EDİTÖR'DEN

Değerli "Güvenlik Bilimleri Dergisi" okuyucularımız,

Güvenlik Bilimleri Dergimizin Ekim Özel sayısını sizlerin beğenisine ve istifadesine sunmanın gurur ve heyecanını yaşıyoruz. Ekim Özel sayımızda yer alan güvenlik teknolojileri ve kolluk uygulamaları temaları altında hazırlanan araştırma makaleleri ve kitap incelemelerinin alan yazına değerli katkılar sunacağını değerlendiriyoruz.

Günümüz güvenlik ekosistemi, yalnızca yeni donanımların ve yazılımların sahaya girmesiyle değil; karar alma döngülerinin veriye dayalı hale gelmesi, etik-yasal çerçevelerin yeniden tanımlanması ve kurumsal kapasitenin dijital dönüşüme uyarlanmasıyla da çok katmanlı bir dönüşüm yaşıyor. Yapay zekâ, IoT ve gömülü sistemler gibi teknolojiler bir yandan daha hızlı ve isabetli müdahale kabiliyeti sağlarken, diğer yandan mahremiyet, ayrımcılık riski, hesap verebilirlik ve meşruiyet gibi hassas alanlarda yeni sorular doğuruyor. Bu sayıda yer alan çalışmalar, tam da bu gerilimi –teknoloji ile yönetişimin, hız ile hakkaniyetin, güvenlik ile özgürlüklerin– kesişiminde konumlanıyor; farklı disiplinlerden gelen özgün katkılarla bütüncül bir çerçeve sunuyor.

DURAKLAR'ın *"Yapay Zekâ Destekli Güvenlik Sistemlerinde Elektronik Bileşenlerin Rolü: IoT ve Gömülü Sistem Entegrasyonu"* başlıklı çalışması, güvenliğin mühendislik boyutunu sahici bir operasyonel anlatıya dönüştürüyor. Gömülü kontrolcüler, düşük güçlü YZ çipleri, sensör ağları ve haberleşme katmanlarının, bulut/kenar bilişim mimarileriyle birlikte gerçek zamanlı algılama–karar–icra döngüsünü nasıl hızlandırdığını örnekleyerek; yüz tanıma ve biyometri, siber güvenlik, akıllı şehirler, otonom sistemler ve sınır güvenliği gibi saha uygulamalarında performans/enerji/mahremiyet üçgenini dengelemeye yönelik

tasarım ilkelerini ortaya koyuyor. Çalışma, Türkiye'nin ulusal YZ stratejisiyle uyumlu yatırım alanlarını işaret ederken, etik ve hukuki risklerin tasarım sürecine "baştan" entegre edilmesi gerektiğini gösteriyor; böylelikle güvenlikte mühendislik mükemmelliğinin tek başına yeterli olmadığını, normatif ve kurumsal düzeneklerle birlikte düşünülmesi gerektiğini vurguluyor.

OZAN'ın *"Akıllı Şehirlerde Kamu Güvenliğinin Yeniden İnşası: Kolluk Uygulamalarında Güvenlik Teknolojileri ve Etik Hususlar*" başlıklı makalesi, akıllı şehir güvenliğini salt bir teknoloji envanteri olmaktan çıkarıp yönetişim ilkeleriyle ilişkilendiriyor. Büyük veri, YZ, IoT ve yüz tanıma gibi bileşenlerin karar destek ve öngörücü kolluk kapasitesini nasıl artırdığını somut vakalarla incelerken; şeffaflık, hesap verebilirlik ve temel hakların korunması ekseninde "meşru teknoloji" tasarımını tartışmaya açıyor. ABD, Çin, Singapur ve Avrupa'dan örnekler üzerinden geliştirilen karşılaştırmalı çerçeve, teknolojik kabiliyetin demokratik normlarla eklemlenmediği durumlarda sosyal lisansın kaybı, önyargılı modeller ve kurumsal güven erozyonu gibi sonuçlar doğurabileceğine işaret ediyor.

