Recommendations on countering the use of digital communication platforms by organized crime: tasks of law enforcement agencies, state security agencies and international cooperation

Author: Prof. Vasily K. Isaul

Date: 01.06.2026

Table of Contents

To whom the article is addressed

The article is addressed to the scientific community and practitioners working at the intersection of criminology, criminal law, information law, theory of state and law, digital forensics and public administration, as well as law enforcement officers, state security agencies, financial intelligence units, investigation, prosecutor's office and international police cooperation. In addition, it can be useful for public policy makers, national security experts, teachers and researchers studying the transformation of organized crime in a digital platform environment.

Summary

The article explores organized crime in digital communication environments as a complex socio-legal, infrastructural and managerial phenomenon. It is substantiated that digital platforms have ceased to be neutral channels for transmitting information and have turned into a stable environment for the existence, coordination, masking and reproduction of criminal networks. It is shown that modern crime uses platform logic to recruit, allocate roles, hide traces, financial support, transfer audiences between channels and quickly recover from blockages. Particular attention is paid to the strategic formulation of the problem for law enforcement agencies, the need to move from reactive response to proactive identification of criminal ecosystems, as well as the development of interdepartmental centers of digital countermeasures, digital intelligence, criminal analysis, standardization of digital evidence fixation and a risk-oriented prioritization model. Approaches to the use of financial intelligence, the tasks of state security agencies, issues of international cooperation, including the role of Interpol, Europol, the United Nations Office on Drugs and Crime and other international structures, as well as measures for prevention and information and legal impact. It is concluded that effective counteraction is possible only if there is an integrated combination of legal, organizational, analytical, technical, preventive and international mechanisms aimed not only at suppressing individual episodes, but also at destroying the infrastructure of digital organized crime itself.

1. INTRODUCTION

At the beginning of the XXI century, it became finally obvious: digital communication platforms can no longer be considered as simple and neutral channels for transmitting messages. Their public role has changed qualitatively. They have turned into multi-level socio-technical environments, where everyday communication, the dissemination of socially significant information, business coordination, institutional interaction, informal horizontal ties and various forms of illegal activity coexist at the same time. This creates a new reality in which crime does not just use technical means to commit individual acts, but is embedded in the very fabric of digital communication, adapts to the logic of the platform organization and benefits from the architecture of the modern information environment. It is here that one of the most important lines of modern confrontation between public power, law and order and organized crime passes.

The problem, therefore, is not the very fact of the presence of illegal content or criminal communications in the digital environment, but in a much deeper phenomenon: digital platforms are becoming a sustainable infrastructure for criminal activity. Organized criminal communities use them not by chance, not auxiliary and not in the mode of one-time contacts, but as a long-term, flexible and constantly reproduced environment for finding performers, distributing roles, masking intentions, maintaining discipline, expanding the client base, legitimizing illegal supply in the eyes of a mass audience and operational restoration of disrupted interaction channels. Under these conditions, the platform no longer acts as an external tool, but as an environment for the existence of a criminal network. This circumstance requires a fundamental revision of both scientific ideas about digital crime and practical approaches of the state to its prevention, detection and suppression.

It should be emphasized that modern organized crime is increasingly abandoning the previous logic of spatial isolation, conspiratorial isolation and reliance solely on hard-to-reach sections of the network. On the contrary, a significant part of criminal activity moves to those digital spaces that are built into the daily life of millions of citizens. Such a transformation has far-reaching consequences. Firstly, the former symbolic distance between the "ordinary" user and the criminal environment disappears: the illegal proposal begins to be perceived as one of the many messages in the general information flow. Secondly, the psychological barrier to entering illegal practices is reduced, since communication with a potential recruiter, intermediary or distributor takes the form of a familiar and technologically simplified interaction. Thirdly, conditions are created for the gradual normalization of criminal behavior patterns, when an illegal action loses a halo of exclusivity in public perception and begins to disguise itself as a kind of "ordinary" digital activity. The danger lies not only in the concealment of crime, but also in its everyday life.

A significant factor in the growth of this threat is the combination of several properties of modern digital platforms. These include high speed of information dissemination, low costs of creating and replicating information materials, relative ease of access to a wide audience, technical ability to use closed communities and pseudonymous accounts, as well as poor transparency of internal information management procedures. As a result, criminal structures gain a unique advantage: they can quickly rebuild communication routes, scale their presence, test ways to influence different audiences and reproduce channels destroyed by law enforcement agencies at minimal cost. The removal of individual accounts, communities or information materials in such conditions does not in itself mean the destruction of a criminal network. On the contrary, it often only encourages her to more complex adaptation, dispersal and transition to new forms of camouflage. The digital environment provides organized crime with not only a means of communication, but also a mode of constant adaptive resilience.

