Detection of anomalies, unauthorized activity, compromised devices, and security-relevant events	Audit logs, monitoring dashboard, device status tracking, session activity records, security event visibility without access to plaintext content
Respond	Incident response, containment, access revocation, and operational coordination	Session revocation, device blocking, administrative intervention, secure incident-response communications, isolation of compromised endpoints
Recover	Restoration of secure operations after incidents or failures	Persistent ratchet-state recovery, secure session restoration, infrastructure continuity, re-registration of trusted devices, restoration of protected communications

As summarized in Table 2, enterprise secure messaging contributes not only to information protection but also to governance, asset management, threat detection, coordinated incident response, and secure recovery. This demonstrates that modern communication platforms can function as integral components of internationally recognized cybersecurity management frameworks.

3. Strategic Relevance for Critical Information Infrastructure

The rapid digitalization of banking, government, healthcare, telecommunications, transportation, and industrial sectors has significantly increased the strategic importance of trusted enterprise communications. Dependence on externally controlled communication ecosystems introduces additional cybersecurity, operational, and geopolitical risks, particularly for operators of critical information infrastructure.

Enterprise communication platforms capable of sovereign deployment, centralized governance, strong cryptographic protection, and resilient operation therefore contribute to digital sovereignty while supporting regulatory compliance, operational continuity, and protection of critical services.

4. Enterprise Secure Communication Architecture as a Strategic Cybersecurity Model

Building upon these strategic requirements, the proposed Enterprise Secure Communication Architecture (ESCA) provides a conceptual model that integrates secure communications into modern cybersecurity governance. ESCA combines five complementary domains-Cryptographic Assurance, Enterprise Governance, Infrastructure Sovereignty, Operational Resilience, and Strategic Alignment-into a unified enterprise cybersecurity architecture.

Rather than treating secure messaging solely as an encrypted communication service, ESCA positions enterprise communications as a strategic cybersecurity capability supporting governance, regulatory

compliance, operational resilience, and protection of critical information infrastructure.

The practical implementation of these architectural principles through the PRIVATGRAM platform demonstrates how modern Signal-class cryptography can be extended with enterprise administrative mechanisms to support long-term organizational resilience and national cybersecurity objectives.

2. Conclusion

The rapid digitalization of critical information infrastructure has transformed enterprise communications into a strategic component of organizational cybersecurity. Modern cybersecurity strategies adopted by the United States, the European Union, and the Republic of Uzbekistan increasingly emphasize resilience, governance, infrastructure sovereignty, and protection of critical infrastructure, demonstrating that secure communications extend far beyond conventional encrypted messaging.

This research proposed the Enterprise Secure Communication Architecture (ESCA) as a conceptual framework integrating Signal-class cryptography with enterprise governance, infrastructure sovereignty, operational resilience, and strategic cybersecurity alignment. Unlike conventional secure messaging architectures, ESCA positions secure communications as an integral component of enterprise cybersecurity and protection of critical information infrastructure.

As a practical implementation of the proposed concept, the study examined the PRIVATGRAM secure corporate messenger, demonstrating that modern cryptographic mechanisms-including X3DH, Double Ratchet, AES-256-GCM, HKDF, and Curve25519-can be effectively combined with enterprise administrative mechanisms to support organizational resilience and regulatory compliance.

The principal scientific contribution of this research is the development of the Enterprise Secure Communication Architecture (ESCA) as a conceptual model extending secure messaging into a comprehensive enterprise cybersecurity architecture. The proposed framework may serve as a methodological foundation for future research on secure enterprise communications, cyber resilience, digital sovereignty, and protection of critical information infrastructure.

References

1. European Parliament and Council of the European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). https://eur-lex.europa.eu/
2. European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (Digital Operational Resilience Act – DORA). https://eur-lex.europa.eu/
3. Krawczyk, H., & Eronen, P. (2010). HMAC-based Extract-and-Expand Key Derivation Function (HKDF) (RFC 5869). Internet Engineering Task Force. https://doi.org/10.17487/RFC5869
4. Langley, A., Hamburg, M., & Turner, S. (2016). Elliptic Curves for Security (RFC 7748). Internet Engineering Task Force. https://doi.org/10.17487/RFC7748
5. Marlinspike, M., & Perrin, T. (2016). The X3DH Key Agreement Protocol. Signal Foundation. https://signal.org/docs/specifications/x3dh/
6. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
7. Odebade, A. T., & Benkhelifa, E. (2023). A Comparative Study of National Cyber Security Strategies of Ten Nations. arXiv. https://arxiv.org/abs/2303.13938
8. Perrin, T., & Marlinspike, M. (2016). The Double Ratchet Algorithm. Signal Foundation. https://signal.org/docs/specifications/doubleratchet/
9. Republic of Uzbekistan. (2022). Law of the Republic of Uzbekistan No. ZRU-764 "On Cybersecurity".
10. Republic of Uzbekistan. (2025). Cybersecurity Strategy of the Republic of Uzbekistan. https://lex.uz/ru/docs/8079279
11. Republic of Uzbekistan. (2023). Presidential Resolution No. PP-167 "On Measures to Further Improve the Cybersecurity System of Critical Information Infrastructure Facilities".
12. The White House. (2023). National Cybersecurity Strategy. https://www.whitehouse.gov/
13. Dworkin. M. (2007). Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC (NIST Special Publication 800-38D). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-

38D
14. Valiulin. A. (2026). Architecture of the PRIVATGRAM Secure Corporate Messenger for Critical Infrastructure Based on X3DH and Double Ratchet Protocols. The American Journal of Engineering and Technology, 8(05), 159–164. https://doi.org/10.37547/tajet/Volume08Issue05-15