BİLBAY'ın *"Türkiye'de Kolluk Hizmetlerinde Dijitalleşme ve Kentsel Güvenlik"* başlıklı çalışması, hızlı kentleşmenin doğurduğu güvenlik risklerini YZ tabanlı gözetim, büyük veri analitiği ve IoT uygulamalarının fırsat ve sınırlarıyla birlikte ele alıyor. Çalışma, verimlilik ve hızlı müdahale kapasitesindeki kazanımları kabul etmekle birlikte; bireysel mahremiyet, siber güvenlik ve algoritmik tarafsızlık risklerini görmezden gelmeyen dengeli bir kamu yönetimi yaklaşımı öneriyor. Böylece dijitalleşmenin, tek yönlü bir "teknik çözüm" değil; politika tasarımı, hukuki uyum ve toplumsal meşruiyet bileşkesi olduğu hatırlatılıyor.

Saha başarısının yalnızca teknoloji seçimiyle değil, kurumsal koordinasyonla mümkün olduğunu gösteren bir diğer katkı, **KURBAN**'ın *"Dijital Kolluk Hizmetlerinin Koordinasyonunda ve Yönetiminde Kurumsallaşmanın Önemi:*

Birleşik Krallık Örneği" başlıklı makalesi. Çalışma, çok kaynaktan beslenen veri ekosistemlerinde öngörücü polisliğin "uygulama gücü" kazanabilmesi için yönetişim, finansman ve standartlaşma eksenlerinde kurumsal kapasitenin nasıl inşa edildiğini Police Digital Service modelini mercek altına alarak açıklıyor. Birlikte çalışabilirlik, kaynak öncelikleme ve stratejik uyum gibi başlıklarda sunulan çıkarımlar, dijital kolluk mimarisi için ölçeklenebilir bir yol haritası sunuyor.

Vatandaş–kolluk etkileşiminin dijital platformlar üzerinden yeniden örgütlendiğini gösteren **YOLCU**'nun *"Kamu Güvenliğinin Dijitalleşmesi: Türkiye'de Mobil İhbar Uygulamaları Üzerinden Kolluk–Vatandaş Etkileşimi"* başlıklı makalesi, KADES, UYUMA, HAYDİ ve EGM KAAN Mobil uygulamalarını tematik odakları ve kullanım dinamikleriyle analiz ediyor. Bulgular, hızlı müdahale ve veri temelli planlamanın yanı sıra, katılımcı yönetişim kapasitesinin güçlendiğini ortaya koyuyor. Çalışma, mevcut başarının sürdürülebilirliği için teknik güncellemeler kadar, eğitim, geri bildirim mekanizmaları ve erişilebilirlik ilkelerinin de kritik olduğunu gösteriyor.

TOY'un *"Emniyet Teşkilatında Güvenlik Teknolojilerinin Kullanımı: Türkiye'de Seçilmiş Şehirler Üzerinden Karşılaştırmalı Bir Analiz"* başlıklı araştırması, İstanbul, Ankara, İzmir, Antalya, Gaziantep, Erzurum ve Diyarbakır örnekleri üzerinden suç önleme, olay müdahalesi, soruşturma ve denetim/izleme işlevlerinde teknoloji kullanım düzeylerini karşılaştırmalı olarak ortaya koyuyor. Altyapı, insan kaynağı, donanım ve yerel ihtiyaçların belirleyici olduğu bulgular, tek tip bir teknoloji stratejisi yerine yerel bağlama duyarlı, dengeli ve sürdürülebilir planlamaların gereğini ikna edici biçimde gösteriyor.

