The Rise Of Cybercrime: Challenges For Criminal Law In The Digital Age

Dr. Surbhi Dubey Dadhich

Specialization in criminal law Email id: surbhi15dubey@gmail.com

Keywords:
Cybercrime, digital evidence, jurisdiction, attribution, encryption, privacy, ransomware, cross-border data, corporate liability, international cooperation.

Abstract
Cybercrime has evolved from fringe misconduct to a pervasive, economically consequential, and geopolitically sensitive threat. Offenses now range from phishing and ransomware to industrial espionage, cryptojacking, and AI-powered fraud—blurring the line between traditional and technology-enabled crimes. This paper surveys the principal challenges that cybercrime poses to criminal law and criminal procedure, focusing on jurisdiction, attribution, digital evidence, encryption, privacy, corporate responsibility, and international cooperation. It highlights doctrinal gaps—such as outdated offense definitions and insufficient liability frameworks for platform intermediaries—as well as procedural obstacles like cross-border data access and chain-of-custody management for volatile evidence. The analysis also assesses the interplay of rights and security, including risks of overbroad surveillance and the need for proportionate investigative powers. Finally, the paper proposes policy and legal reforms: technology-neutral drafting, clearer extraterritoriality rules, safeguards for cross-border data requests, calibrated encryption approaches, victim-centric remedies, and better resourcing for cyber units. The conclusion emphasizes a balanced, multi-stakeholder strategy: modernized substantive law and procedure, stronger international instruments, and operational collaboration among law enforcement, industry, and civil society.

INTRODUCTION

The last decade and a half has seen cybercrime evolve from a niche policing problem into a pervasive, economically and socially disruptive phenomenon that tests the limits of traditional criminal law. Rapid digitalisation, the proliferation of cloud services and the rise of commodified cybercrime tools (malware-as-a-service, ransomware kits, botnets-for-hire) have expanded both the scale and sophistication of offending. International agencies and threat-monitoring bodies document steady increases in phishing, ransomware and data-theft incidents and emphasise how transnationality and speed complicate investigation and prosecution. These empirical trendlines—reported by organisations such as ENISA and UNODC—frame cybercrime as a systemic, cross-border challenge rather than merely an episodic technical nuisance.

Scholarly work since 2010 has tracked and theorised these changes from multiple angles. Majid Yar's Cybercrime and Society (and its later editions) situates cybercrime within broader social and criminological frameworks, arguing that technological change reshapes offending patterns and normative responses. Yar (with Steinmetz in later editions) explores how old categories—property crime, fraud, organised crime—are reconfigured in digital settings, pressing the law to adapt conceptual categories as well as practical responses. Likewise, Susan W. Brenner's influential text Cybercrime: Criminal Threats from Cyberspace maps the diversity of cyber-enabled and cyber-dependent offences and foregrounds the tension between

enforcement needs and civil liberties. Together these works provide foundational syntheses that scholars and policymakers repeatedly return to when assessing legal adequacy.

A persistent theme in the literature is the mismatch between legal doctrines developed for territorially-bounded wrongdoing and crimes that effortlessly cross jurisdictions or hide behind anonymising infrastructure. David S. Wall and collaborators have emphasised the distributed, often "disorganised" structure of contemporary cybercriminal networks, and the way cloud architectures and digital intermediaries complicate who is a victim, where harm occurs, and which state has investigative primacy. This fragmentation undermines traditional models of evidence-gathering, custody, and criminal process, generating calls for international cooperation that are often hampered by varying legal standards and resource gaps across states.

Legal scholars have also highlighted doctrinal vagueness and prosecutorial overreach as central challenges. Orin S. Kerr's work on computer-trespass doctrines and the interpretation of statutes such as the United States' Computer Fraud and Abuse Act (CFAA) illustrates how uncertain statutory language can criminalise everyday online behaviour or, conversely, leave serious intrusions insufficiently proscribed. Debates around the CFAA and analogous statutes demonstrate the double risk: laws that are too broad threaten civil liberties and suffer constitutional challenges, whereas laws that are too narrow or poorly aligned with technology permit impunity for novel harms.