The scientific significance of the problem under consideration is determined by the fact that it is at the intersection of several major research areas: criminology, criminal law, theory of state and law, information law, sociology of communications, management theory, forensic examination of digital traces and national security practices. Organized crime in the digital environment does not fit into traditional study schemes, since it combines the features of a network structure, high distribution, functional flexibility and cross-border. Its participants can be in different states, use different legal regimes, divide the stages of illegal activity among themselves, and at the same time maintain organizational unity through stable digital channels. In these conditions, the classic models of investigation, built around a localized place of commission of the act, a limited circle of participants and materially fixed traces, face serious limits of applicability. Science is faced with the task of describing not a separate digital episode, but the holistic infrastructure logic of modern crime.

Particular attention should be paid to the fact that digital platforms create a favorable environment for combining different stages of criminal activity in a single communication circuit. Where earlier preparation, advertising, search for performers, transmission of instructions, profit distribution, psychological pressure and control of execution could be separated by time, space and communication channels, now they are often combined in one digital space. This provides unprecedented speed of the management cycle within the criminal network. Decisions are made faster, the connections between organizers and performers become tighter, and the managerial distance between the center and the periphery is reduced. Moreover, the digital environment itself contributes to the formation of new types of criminal discipline: a community member can be under constant information influence, receive regular instructions, report on the fulfillment of tasks, be subject to internal control and sanctions. Organized crime

in the digital environment is increasingly taking on the features of a continuously operating managed system.

Equally important is the social aspect of the problem. Digital platforms, being spaces of mass stay of citizens, become an arena of struggle not only for information, but also for norms, representations, admissibility of certain practices. Criminal communities seek not only to hide, but to integrate into the environment, mimic legitimate activity, use the language of everyday life, techniques of visual and semantic simplification, trusting forms of appeal and mechanisms of group identification. This makes illegal exposure especially dangerous for young people, socially vulnerable groups, people with a low level of legal culture and citizens in a state of economic or psychological instability. Involvement in criminal activity in such conditions can be carried out gradually, through a consistent deformation of perception: from simple observation of an illegal proposal - to its admission, from admission - to trial participation, from participation - to sustainable criminal involvement. The digital environment transforms recruitment from an exceptional act into a stretched and technologically accompanied process of social reformatting of the personality.

That is why countering organized crime in digital communication environments cannot be limited to criminal law response to acts already committed. The repressive mechanism remains necessary, but it is clearly not enough. If the state is limited only to investigating individual episodes and punishing the identified perpetrators, it inevitably acts with delay, responding to the consequences, and not to the mechanisms of reproduction of the threat. Meanwhile, the very nature of the digital criminal environment requires a different approach - systematic, proactive, interdepartmental, scientifically based and technologically equipped. Such an approach should include prevention, criminological forecasting, constant analytical support, the development of digital intelligence, improving legal regulation, strengthening international cooperation, the formation of uniform standards for the exchange of information and the creation of mechanisms for a rapid interstate response. Only a combination of legal, organizational, technical and preventive measures can disrupt the infrastructural stability of criminal networks.

At the same time, the correlation between the tasks of ensuring security and observing human rights and freedoms is especially difficult. Digital platforms are a space for the realization of freedom of communication, dissemination of information, participation in public life and professional activities. Consequently, government intervention in this area inevitably affects fundamental legal values. Hence the need for extremely accurate, proportionate and lawful regulation, capable of simultaneously protecting society from the criminal use of platforms and not turning the fight against crime into a basis for arbitrarily restricting legitimate communication. Scientific analysis should thus take into account not only the effectiveness of law enforcement mechanisms, but

also the limits of permissible intervention, guarantees of judicial and departmental control, the requirements of provability, verifiability and legal certainty. A strong state in the digital age is not a state of uncontrolled surveillance, but a state of accurate, legal and responsible action.

The relevance of the declared topic is enhanced by the international dimension of the problem. Organized crime operating through digital platforms almost always has a cross-border character. Data can be stored in one jurisdiction, the organizers are in another, the performers are in the third, and the victims are simultaneously in dozens of states. Such a stratification of criminal activity destroys traditional ideas about the territorial connection of the crime and requires new forms of international legal and institutional interaction. Without agreed procedures for requesting, sharing information, preserving digital traces, identifying participants, joint investigations and recognizing electronic evidence, the fight against transnational criminal networks inevitably turns out to be fragmented. Crime has long learned to operate on top of borders; law and public administration have no right to lag behind.

Consequently, the subject of scientific analysis should be not only the identification of certain forms of use of digital platforms for criminal purposes, but also the study of those structural conditions that make such use sustainable, profitable and difficult to suppress. It is about the need to consider the digital platform as a special institutional environment where the interests of users, infrastructure owners, government agencies, law enforcement agencies, international institutions and criminal communities intersect. This environment has its own rules for visibility, dissemination of information, grouping, rating reinforcement of attention, audience segmentation and reproduction of trust. Ignoring these patterns makes the fight against organized crime deliberately reactive and insufficiently effective. You cannot effectively confront a criminal network without understanding the structure of the environment that ensures its viability.