Teknolojinin yaygınlaştığı mecraların başında gelen sosyal medya, etik ve güvenlik boyutlarıyla bu sayının eleştirel mihenk taşlarından birini oluşturuyor. **SÖNMEZER**'in *"Sosyal Medyada Etik, Kişisel Veri Gizliliği ve Güvenlik*

Tehditleri" başlıklı çalışması, anonimlik ve kimlik performanslarının nefret söylemi ve dezenformasyonla nasıl kesiştiğini; platform tasarımı, düzenleyici politika ve kullanıcı sorumluluğunun müşterek bir çözüm alanı gerektirdiğini gösteriyor. Doküman analizi ile desteklenen değerlendirme, baskı/çıkar gruplarının manipülatif içerikleri hızla dolaşıma sokabildiği ortamda, algoritmik şeffaflık ve içerik denetimi kadar medya okuryazarlığının da asli bir güvenlik yetkinliğine dönüştüğünü ortaya koyuyor.

Yüz tanıma teknolojilerinin kolluk uygulamalarında etik çerçevesini tartışan **KAYACI**'nın *"The Ethical Dimensions of Law Enforcement's Use of Facial Recognition Technology"* başlıklı makalesi, mahremiyet, ayrımcılık riski, yaygın gözetim hissi, şeffaflık ve hesap verebilirlik eksenlerinde ilkeler seti öneriyor. Literatürün kavramsal envanterini bütüncül bir değerlendirmeye dönüştüren çalışma, meşru amaçla toplanan biyometrik verilerin, tasarım kusurları veya operasyonel önyargılar nedeniyle etik dışı sonuçlar doğurabileceği uyarısını yaparak, "güvenlik için özgürlüklerden vazgeçmeyen" dengeli bir uygulama çerçevesi çiziyor.

Kamu güvenliğinin küresel standartlarla olan bağını tarihsel bir izlekte ele alan **BÖREKÇİ ŞAHAN**'ın *"Evolving Phenomenon: The FATF"* başlıklı makalesi, G7 inisiyatifi olarak 1989'da başlatılan FATF'ın kara para aklama, terörizmin finansmanı ve yayılmanın finansmanı alanlarında standart koyucu rolünün evrimini yıllık raporlar ve zirve bildirileri üzerinden sistematik biçimde haritalıyor. Çalışma, esneklik ve uyum yeteneğinin küresel yaygınlaşmayı mümkün kıldığını teslim ederken, genişleyen yetki alanının temel yapı taşlarından uzaklaşma riski taşıdığı uyarısını yapıyor; böylece finansal güvenliğin yalnızca teknik uyum değil, stratejik odak ve ölçeklenebilir yönetişim meselesi olduğunu hatırlatıyor.

Elektromanyetik spektrumun güvenlikteki kritik rolünü somut bir kırılganlık başlığı üzerinden ele alan **YILMAZ**'ın *"Strategic Role of GNSS in Security*

Technologies and Alternative Approaches to National Navigation Systems" başlıklı çalışması, küresel konumlama altyapısının jammer/spoofer saldırılarına ve jeopolitik bağımlılığa açık yapısını tartışıyor. eLoran, DGNSS ve RTK gibi yersel çözümlerle GNSS'in tamamlandığı çok katmanlı bir seyrüsefer mimarisinin, ulusal güvenliğin sürdürülebilirliği için stratejik gereklilik olduğunu savunuyor; böylece "alternatif/yedekli" mimarilerin önemini, elektronik harp ve siber tehditler çağında ikna edici biçimde temellendiriyor.

Denizcilik alanında siber güvenlik ve mahremiyet boyutlarını kuramsal çerçeve, vaka incelemeleri ve gelecek perspektifleriyle bütünleştiren **ERDOĞAN** ve **ERDOĞAN**'ın *"Cybersecurity and Privacy in Maritime Security: Theories, Challenges, Case Studies and Future Prospects"* başlıklı makalesi, hızla dijitalleşen denizcilik ekosisteminde kritik altyapıların karşı karşıya olduğu riskleri ve yönetişim seçeneklerini netleştiriyor. Çalışma, limanlardan gemi sistemlerine uzanan saldırı yüzeyinde çok katmanlı güvenlik mimarisinin ve uluslararası iş birliğinin belirleyici olduğunu vurgulayarak, politika ve uygulama için somut bir yol haritası sunuyor.