Between 2010 and 2024 the literature has therefore clustered around several practical and normative priorities: updating legal definitions (what counts as 'access', 'interference', or 'theft' in digital contexts); designing effective cross-border investigative frameworks and mutual legal assistance; balancing privacy and surveillance in cyber-investigations; and strengthening capacity among law enforcement, prosecutors and judiciaries. Empirical and policy reports (ENISA, UNODC) have complemented doctrinal scholarship (Yar, Brenner, Kerr, Wall) by documenting emergent threats—ransomware monetisation, supply-chain attacks, deepfakes—and the institutional shortfalls in responding to them.

This study builds on that multidisciplinary literature to examine how criminal law has responded to the digital turn: where statutory and prosecutorial practices have succeeded, where they have produced harms or inconsistency, and what doctrinal and institutional reforms are most plausible given political and technical constraints. By synthesising empirical threat data with doctrinal critique and comparative perspectives from the 2010–2024 literature, the paper seeks to identify realistic reform pathways that protect rights while enhancing the capacity to deter and punish serious cyber offending.

EVOLVING CYBERCRIME LANDSCAPE

The landscape of cybercrime has undergone a profound transformation over the past two decades, driven by rapid technological advancements, the proliferation of digital devices, and the globalization of internet access. Cybercrime has evolved from isolated acts of digital vandalism into complex, organized, and transnational operations that challenge traditional notions of jurisdiction, law enforcement, and criminal accountability.

In the early days of the internet, cybercrime largely consisted of relatively unsophisticated activities such as website defacement, email phishing, and virus dissemination by individual hackers seeking notoriety. Today, however, cybercriminals operate with professional precision, leveraging advanced tools such as ransomware, distributed denial-of-service (DDoS) attacks, and cryptocurrency laundering schemes. The emergence of the "dark web" has provided an illicit marketplace for stolen data, hacking tools, and criminal services, allowing even inexperienced actors to commit high-impact crimes with minimal technical expertise.

Another defining feature of the evolving cybercrime landscape is the growing role of state-sponsored and politically motivated cyberattacks. Nation-state actors engage in espionage, sabotage, and disinformation campaigns, blurring the line between conventional crime and acts of cyber warfare. This trend heightens global security risks and exposes critical infrastructure—such as power grids, healthcare systems, and financial networks—to unprecedented vulnerabilities.

Technological innovation continues to create new opportunities for malicious exploitation. The rise of cloud computing, artificial intelligence (AI), and the Internet of Things (IoT) has expanded the attack surface dramatically. Cybercriminals now exploit insecure IoT devices to build massive botnets, use AI to craft convincing deepfakes or automate phishing, and target sensitive data stored in inadequately protected cloud environments. These innovations have increased both the scale and the anonymity of cybercrime, making detection and attribution significantly more difficult.

The borderless nature of cyberspace further complicates enforcement efforts. Offenders can launch attacks from jurisdictions with weak legal frameworks or limited investigative capacity, evading prosecution while inflicting damage worldwide. As a result, traditional criminal law—designed for geographically defined offenses—struggles to address crimes committed in decentralized, anonymous digital environments.

The evolving cybercrime landscape underscores an urgent need for adaptive legal mechanisms, stronger international cooperation, and investment in cybersecurity capabilities. Criminal law must evolve alongside technology, incorporating updated definitions of cyber offenses, modernized evidence collection procedures, and harmonized cross-border enforcement strategies. Without these reforms, cybercriminals will continue to exploit legal gaps and technological blind spots, posing escalating threats to individuals, organizations, and national security alike.

CORE CHALLENGES FOR CRIMINAL LAW

The rapid expansion of digital technology has transformed how crimes are committed, investigated, and prosecuted, presenting unprecedented challenges for criminal law. Unlike traditional crimes, cybercrimes transcend geographic borders, involve complex technical mechanisms, and evolve at a pace far exceeding the ability of legal systems to adapt. These characteristics create fundamental difficulties in maintaining effective deterrence, fair enforcement, and consistent application of justice.

1. Jurisdictional Conflicts: Cybercrimes frequently cross national boundaries, making it unclear which country's laws apply and how offenders can be apprehended. Criminal law has historically been rooted in territorial sovereignty, but digital networks ignore such boundaries. This creates hurdles in extradition, cooperation, and enforcement, often leaving perpetrators beyond the reach of local courts.