The present study assumes that organized crime in digital communication environments should be viewed as a complex socio-legal and managerial phenomenon requiring comprehensive analysis. It is necessary to establish how platform logic strengthens the stability of criminal structures; what functions digital environments perform in the mechanism of a criminal organization; why traditional law enforcement tools prove limited; what legal, technological and organizational changes are necessary for an adequate state response; how preventive and repressive measures should be combined; and finally, how to build a model of counteraction that is both effective, legal and commensurate with the scale of the threat. The question is very clear: either the state will learn to act in the logic of the digital age, or organized crime will continue to use its advantages faster and more sophisticated than public power.

The purpose of this introduction is to justify the need to move from a fragmented perception of individual digital criminal episodes to an understanding of organized crime as a networked, adaptive and infrastructurally rooted form of criminal activity. Based on this, the subsequent presentation should be aimed at disclosing the mechanisms of the functioning of criminal communities on digital platforms, analysing the vulnerabilities of the existing legal and organizational response, as well as formulating proposals for improving state policy in this area. The scientific and practical task is not just to describe the threat, but to develop a holistic model for its containment and destruction.

2. STRATEGIC PROBLEM STATEMENT FOR LAW ENFORCEMENT AGENCIES

For law enforcement agencies and structures ensuring state security, a radical revision of the very subject of countering digital crime is now of paramount importance. The most dangerous methodological error remains the idea of it as a set of separate, weakly interconnected episodes: illegal sale, fraudulent theft, distribution of prohibited information, recruitment, legalization of criminal proceeds, coordination of violent actions or circulation of forged documents. Such a view, for all its external convenience for departmental accounting, no longer corresponds to the real picture of what is happening. It breeds a false sense that every digital crime exists in isolation, as an autonomous case requiring only private legal assessment and private investigative response. Meanwhile, the modern criminal environment in the digital space develops not as the sum of episodes, but as a stable, self-reproducing, adaptable criminal environment with its own rules, internal separation of roles, self-defence mechanisms and the ability to quickly update.

That is why the strategic formulation of the problem should proceed from the recognition that today the state is not facing individual offenders who act randomly and haphazardly, but digital criminal ecosystems. This concept requires special attention, since it does not reflect a metaphor, but the true organizational nature of modern crime. We are talking about such collections of persons, means of communication, methods of concealment, calculation channels, methods of influencing the audience and schemes for distributing functions that form an integral environment of criminal existence. In this environment, some participants produce an illegal product, others ensure its distribution, others maintain trust in the site, the fourth resolve disputes, the fifth are engaged in attracting new performers, the sixth are responsible for hiding traces, the seventh redistribute cash flows, and the eighth restore the disrupted infrastructure after external influence. Consequently, the law enforcement agencies face not just an offense as a legal fact, but a complex socio-technical organism, in which a separate criminal act is only a visible part of a much deeper process.

Of fundamental importance is the fact that such ecosystems have a distributed structure. This means the absence of a single center, the destruction of which

would automatically entail the destruction of the entire illegal network. Organizational stability is achieved through role dispersal, duplication of communication channels, the use of many accounts, the distribution of functions between administrators, intermediaries, technical performers, carriers, recruiters, custodians of funds and persons providing information cover. In such a structure, the liquidation of one participant or one node does not destroy the system as a whole: another element is quickly embedded in its place, and the network itself continues to function, changing only the form of external manifestation. For law enforcement agencies, this means that the search for a formal organizer is no longer a sufficient condition for success, since the criminal environment can exist even after the loss of individual coordinators.

An equally important feature is the high recovery rate after blocking and suppressing. The digital criminal environment has long mastered the practice of multiple redundancy. Removing a communication channel, closing one site, restricting access to a certain resource or identifying a separate group of participants does not stop illegal activity, but most often transfers it to another space, to another site, under a different designation and with new technical parameters. Such an environment is prepared in advance for state intervention: spare notification channels, mirror resources, hidden methods of notifying the audience, conditional transition signals, pre-distributed lists of new access points are created. This implies the most important practical conclusion: a one-time restrictive impact without subsequent systemic support often only records the moment of migration, but does not stop the criminal process. Moreover, in some cases, blocking one visible link even contributes to additional consolidation of the community, which begins to perceive itself as a beleaguered but viable environment, requiring even greater closeness and discipline.

Of particular difficulty is the international nature of communications, which destroys the usual territorial ideas about the crime. In a digital environment, the organizer can be in one country, the technical intermediary in another, the performer in the third, the victim in the fourth, and the money trail can pass through a chain of sites and settlement funds outside the jurisdiction of each of these states. At the same time, communication between participants is carried out continuously, quickly and often within the framework of distributed communities, whose participants have never met in person. For law enforcement agencies, this means that the spatial localization of the crime loses its former certainty, and therefore the traditional mechanisms of departmental and interstate coordination, built on relatively slow procedures for requests and approvals, are lagging behind the pace of criminal activity. If the state machine maintains an inertial rhythm, and the criminal environment operates in the rhythm of instantaneous movement and continuous restructuring, then the advantage inevitably shifts in favor of the criminal.