Kriptografinin teorik derinliğini pratik bir anahtar üretim problemine bağlayan **GÜR** ve **GÜR**'ün *"Graph-Based Cryptographic Key Generation for Secure Text Encryption"* başlıklı çalışması, mono-alfabetik bir ön katmanla desteklenen, Kruskal algoritmasına dayalı minimum yayılma ağacı üzerinden ortak anahtar türeten iki aşamalı bir şema öneriyor. Komşuluk matrisleri ve izomorfizm özellikleriyle güçlendirilen yaklaşımın kaynak etkinliği ve saldırı dayanımı analizleri, önerinin metin şifreleme senaryolarında uygulanabilir ve dirençli bir alternatif sunduğunu gösteriyor.

Güvenliğin yalnızca teknik aygıtlarla değil, kültürel-simgesel düzeyde de üretildiğini gösteren **ÖZKAN** ve **DİNÇ**'in *"Rosgvardiya'nın Güvenlik Anlayışı ve Dijital Gözetim: Rusya'da Yeni Bir Toplumsal Denetim Mekanizması"* başlıklı

makalesi, Foucault'nun disipliner iktidarı ve Alexander'ın kültürel performans kuramı üzerinden Rosgvardiya'nın dijital gözetim altyapıları, kamusal performansları ve medya temsilleriyle güvenlik, otorite ve hiyerarşi anlatılarını nasıl yeniden ürettiğini ortaya koyuyor. Böylece güvenliğin teknik pratik kadar bir "anlam rejimi" olduğunu, kurumların simgeler ve ritüeller aracılığıyla toplumsal meşruiyet inşa ettiğini gösteriyor.

Çevresel tehditlerin kolluk operasyonlarına etkisini strateji ve kapasite inşası perspektifinden ele alan **ÖZTÜRK**'ün *"Kolluk Kuvvetlerinin Çevresel Tehditlere Karşı Kullanacağı Akıllı Güvenlik Teknolojileri: Kamu Yönetimi Perspektifinden Stratejik Yaklaşımlar ve Politikalar"* başlıklı makalesi, iklim kaynaklı riskler, doğal afetler ve çevresel suçlarla mücadelede YZ destekli izleme, drone ve sensör ağları ile veri analitiğinin özgün değerini tartışıyor. Altyapı yatırımları, insan kaynağı ve eğitim gereksinimlerine işaret eden çalışma, kamu yönetimi desteği ve çok paydaşlı iş birlikleri olmaksızın teknolojinin beklenen etkiyi yaratamayacağını veriye dayalı biçimde gösteriyor.

Suç önleme stratejilerinin karşılaştırmalı incelemesini sunan **SARIBEY** ve **BAL**'ın *"Türkiye'deki ve Birleşik Arap Emirlikleri'ndeki Suç Önleme Stratejilerinin Çağdaş Kolluk Hizmetleri ve Toplum Güvenliği Sistemleri Bağlamında Karşılaştırılması"* başlıklı çalışması, BAE'de iris tanıma, "Şahin Gözü", robotik devriyeler ve YZ departmanı gibi uygulamaların suçu azaltmadaki etkilerini verilerle tartışıyor; Türkiye'deki hukukî ve toplumsal bağlamda uyarlanabilirliğin imkân ve sınırlarını dengeli biçimde değerlendiriyor. Bulgular, teknoloji transferinin "çoğalt-yapıştır" değil, bağlamsal uyarlama ve kademeli geçiş gerektiren bir yönetişim meselesi olduğunu teyit ediyor.