2. Outdated Legal Frameworks: Many criminal statutes were written for a pre-digital era and lack provisions for offenses like ransomware attacks, cryptocurrency-based laundering, or large-scale data theft. Legislators struggle to draft laws that are both technologically relevant and flexible enough to address emerging threats without becoming obsolete within a few years.

3. Evidentiary and Investigative Barriers: Collecting and preserving digital evidence is technically demanding. Data can be encrypted, remotely stored, or deliberately wiped within seconds. Moreover, the need to balance privacy rights with surveillance measures complicates investigations. Courts often face uncertainty over admissibility, authenticity, and chain of custody for electronic evidence.

4. Attribution and Anonymity: Unlike physical crimes where perpetrators leave tangible traces, cybercrimes can be carried out anonymously using VPNs, proxies, or botnets. Determining who is responsible is often speculative, leading to difficulties in prosecution and an increased risk of wrongful attribution.

5. International Cooperation and Harmonization: Cybercrime control requires collaboration among law enforcement agencies worldwide, yet varying legal systems, political interests, and resource disparities hinder cooperation. Even when treaties like the Budapest Convention exist, not all states are signatories, and enforcement standards remain inconsistent.

6. Ethical and Human Rights Concerns: Efforts to combat cybercrime often involve expanded surveillance, data retention, and stricter regulatory controls, raising questions about civil liberties. Balancing state security needs with individual freedoms remains a critical challenge for lawmakers.

In sum, the rise of cybercrime forces criminal law to evolve rapidly. Policymakers must modernize statutes, develop specialized expertise, and enhance international frameworks while safeguarding due process and human rights. The digital age demands a criminal justice system that is both technologically competent and globally coordinated to effectively address these complex threats.

ENCRYPTION, PRIVACY, AND PROPORTIONALITY

Encryption has emerged as both a shield and a challenge in the digital age. It secures communications, financial transactions, and personal data against unauthorized access, forming a cornerstone of individual privacy and digital trust. However, the same technology that protects citizens also frustrates law enforcement agencies investigating cybercrime. Criminals employ end-to-end encryption to conceal illicit activities ranging from financial fraud to cyber-espionage, making lawful interception increasingly complex. This dual character of encryption lies at the heart of the current policy and legal debate.

The principle of privacy, recognized under international human rights law, demands that governments avoid arbitrary or intrusive surveillance. In cyberspace, where vast quantities of sensitive information flow continuously, maintaining privacy is essential to prevent abuse, identity theft, and chilling effects on free expression. Yet privacy cannot be absolute; criminal law must ensure that serious cyber offenses are investigated effectively. This tension calls for a framework based on **proportionality**—ensuring that any restriction on privacy rights is justified, targeted, and limited to what is strictly necessary.

Proportionality requires a careful balance between competing interests. Blanket decryption mandates or "backdoors" risk weakening cybersecurity for all users, exposing systems to hackers and hostile actors. Conversely, granting unbreakable privacy to malicious actors may paralyze law enforcement efforts. Courts and legislatures are grappling with where to draw the line: judicially authorized access, robust oversight mechanisms, and transparency requirements are often proposed as safeguards to prevent misuse of surveillance powers.

Furthermore, technological and legal solutions must evolve together. Innovations such as secure enclaves, split-key escrow systems, and privacy-preserving investigation techniques illustrate attempts to reconcile investigative needs with strong encryption. However, such measures are not foolproof and require clear statutory authority and international cooperation, given that cybercrime transcends borders.

Ultimately, the debate over encryption, privacy, and proportionality reflects a deeper struggle to adapt criminal law to the realities of the digital age. Overbroad surveillance powers may erode public trust in government and technology alike, while excessive resistance to lawful access may embolden cybercriminal networks. Achieving a workable equilibrium demands multi-stakeholder dialogue—among lawmakers, technologists, civil society, and law enforcement—to craft rules that preserve both security and fundamental freedoms. In this way, encryption is not treated solely as an obstacle, but as a tool whose responsible use, guided by proportional legal frameworks, strengthens both individual rights and collective safety.