The use of pseudo-anonymity is one of the most important pillars of the stability of the digital criminal environment. It should be emphasized that this is not about the complete invulnerability of the offender, but about the multi-layered concealment of his true position, which makes it difficult to attribute actions, complicates the linking of digital traces with a specific person and increases the costs of the investigation. The criminal consistently crushes information about himself, changes accounting designations, uses intermediate means of communication, hides his location, resorts to intermediaries, technical substitutions and one-time means of access. Thus, he does not disappear for investigation completely, but seeks to increase the price of his discovery, make it laborious, lengthy and obviously less effective. Strategically, this means that the state is faced not just with the fact of concealment of identity, but with an industry of controlled indistinguishability, which is put on stream and used as a standard measure of criminal security.

Reputational mechanisms, which have long been given insufficient attention, also play a serious role. It is a mistake to believe that the criminal environment is based only on fear or direct profit. On the contrary, digital criminal communities are actively forming their own trust systems: reviews, ratings, evidence of reliability, confirmation of fulfillment of obligations, sanctions for deception, arbitration procedures, admission rules and symbolic signs of belonging to the "verified" circle. These mechanisms make deeply pragmatic sense. They reduce internal uncertainty, reduce the risk of mutual fraud within the criminal environment, strengthen the loyalty of participants and create a false sense of orderliness and security in new faces. Therefore, for law enforcement agencies, a reputation in a criminal environment should be considered as a functional resource of the illegal economy, and not as a side social background. Where trust is maintained between unfamiliar participants, conditions are created for scaling criminal activity.

The combination of open and closed interaction loops deserves special analysis. Modern criminal ecosystems rarely exist only in a completely hidden form. In contrast, they use open visibility as a shell to conceal deep levels of organization. The outer circuit can be disguised as news discussion, household communication, consulting activities, commercial mediation, cultural interests, entertainment communication or mutual assistance. Through this external layer, primary attention is attracted, stakeholders are selected, trust is formed and gradual involvement in more closed forms of communication is carried out. Only then the participant is transferred to special channels, closed groups, personal contacts, technically isolated spaces or temporary communication chains. As a result, the open and hidden here are not opposed, but functionally connected: openness serves as an entrance, closeness serves as a protection mechanism, and the transition between them becomes part of criminal technology.

An equally dangerous feature is the quick transfer of the audience between channels, chats, bots and mirror resources. For modern digital crime, the audience is not a random collection of observers, but a strategic asset. That is why criminal groups in advance build ways to keep it and instantly move. The user is inspired to monitor spare access points, save backup designations, use alternative entry routes, trust certain alerts and, in case of blocking, immediately switch to a new environment. From the point of view of law enforcement agencies, not only the technical side of the issue matters here, but also the social manageability of the audience, its discipline, the habit of obeying internal signals and the willingness to follow the coordinators regardless of the change of site. Where the audience is portable, the very blocking of the information medium loses its decisive importance. The shell is destroyed, but the community is preserved, and therefore the possibility of reproduction of criminal activity is preserved.

Among the most alarming signs is the ability to disguise criminal activity as ordinary information, commercial or social communication. This circumstance has not only tactical, but also deep strategic significance. The criminal environment deliberately dissolves illegal signals in an array of outwardly legitimate everyday life. Illegal offers can look like private ads, recruiting actions like an invitation to work, coordinating a crime like a household discussion, giving directions like neutral correspondence, and role assignments like normal business interactions. Such mimicry pursues several goals at once: to reduce the likelihood of automatic detection, to complicate the legal assessment of the content of the message, to make it difficult to prove intent, and also to ensure the psychological addiction of the audience to the presence of a criminal element. This implies the most important conclusion for law enforcement practice: modern digital crime seeks not only to hide, but also to normalize its presence, fitting itself into the fabric of everyday communication so that the illegal is perceived as familiar, technically neutral and socially tolerant.

All of the above leads to a fundamental conclusion: the object of counteraction should be not only a single illegal material, not only a single performer and not only a specific episode, but the entire infrastructure for the production, distribution, maintenance and reproduction of criminal activity. In other words, if the state is limited to the removal of individual messages, the detention of individual couriers, the blocking of individual pages or the suppression of individual financial transactions, without destroying the mechanisms of staffing, trust exchange, coordination, routing of cash flows, distribution of tasks and the restoration of broken ties, then it strikes at the surface, not at the base. Such a response may be necessary, but it is not enough in itself. Strategically, the fight against digital crime should be aimed at breaking the reproducing cycle, in which criminal activity is not just carried out, but again and again creates conditions for its own continuation.