Bu sayı, güvenliğin teknik tasarım, kurumsal kapasite, etik-yasal normlar ve kültürel meşruiyetin birlikte düşünülmesi gereken bir "bütün" olduğunu güçlü

biçimde teyit ediyor. Yapay zekâ ve gömülü sistemlerin sahada ürettiği hız ve doğruluk kazanımları, ancak şeffaflık ve hesap verebilirlikle desteklendiğinde sürdürülebilir bir toplumsal mutabakata dönüşebiliyor. Kritik altyapıların yedekli ve çok katmanlı tasarımı, siber-fiziksel tehdit ortamında kırılganlıkları azaltırken; dijital kolluk mimarisinin başarısı, verinin kalitesi kadar kurumsal koordinasyon ve vatandaşla kurulan güven ilişkisine bağlı. Sosyal medya, finansal gözetim ve kültürel güvenlik rejimleri üzerine yapılan çalışmalar ise, güvenliğin yalnızca bir "teknoloji yatırımı" değil; aynı zamanda bir anlam, hak ve yönetişim projesi olduğunu hatırlatıyor. Bu çerçevede, araştırmacılarımıza, sahadan ve kurumsal dünyadan katkı veren tüm paydaşlarımıza ve titiz değerlendirmeleriyle bu bütünlüğü mümkün kılan hakemlerimize teşekkür eder; okurlarımıza ilham verici ve ufuk açıcı bir okuma dileriz. Bu vesile ile bu sayının yayınlanmasına katkı veren tüm bilim insanlarımıza teşekkür ediyorum.

Hoşçakalın…

Prof.Dr. Osman KÖSE
Baş Editör

EDITOR'S NOTE

Dear Readers of the Journal of Security Sciences,

We are proud and excited to present our research and review articles, which we believe will make valuable contributions to the literature on current problems in security sciences, for your appreciation and use in the October issue of our Journal of Security Sciences. We believe that the research articles and book reviews in our October issue, prepared under the themes of security technologies, and policing applications, will provide valuable contributions to the literature.

Today's security ecosystem is undergoing a multilayered transformation not only through the deployment of new hardware and software in the field, but also via the datafication of decision-making cycles, the redefinition of ethical-legal frameworks, and the adaptation of institutional capacity to digital transformation. While technologies such as artificial intelligence (AI), the Internet of Things (IoT), and embedded systems enhance the speed and precision of response, they simultaneously raise new questions in sensitive domains including privacy, discrimination risk, accountability, and legitimacy. The contributions in this issue are situated precisely at these intersections—between technology and governance, speed and fairness, security and liberty—offering a holistic framework through original, interdisciplinary perspectives.

DURAKLAR's article, *"The Role of Electronic Components in AI-Enabled Security Systems: IoT and Embedded System Integration,"* translates the engineering dimension of security into a substantive operational narrative. By demonstrating how embedded controllers, low-power AI chips, sensor networks, and communication layers—together with cloud/edge computing architectures—accelerate the perceive–

decide–act loop in real time, the study distills design principles that balance the performance/energy/privacy triangle across field applications such as facial recognition and biometrics, cybersecurity, smart cities, autonomous systems, and border security. Aligned with Türkiye's national AI strategy, the article identifies priority investment areas while showing that ethical and legal risks must be integrated into design "from the outset," underscoring that engineering excellence alone is insufficient without concurrent normative and institutional arrangements.

OZAN's contribution, *"Rebuilding Public Security in Smart Cities: Security Technologies and Ethical Considerations in Law Enforcement Practices,"* moves smart-city security beyond a mere inventory of technologies and anchors it in principles of governance. Examining how big data, AI, IoT, and facial recognition enhance decision support and predictive policing through concrete cases, the article opens a debate on "legitimate technology" within a framework of transparency, accountability, and the protection of fundamental rights. Through a comparative lens spanning the United States, China, Singapore, and Europe, it cautions that where technological capability is not articulated with democratic norms, outcomes may include loss of social license, biased models, and institutional trust erosion.

BİLBAY's study, *"Digitalization in Law Enforcement and Urban Security in Türkiye,"* addresses the security risks produced by rapid urbanization alongside the opportunities and limits of AI-based surveillance, big-data analytics, and IoT applications. While acknowledging gains in efficiency and rapid intervention capacity, the article advances a balanced public-administration approach that does not overlook risks related to individual privacy, cybersecurity, and algorithmic neutrality, thereby reminding us that digitalization is not a one-dimensional "technical fix," but a composite of policy design, legal compliance, and societal legitimacy.