CORPORATE AND PLATFORM LIABILITY

The rapid growth of digital technologies has transformed corporations and online platforms into critical intermediaries for communication, commerce, and information exchange. However, this central role has also made them key nodes in the proliferation of cybercrime. Corporate and platform liability refers to the legal responsibility of organizations whose services, infrastructure, or policies enable—or fail to prevent—criminal activities in cyberspace. As cybercrime becomes more sophisticated, questions arise regarding how far liability should extend beyond individual perpetrators to encompass the businesses that host, facilitate, or indirectly profit from malicious conduct.

Corporate responsibility in cybercrime prevention is no longer limited to maintaining internal cybersecurity. Companies must ensure that their networks are not exploited for illegal data harvesting,

ransomware deployment, or fraud schemes. Financial institutions, cloud service providers, and e-commerce firms are increasingly required to adopt robust monitoring systems, mandatory breach reporting mechanisms, and transparent risk-management practices. Failure to meet these obligations can lead to regulatory penalties, civil lawsuits, and reputational damage.

Platform liability presents even more complex legal challenges. Social media companies, online marketplaces, and communication platforms often claim that they are mere conduits for user-generated content, shielded by "safe harbor" provisions under laws like the U.S. Communications Decency Act (Section 230) or the EU's e-Commerce Directive. Yet these protections are under scrutiny as platforms are repeatedly exploited for phishing schemes, malware distribution, human trafficking, and terrorist propaganda. Regulators and courts increasingly debate whether platforms should bear partial responsibility for failing to remove harmful content, inadequately verifying users, or profiting from illegal transactions conducted through their services.

The global nature of cybercrime further complicates enforcement. A platform headquartered in one jurisdiction may host content or facilitate crimes affecting victims worldwide. Divergent national laws on intermediary liability create uncertainty, while overly strict rules risk stifling innovation and free speech. The EU's Digital Services Act (2022) and India's Information Technology (Intermediary Guidelines) Rules (2021) illustrate emerging regulatory efforts to impose "due diligence" obligations without turning platforms into full-scale law enforcement agencies.

In sum, the rise of cybercrime demands a careful recalibration of corporate and platform liability. Legal frameworks must balance competing interests: protecting consumers and national security, encouraging innovation, and upholding fundamental freedoms. Future reforms are likely to focus on shared responsibility models, where corporations and platforms must proactively detect, report, and mitigate cybercrime in collaboration with regulators, without assuming unlimited liability for every unlawful act online.

INTERNATIONAL COOPERATION AND HARMONIZATION

The borderless nature of cyberspace has transformed crime into a global phenomenon. Cybercriminals can operate from any jurisdiction, targeting victims and infrastructure in multiple countries simultaneously. This transnational character makes international cooperation and harmonization of laws essential to effectively investigate, prosecute, and deter cybercrime. Traditional legal frameworks—designed for geographically confined offenses—are insufficient in dealing with crimes such as ransomware attacks, phishing, identity theft, and state-sponsored hacking campaigns.

International cooperation primarily involves information sharing, joint investigations, extradition agreements, and capacity building. Law enforcement agencies must coordinate through platforms such as INTERPOL's Cybercrime Directorate or the European Union Agency for Cybersecurity (ENISA) to track perpetrators who exploit jurisdictional gaps. Timely exchange of digital evidence—often volatile and easily altered—is critical, yet many legal systems lack compatible procedures for obtaining or admitting such evidence across borders. Mutual Legal Assistance Treaties (MLATs), though valuable, are frequently criticized for being slow and bureaucratic, creating safe havens for cybercriminals.

Harmonization of legal frameworks addresses disparities in how countries define and penalize cyber offenses. For example, what constitutes "unauthorized access" or "critical infrastructure sabotage" may vary significantly between jurisdictions, creating obstacles for cross-border prosecutions. Instruments such as the **Budapest Convention on Cybercrime (2001)** represent major steps toward standardization by encouraging signatory states to adopt common definitions, procedural tools, and safeguards for digital investigations. However, not all major cyber powers are signatories, reflecting geopolitical tensions and differing views on internet governance and sovereignty.

Moreover, harmonization is not limited to criminal statutes; it extends to digital evidence handling, data protection standards, and private sector collaboration**.** Global corporations, internet service providers, and

cloud platforms play pivotal roles in investigations. Aligning legal obligations regarding data disclosure or breach reporting ensures investigators can obtain critical information without conflicting with privacy or trade laws.