This directly implies the requirement to switch from a reactive model to a proactive one. The reactive model is based on the logic of the subsequent answer: the crime has been committed, the investigation has begun, evidence is being collected, persons are being identified, procedural measures are being applied. This logic retains its meaning and cannot be canceled, but in a digital criminal environment it turns out to be strategically late. The state, which invariably comes after the completion of the criminal act, actually cedes the initiative to the enemy. On the contrary, the proactive model assumes a shift in attention to early signs of threat formation: the appearance of stable criminogenic patterns of behavior, repetitive ways of involvement, signs of hidden coordination, unusual audience migrations, links between information activity and monetary movements, as well as the recurrence of certain role schemes. This means that law enforcement agencies should be able to see not only what has already been accomplished, but also what is still taking shape.

In a practical sense, such a statement of the question requires, first of all, the identification of criminogenic patterns, that is, steadily repeating configurations of actions, messages, transitions and connections indicating the formation of an unlawful process. This is not about arbitrary suspicion and not about an extensive interpretation of the everyday behavior of citizens, but about the scientifically based allocation of typical signs of a criminal organization of the digital environment. For some types of crime, the repetition of recruiting formulas and the sequence of transferring a person from open communication to a closed circuit can be decisive; for others - a combination of an information offer with quick financial support; for the third, the regular appearance of the same intermediaries serving different outwardly unrelated episodes. It is the repeatability, structural similarity and functional connectivity of the features that matters. Where the scheme is repeated, it is often not an accident that acts, but a system.

Along with this, it is necessary to search for coordination nodes, that is, those points where the flows of instructions, role distribution, resolution of internal disputes, updating access rules, confirmation of the reliability of participants and reallocation of resources intersect. It should be emphasized that such nodes do not always coincide with the formal organizer. Often, the central figure is hidden or generally dispersed, while real management is carried out through a set of intermediary centers: technical, financial, information, personnel. In one case, the key is a person who does not commit the main criminal act, but ensures the admission of new participants. In another, an intermediary who supports trust and calculations. In the third - an administrator who does not touch an illegal product, but connects manufacturers, distributors and performers. Therefore, a coordination node is not necessarily the top of a hierarchy; this is a point whose loss is painful for the entire network.

Equally important is the identification of recruitment mechanisms, since it is through them that the digital criminal environment turns a casual observer into a participant, then into an executor, and sometimes into a convinced bearer of the criminal norm. Recruitment in the digital space is rarely crude and straightforward. Much more often, it is based on gradual retraction: first, a person is offered harmless interaction, then they demonstrate the ease of earning money, then they normalize the risk, then replace the legal assessment with everyday excuses, then they include him in a small group, where the psychological pressure of belonging is triggered. In the future, test orders, partial obligations, the accumulation of mutual compromising information and the transformation of the contractor into a dependent link follow. For the state, understanding these stages is extremely important, since effective prevention does not begin at the stage of completed involvement, but at the stage of the first signs of criminal selection and psychological processing.

A special place is occupied by the analysis of digital routes for the movement of illegal services, funds, information and performers. Modern crime exists as a movement: from proposal to contact, from contact to agreement, from agreement to calculation, from calculation to execution, from execution to concealment of traces, from concealment to restoration of the channel. Each of these transitions leaves traces not necessarily in the form of direct recognition, but in the form of a sequence of actions, repeated connections, temporal coincidences, anomalous movements and functionally conjugate events. The task of law enforcement agencies is not only to fix the final result, but also to reconstruct the traffic chain. The route of a crime is often more important than its individual point, because it is in the route that intermediaries, reserve links, vulnerabilities and hidden service centers appear.

All this leads to the need for a new institutional view. Law enforcement agencies should consider digital crime not as a peripheral application to traditional forms of illegal activity, but as an environment in which old ones are re-organized and new forms of criminal behavior are born. In this environment, not only the way a crime is committed, but also the logic of criminal stability, scaling and self-preservation is changing. That is why successful counteraction is impossible without combining legal analysis, criminology, organization theory, social psychology, linguistic research of communication, the study of network connections and constant interdepartmental interaction. It is not necessary to partially adapt the old methods to the new conditions, but to form a full-fledged strategy of a proactive state presence in the digital space.

So, the strategic statement of the problem for law enforcement agencies should proceed from several immutable provisions. First, digital crime is not a collection of individual incidents, but a complex ecosystem with the ability to self-organize, migrate and reproduce. Secondly, its stability is ensured by the distribution, speed of restoration, international relations, pseudo-anonymity, internal trust

mechanisms, the connection of open and closed contours, audience portability and mimicry for legitimate communication. Thirdly, the entire infrastructure of criminal existence, and not just individual manifestations, should be the true object of opposition. Fourth, strategic success is possible only by moving to proactive identification of criminogenic patterns, coordination nodes, recruitment mechanisms and routes of movement of illegal resources. This is the main task of the modern state: not to catch up with the criminal environment after the next episode, but to deprive it of the ability to organize, expand and re-birth.