Another contribution demonstrating that field effectiveness depends not only on technology selection but also on institutional coordination is **KURBAN**'s *"The Importance of Institutionalization in the Coordination and Management of Digital Law-Enforcement Services: The United Kingdom Example."* By scrutinizing the Police Digital Service model, the study explains how institutional capacity in governance, financing, and standardization is constructed so that predictive policing within multi-source data ecosystems can acquire "implementation power." Insights on interoperability, resource prioritization, and strategic alignment offer a scalable roadmap for digital law-enforcement architectures.

YOLCU's article, *"The Digitalization of Public Security: Law-Enforcement–Citizen Interaction through Mobile Reporting Applications in Türkiye,"* shows how the interaction between citizens and law enforcement is being reorganized via digital platforms. Analyzing KADES, UYUMA, HAYDİ, and EGM KAAN Mobile in terms of thematic foci and usage dynamics, the findings indicate that, in addition to enabling rapid response and data-driven planning, these systems strengthen participatory governance capacity. The study shows that, to sustain present successes, technical updates must be complemented by training, feedback mechanisms, and accessibility principles.

TOY's research, *"The Use of Security Technologies in the Turkish National Police: A Comparative Analysis across Selected Cities,"* offers a comparative assessment of technology use in crime prevention, incident response, post-incident investigation, and oversight/monitoring across Istanbul, Ankara, Izmir, Antalya, Gaziantep, Erzurum, and Diyarbakır. The results—shaped by infrastructure, human resources, equipment, and local needs—demonstrate persuasively that, rather than a one-size-fits-all approach, technology strategies should be locally attuned, balanced, and sustainable.

As one of the most pervasive domains of technological diffusion, social media functions as a critical axis of ethics and security in this issue. **SÖNMEZER**'s article, *"Ethics, Personal Data Privacy, and Security Threats on Social Media,"* shows how anonymity and identity performances intersect with hate speech and disinformation, and argues that platform design, regulatory policy, and user responsibility must converge to form a shared space of solutions. Supported by document analysis, the study demonstrates that in environments where pressure/interest groups can rapidly circulate manipulative content, algorithmic transparency and content moderation are as essential as media literacy—now emerging as a core security competence.

KAYACI's *"The Ethical Dimensions of Law Enforcement's Use of Facial Recognition Technology"* delineates a principled framework for the use of facial recognition in policing, engaging issues of privacy, discrimination risk, the sense of pervasive surveillance, transparency, and accountability. Converting a conceptual literature inventory into an integrated assessment, the study warns that biometric data collected for legitimate public purposes may nonetheless produce unethical outcomes due to design flaws or operational bias, thereby outlining a balanced approach that "does not trade liberty for security."

BÖREKÇİ ŞAHAN's article, *"Evolving Phenomenon: The FATF,"* situates public security within global standards along a historical trajectory. Systematically mapping the evolution of FATF's standard-setting role in combating money laundering, terrorist financing, and proliferation financing since its initiation by the G7 in 1989 through annual reports and summit communiqués, the study acknowledges that flexibility and adaptability facilitated global diffusion while warning that an expanding mandate risks drifting from foundational building blocks—thus underscoring that financial security is not merely technical compliance, but also a matter of strategic focus and scalable governance.

Addressing a concrete vulnerability within the security-critical electromagnetic spectrum, **YILMAZ**'s article, *"The Strategic Role of GNSS in Security Technologies and Alternative Approaches to National Navigation Systems,"* discusses the exposure of global positioning infrastructure to jamming/spoofing and geopolitical dependence. Advocating a multilayered navigation architecture in which GNSS is complemented by terrestrial systems such as eLoran, DGNSS, and RTK, the study argues that a hybrid, redundant design is a strategic necessity for sustainable national security—convincingly grounding the importance of "alternative/backup" architectures in an era of electronic warfare and cyber threats.