Challenges persist. National security concerns, varying human-rights standards, and competition over technological dominance can hinder consensus. Some states favor strict state control of cyberspace, while others emphasize individual freedoms and open networks. Building trust through diplomatic dialogue, cyber norms, and capacity-building programs is therefore vital.

Ultimately, international cooperation and harmonization form the backbone of an effective global response to cybercrime. By aligning substantive laws, streamlining investigative procedures, and fostering real-time collaboration, nations can close jurisdictional loopholes and present a united front against increasingly sophisticated cyber threats. Without such collective effort, criminal law will lag behind technological advances, leaving societies, economies, and critical infrastructure vulnerable to digital exploitation.

PROCEDURAL INNOVATIONS FOR THE DIGITAL AGE

The rapid evolution of technology has transformed how crimes are committed, investigated, and prosecuted. Traditional criminal procedures, designed for physical evidence and face-to-face interactions, are increasingly inadequate in dealing with cybercrime's borderless, fast-moving, and highly technical nature. Procedural innovations have therefore become essential to ensure that criminal law remains effective, fair, and adaptable in the digital age.

One major innovation is the development of specialized cybercrime investigation units equipped with digital forensics expertise. These units employ advanced tools to trace IP addresses, recover deleted data, decrypt communications, and identify malicious code, allowing investigators to collect admissible digital evidence without violating privacy safeguards. Parallel to this, automated evidence-preservation protocols now enable law enforcement to issue rapid data-retention requests to internet service providers, ensuring that critical information is not lost due to routine deletion practices.

International cooperation mechanisms have also evolved to meet the challenges posed by cybercrime's transnational character. Frameworks like the Budapest Convention on Cybercrime promote standardized procedures for cross-border evidence sharing, while newer initiatives involve direct, expedited channels between law enforcement agencies and global tech companies. These mechanisms reduce delays caused by traditional diplomatic processes, which are ill-suited to crimes that can unfold in minutes rather than months.

On the judicial side, digital evidence management systems have been introduced to maintain chain of custody, authenticate metadata, and ensure integrity during trials. Virtual case management platforms also streamline complex cybercrime prosecutions, enabling secure collaboration between prosecutors, forensic analysts, and regulators. Courts are increasingly recognizing electronic evidence formats such as blockchain-verified records and AI-generated reports, provided they meet rigorous reliability standards.

In addition, procedural safeguards for individual rights have been modernized. Since digital investigations often involve accessing personal communications or vast datasets, judicial oversight, warrants tailored to digital contexts, and minimization principles (limiting the scope of surveillance) are being codified to protect privacy while enabling effective enforcement.

Emerging innovations such as AI-assisted threat detection, predictive analytics, and secure digital identity verification are also influencing procedural frameworks. While these tools enhance efficiency, they raise concerns about bias, transparency, and due process, prompting calls for oversight bodies and standardized audit mechanisms.

In sum, procedural innovations in the digital age aim to balance three imperatives: effectiveness in combating sophisticated cybercrimes, respect for fundamental rights, and adaptability to evolving technologies. Criminal law is moving from rigid, paper-based processes to agile, technology-enabled frameworks capable of addressing crimes that transcend geography and time zones—ensuring justice remains both attainable and legitimate in an era dominated by data.

POLICY RECOMMENDATIONS

The rapid evolution of technology has expanded the scale and sophistication of cybercrime, outpacing existing legal frameworks. To address these challenges, policymakers must focus on strengthening legislation, enhancing investigative capabilities, and fostering international cooperation.

First, updating criminal laws to reflect emerging threats is critical. Traditional statutes often fail to cover crimes involving artificial intelligence, cryptocurrency, deepfakes, and data breaches. Laws must provide clear definitions of cyber offenses, establish jurisdictional clarity for cross-border cases, and impose proportionate penalties to deter offenders.

Second, building specialized cybercrime units within law enforcement agencies is essential. These units require advanced tools, digital forensics capabilities, and continuous training to trace encrypted communications, analyze malware, and attribute attacks accurately. Governments should also invest in public–private partnerships to share threat intelligence, as many critical infrastructures are privately operated.

Third, international collaboration must be intensified**.** Cybercrime rarely respects national borders, making unilateral enforcement efforts insufficient. Harmonizing legal standards, adopting extradition treaties, and supporting frameworks like the Budapest Convention can help close jurisdictional gaps exploited by cybercriminals.