3. RECOMMENDATIONS FOR LAW ENFORCEMENT AGENCIES

3.1. creation of specialized interdepartmental centers of digital counteraction

In modern conditions, crime has finally gone beyond the usual material space and is firmly entrenched in the digital environment, where the speed of information transfer, anonymization of participants, branching of communication channels and the cross-border nature of interactions greatly strengthen the stability of criminal entities. It is here today that criminal schemes are formed, recruitment is carried out, illegal actions are coordinated, roles are distributed, criminal proceeds are legalized, traces are destroyed and constant work is being done to evade state control. At the same time, not only the technical equipment of criminal networks, but also their organizational flexibility poses a particular danger: they act quickly, decentralized, secretly and are able to adapt with lightning speed to changes in law enforcement practice. In this situation, departmental disunity ceases to be just an administrative flaw - it turns into a direct factor in the vulnerability of the state.

Therefore, the creation of permanent specialized interdepartmental centers of digital counteraction should not be considered as an optional organizational measure, but as a necessary condition for ensuring the effectiveness of the fight against modern crime. Such centers are designed to combine in a single institutional structure those forces and means that, when disconnected, inevitably lose a significant part of their potential. We are talking about the unification of operational units, units for combating crime in the digital environment, structures specializing in combating organized crime, financial intelligence units, specialists in the field of digital forensics, analysts of open sources and social environments, experts in linguistic and behavioral analysis, as well as representatives of the prosecutor's office and investigative bodies. Only such a union allows you to bridge the dangerous gap between the detection of signs of criminal activity, its analytical comprehension, procedural consolidation of evidence and the subsequent prosecution of the perpetrators.

The meaning of the creation of these centers is not in the mechanical concentration of representatives of various departments in one room and not in the formal institution of the next coordination structure. Their fundamental task

is to form a unified rapid response system in which operational, analytical, technical and procedural resources act as parts of one state mechanism. If such a mechanism is not created, the information obtained by one unit remains inaccessible to another; traces of criminal activity are lost due to delay; digital evidence is not properly secured; financial flows are identified late; international requests are sent when criminal entities have already changed the communication channels used, settlement means and identification features. As a result, the state machine, possessing a significant set of forces and means, acts slower and more fragmented than criminal networks, for which speed has long become the main resource for survival.

It should be emphasized that a specialized interdepartmental center for digital counteraction should be built on the principles of constant, not episodic interaction. Practice shows that temporary working groups created for a specific case or in response to an already developed crisis are not able to ensure a steady accumulation of competencies, the formation of uniform methods, the reproducibility of analytical decisions and the reliability of interdepartmental information links. Only a permanent structure can turn disparate professional skills into a holistic system of state opposition. The constant mode of operation allows not only to respond to crimes already committed, but also to proactively identify threats, observe the transformation of criminal models, track technological innovations among criminal communities and prepare legal, organizational and tactical responses in advance.

The composition of such a center should be determined by the logic of digital crime itself, which is complex, multi-layered and interdisciplinary. Operational units are necessary to obtain primary information, document the activities of suspects, conduct covert activities and practical implementation of the developed materials. Units specializing in combating crime in the digital environment provide an understanding of the technical architecture of illegal activities, ways to hide digital traces, anonymization mechanisms and features of the functioning of distributed communication platforms. Organized crime units bring to the work of the center experience in identifying and suppressing stable criminal communities, knowledge in the field of criminal hierarchy, role distribution, internal disciplinary mechanisms and methods of external cover for illegal activities. Financial intelligence allows you to reveal the movement of criminal proceeds, establish schemes for their dispersion and disguise, identify the connection between digital activity and the material base of the criminal community.

The role of specialists in the field of digital forensics is extremely important. It is they who ensure the correct detection, removal, preservation, research and interpretation of digital traces, without which even the most valuable information risks losing its evidentiary value. In conditions when criminals actively use remote storage of information, encrypted communication channels,

multilayer identification systems and methods of automatic destruction of content, errors at the stage of technical fixation may turn out to be irreversible. Digital evidence is fragile: it is easy to lose, distort, challenge, and therefore professionalism in this area should not be an auxiliary, but a backbone element of all interdepartmental work.

Analysts of open sources and social environments, as well as specialists in linguistic and behavioral analysis, are equally important. Their participation allows you to go beyond purely technical observation and see in the digital space not a set of disparate messages, but a complex environment of communicative signals, semantic codes, symbolic markers and behavioral patterns. Criminal communities rarely speak directly about their intentions; they use jargon, allegories, allusions, stable rhetorical formulas, group memetic constructions, substitute designations of goods, services and actions. The analysis of such elements makes it possible to establish the true content of the communication, to identify the degree of involvement of the participants, to recognize the stages of preparation of the crime, to distinguish a casual observer from an active coordinator. Moreover, behavioral analysis allows you to identify typical scenarios of digital conspiracy, determine the moments of a change of tactics, record signs of intra-group tension, preparation for the movement of assets, or attempts to urgently curtail the communication infrastructure.