ERDOĞAN and **ERDOĞAN**'s contribution, *"Cybersecurity and Privacy in Maritime Security: Theories, Challenges, Case Studies and Future Prospects,"* integrates theoretical framing, case studies, and forward-looking perspectives on cybersecurity and privacy in the maritime domain. Clarifying the risks faced by rapidly digitalizing maritime ecosystems and the governance options available, the study emphasizes that multilayered security architectures and international cooperation are decisive across the attack surface spanning ports to ship systems, thereby offering a concrete roadmap for policy and practice.

Linking the theoretical depth of cryptography to a practical key-generation problem, **GÜR** and **GÜR**'s *"Graph-Based Cryptographic Key Generation for Secure Text Encryption"* proposes a two-stage scheme that derives a shared key via a minimum spanning tree using Kruskal's algorithm, layered atop a monoalphabetic preliminary stage. Strengthened through adjacency matrices and graph isomorphism properties, the approach shows resource efficiency and attack resilience in its security analysis, indicating a viable and robust alternative for text-encryption scenarios.

Demonstrating that security is produced not only through technical apparatuses but also at cultural-symbolic levels, **ÖZKAN** and **DİNÇ**'s article, *"Rosgvardiya's*

Security Understanding and Digital Surveillance: A New Mechanism of Social Control in Russia," draws on Foucault's theory of disciplinary power and Alexander's theory of cultural performance to show how Rosgvardiya, through digital surveillance infrastructures, public performances, symbols, and media representations, reproduces narratives of security, authority, and hierarchy. In doing so, the study reveals that security is as much an "order of meaning" as it is a technical practice and that institutions build social legitimacy through symbols and rituals.

Addressing the impact of environmental threats on law-enforcement operations from the perspective of strategy and capacity building, **ÖZTÜRK**'s article, *"Smart Security Technologies for Law Enforcement against Environmental Threats: Strategic Approaches and Policies from a Public-Administration Perspective,"* discusses the distinctive value of AI-supported monitoring, drone and sensor networks, and data analytics in responding to climate-driven risks, natural disasters, and environmental crime. Pointing to infrastructure investment, human-capital development, and training needs, the study provides data-driven evidence that, without public-administration support and multi-stakeholder cooperation, technology alone will not achieve the anticipated impact.

SARIBEY and **BAL**'s comparative analysis, *"A Comparison of Crime-Prevention Strategies in Türkiye and the United Arab Emirates within the Context of Contemporary Law-Enforcement Services and Community-Security Systems,"* examines the effects of practices such as iris recognition, "Hawk Eye," robotic patrols, and AI departments on crime reduction in the UAE, and evaluates their adaptability within Türkiye's legal and social context. The findings confirm that technology transfer is not a "copy-and-paste" endeavor, but a governance challenge requiring contextual adaptation and phased transitions.

Collectively, this issue affirms that security is an integrated "whole" wherein technical design, institutional capacity, ethical-legal norms, and cultural legitimacy

must be considered together. The speed and accuracy gains delivered by AI and embedded systems can only translate into a sustainable social consensus when supported by transparency and accountability. While redundant and multilayered designs mitigate vulnerabilities across cyber-physical threat environments for critical infrastructures, the success of digital law-enforcement architectures depends as much on institutional coordination and the quality of data as it does on the trust relationship forged with citizens. The studies on social media, financial supervision, and cultural security regimes further remind us that security is not simply a "technology investment," but simultaneously a project of meaning, rights, and governance. In this regard, we extend our gratitude to our researchers, to all stakeholders from the field and institutional spheres, and to our reviewers whose meticulous assessments made this coherence possible, and we wish our readers an inspiring and horizon-broadening experience. We also take this occasion to thank all the scholars who contributed to the publication of this issue.

Sincerely…

Prof Osman KÖSE, Ph.D.
Editor in Chief