Fourth, cybersecurity awareness and preventive strategies should complement punitive measures. Public education campaigns, corporate compliance programs, and incentives for adopting robust cybersecurity practices can significantly reduce vulnerabilities. Additionally, mandatory breach-reporting laws can ensure timely responses to attacks and enhance accountability.

Finally, privacy and human rights safeguards must remain central to policy reforms. While empowering authorities to combat cybercrime, legal measures should avoid excessive surveillance or erosion of civil liberties. Independent oversight mechanisms can ensure a balanced approach.

These policy actions—modernizing legislation, investing in expertise, fostering global cooperation, and safeguarding rights—will equip criminal law to meet the complex challenges of cybercrime in the digital age.

CONCLUSION

Cybercrime's ascent reflects the very strengths of digital transformation—speed, scale, and global reach—recast as vectors of harm. Criminal law can meet this challenge if it evolves along three axes. First, fit-for-purpose substantive law must criminalize harmful conduct in technology-neutral terms, recognize aggravated contexts, and clarify jurisdiction for transnational activity. Second, modernized procedural tools—remote searches, data preservation, and narrowly tailored lawful hacking—should be paired with stringent safeguards to protect privacy and civil liberties. Third, international cooperation and operational capacity must accelerate: harmonized laws, faster cross-border data access with rights protections, validated forensic practices, and robust public-private partnerships.

No single actor can solve cybercrime. Legislatures must refine statutes; courts must adapt evidentiary doctrines; law enforcement needs resources and skills; industry must harden systems and share threat intelligence; civil society should scrutinize powers to preserve rights. The guiding principle is balance: deter and disrupt cybercrime while preserving the open, secure, and rights-respecting digital environment upon which modern life depends.

REFERENCES

[1] Rakha, N. A. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mexican Law Review.
Explores the need for standardized protocols and legal frameworks in handling digital evidence amid rising cybercrime cases.

[2] Nurse, J. R. C. (2018). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. (arXiv)

Analyzes how cybercriminals exploit human psychology through social engineering, identity theft, malware, and other vectors.

[3] Nurse, J. R. C., & Bada, M. (2019). The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations. (arXiv)
Investigates the organization, trust dynamics, and operation of cybercrime groups—such as Anonymous and LulzSec—across borders.

[4] Schiliro, F. (2024). From Crime to Hypercrime: Evolving Threats and Law Enforcement's New Mandate in the AI Age. (arXiv)
Introduces the concept of "hypercrime" driven by AI, emphasizing the need for proactive law enforcement strategies.

[5] Rakha, N. A. (Year unspecified). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. International Journal of Law and Policy.
Highlights the lag in legislation relative to emerging technologies like AI, IoT, and blockchain; advocates agile legislative processes and international cooperation.

[6] Kasturi, Y., & Dar, M. A. (2024). Cybercrime in the Digital Age: Challenges and Legal Gaps in India's Cybersecurity Landscape. African Journal of Biomedical Research, 27(6S), 212–224.
Examines India's legal gaps in addressing cybercrime, particularly vulnerabilities affecting women, children, and seniors.

[7] Raj Kumar, C. Cybercrime and the Law: Challenges in Prosecuting Digital Offenses. Indian Journal of Law.
Discusses prosecutorial hurdles in digital offenses—which include gaps in legal frameworks, evidence issues, and jurisdictional complexity—and calls for international collaboration and legal updates.

[8] Nemeikšis, G. (2023). The Challenges of the Digital Age: The Problems of Criminal Liability for Cybercrimes in Lithuanian Law. Acta Prosperitatis, 13(1), 125–138.
Focuses on Lithuania's criminal liability issues related to cybercrimes and the complexities of applying national law to digital offenses.

[9] Budapest Convention on Cybercrime (Council of Europe).
The first international treaty harmonizing cybercrime definitions, procedural tools, and cross-border cooperation mechanisms—covering offenses like illegal access, data interference, fraud, and child pornography.

[10] United Nations Convention against Cybercrime (2024).
A proposed global treaty to combat cybercrime via international cooperation; however, criticized for broad definitions and human-rights concerns. A signing ceremony is planned for October 2025.