The presence of representatives of the prosecutor's office and investigative bodies as part of the center is of fundamental importance. For a long time, a destructive model persisted in law enforcement practice, in which operational material and investigative perspective exist, as it were, in different worlds: some collect information, not always correlating it with future requirements of evidence, others receive this information late and in a form that does not allow them to be fully introduced into criminal proceedings. Meanwhile, in the fight against digital-age crime, procedural impeccability should accompany work from the start, not emerge after the fact as belated legal clearance. The participation of investigative and supervisory representatives allows at an early stage to determine the permissible limits for the use of materials, to formulate investigative versions in a timely manner, to ensure the proper preparation of evidence, to develop a strategy for their further presentation and to minimize the risk of recognizing the collected data as unacceptable.

If we talk about the functional purpose of such centers, then first of all they should carry out constant monitoring of high-risk digital sites. Such sites should be understood not only as well-known network resources, on which illegal content is detected, but also closed communication environments, anonymous interaction channels, thematic communities, semi-legal trading segments, distributed information exchange platforms, as well as rapidly emerging and equally rapidly disappearing digital spaces, designed to recruit participants, sell prohibited items, organize fraudulent schemes, distribution of extremist

materials, coordination of violent actions and other forms of criminal activity. Monitoring should not be limited to mechanical monitoring of the content of messages. It should include identifying activity dynamics, identifying key communicators, tracking lexical code changes, identifying coordination peaks and transitions from propaganda rhetoric to practical guidance.

The second most important area of work should be mapping criminal networks and connections. Here we are talking about the systematic identification of not only individuals, but also the entire structure of relations between them: communication channels, stable roles, coordination nodes, intermediary figures, connections between digital identifiers and real subjects, routes of movement of funds, contact circuits used for recruitment, supply, payment and concealment of criminal activity. Modern organized crime is strong not by individual actors, but by the architecture of connections. Therefore, countering it should be aimed not so much at isolated identification of individual performers as at opening the entire configuration of the community, its functional centers, backup channels, support financial points and international interfaces. Mapping criminal networks makes it possible to move from episodic response to systemic destruction of criminal infrastructure.

The task of identifying typical models of digital conspiracy deserves special attention. Crime in the digital environment has long developed standard and at the same time constantly updated ways to hide their activities. These include fragmentation of communication between different sites, separation of roles between media, using temporary accounts, switching to code language, disguising criminal discussions as everyday communication, the use of remote control, the substitution of geographical and technical signs of presence, the use of intermediaries for the transmission of instructions and means, a sharp change in the intensity of communication before or after the commission of a crime, as well as creating false information trails aimed at disorienting law enforcement. The task of the center is not just to record such techniques after the fact, but to create their classifications, highlight repeating patterns, form signs of early recognition and turn them into practical guidelines for operational and investigative units. Those who learn to see conspiracy as a system will deprive the criminal environment of its main advantage - invisibility.

The next key function of the interdepartmental center should be to support operational developments. Unlike a disparate model, in which each unit conducts only its own fragment of work, the center provides continuous analytical, technical and procedural support for the development from the moment of the initial signal to the stage of initiating a case, bringing charges and, if necessary, international cooperation. This means that any incoming material must be immediately included in the interdepartmental circulation, compared with already available information, checked against digital, financial and behavioral indicators, assessed from the point of view of evidence prospects and risks of loss

of traces. This organization of work does not allow criminal entities to use interdepartmental gaps as a protective space. On the contrary, it creates the effect of continuous persecution, in which each new manifestation of criminal activity is instantly integrated into the overall picture.

Equally important is the accumulation and standardization of digital evidence. Today, one of the most painful problems remains the lack of uniformity in approaches to the collection, description, storage, research and presentation of digital traces. In some divisions, some requirements for fixing content are applied, in others - others; somewhere there is a thorough registration of the sequence of actions with the carrier, and somewhere similar procedures are carried out formally; some specialists describe in detail the data detection environment, others are limited to general formulations. Such heterogeneity undermines confidence in the evidence base, complicates interagency exchange, and creates the basis for procedural disputes and legal challenges. The specialized center should become a place for developing uniform standards for handling digital evidence, mandatory for all involved structures. This applies to the order of fixing screen content, rules for describing network activity, methods of documenting metadata, procedures for removing devices, requirements for ensuring data immutability, conditions for storing copies, regulations for working with remote resources and the procedure for expert interpretation of research results.

A significant place in the activities of the center should be occupied by the preparation of materials for international requests. Digital crime does not recognize state borders, and this is not a metaphor, but a practical reality, confirmed daily by investigations: server capacities can be located in one country, the operator of the criminal scheme in another, the intermediary for transferring funds in the third, and the victims in dozens of states at the same time. With this configuration, any delay in international interaction means the actual loss of the chance for an effective investigation. At the same time, the preparation of materials for foreign partners requires high accuracy, completeness and legal literacy: it is necessary to clearly formulate the circumstances of the case, specify the information sought, indicate their significance for the investigation, comply with procedural requirements, take into account the differences in legal systems and the peculiarities of foreign practices with digital data. A center that accumulates operational, analytical and procedural competence can significantly improve the quality of such requests and reduce the time for their preparation. In the context of the rapid migration of digital traces, it is the speed of international circulation that becomes a decisive factor.

Finally, one of the most significant functions of interdepartmental centers should be the development of standard investigation methods. A special field of state responsibility opens here. While each new case is perceived as almost unique, the law enforcement system is doomed to spend time and again on the

invention of what should have long been translated into the form of stable algorithms. Typing, meanwhile, does not mean coarsening reality; on the contrary, it allows you to identify stable mechanisms of criminal activity, determine the optimal sequence of actions, establish priorities for data seizure, form lists of primary questions for specialists, consolidate models of interdepartmental interaction, develop standard signs of a threat and thereby dramatically improve the quality and speed of the investigation. The technique in the field of digital counteraction is not a bureaucratic document, but a concentrated expression of accumulated professional experience, turned into a tool of practical efficiency.

It should also be noted that the activities of interdepartmental centers cannot be complete without a single internal system of accounting, comparison and assessment of information. This is not only about storing materials, but also about the formation of an integrated analytical space, where digital traces, financial transactions, data on communications, behavioral characteristics, open-source information and procedural documents are linked into a single evidence and intelligence picture. Such a system should provide for the identification of hidden connections, automated warning of the coincidence of significant features, quick access to previously accumulated materials, recording the progress of interdepartmental work and the possibility of retrospective analysis of already completed cases in order to improve practice. Without memory, the system is blind; without comparing information, she is helpless; without analytical unity, it loses to a criminal network that has long learned to act as a whole.

The organizational model of the center should provide for a clear distribution of powers, regulated exchange of information, modes of admission to materials of varying degrees of sensitivity, a system of personal responsibility for the completeness and timeliness of data entry, as well as procedures for the urgent convening of interdepartmental groups in case of detection of signs of an imminent threat. A constant educational and methodological circuit is also needed, since the criminal environment updates its means and techniques much faster than the traditional departmental system manages to process the experience gained. Therefore, the center must perform not only an operational-analytical, but also an educational function: analyze completed cases, form databases of typical errors, distribute guidelines, organize training of employees to work with new forms of digital crime.

In a broader sense, the creation of specialized interdepartmental centers of digital counteraction means a change in the very philosophy of law enforcement. The state should abandon the outdated illusion that the crime can be understood, investigated and suppressed within a narrow departmental framework, when each participant sees only his own part of the picture and jealously protects it from others. This approach was not enough yesterday; today it just gets

dangerous. Criminal networks are defeated not by the number of disparate structures, but by the unity of will, the speed of information exchange, the depth of analysis and the procedural impeccability of joint actions. That is why the interdepartmental center of digital counteraction should be considered as a necessary supporting institution of a modern security system, as a tool not of local departmental convenience, but of strategic state self-sufficiency in the face of rapidly evolving crime.

Thus, the creation of permanent specialized interdepartmental centers of digital counteraction meets several fundamental tasks at once: it ensures overcoming departmental disunity, accelerates the detection and suppression of criminal activity, improves the quality of the evidence base, strengthens international interaction, contributes to the development of uniform methodological approaches and creates conditions for proactive, not delayed response to threats. And if the state really intends not to catch up with crime, but to get ahead of it, then such centers should become not a peripheral element of the law enforcement mechanism, but its nervous node, its analytical heart, its decisive means in the struggle for control of the digital space, where today the security of society, law and order and sovereignty are increasingly determined.

3.2. Development of digital intelligence and criminal analysis

Modern organized crime has long ceased to be just a collection of disparate episodes of violence, extortion, illegal trafficking in prohibited substances, weapons, people and capital. Today, it increasingly exists as a complex, distributed, technologically mediated environment where criminal activity relies not only on physical coercion, but also on managing information flows, hiding digital traces, and constantly reproducing communication channels, confidence circuits, calculation mechanisms and methods of conspiracy. Under these conditions, the law enforcement agencies face not a private, but a strategic task: to move from a predominantly reactive suppression of individual episodes to a systematic identification of the architecture of criminal activity, its repeating functions, its internal dependencies and points of vulnerability.

That is why the development of digital intelligence and criminal analysis should not be considered as an auxiliary direction, but as one of the central foundations of modern law enforcement policy. We are talking about the formation of such an analytical ability of the state, which allows us to see the criminal environment not in the form of a set of disparate messages, but as an integral structure: with its hierarchy, distribution of roles, logistics, recruitment mechanisms, funding channels, information cover schemes and reproducible behavior models. Otherwise, law enforcement agencies are doomed to endlessly fight against external manifestations of criminal activity, without affecting its organizational core.

The analysis of open data is of fundamental importance here. It should not be understood as the mechanical collection of publicly available information, but the systematic extraction of operationally significant information from a variety of heterogeneous sources: pages in online communities, distribution channels for messages, videos, announcements, forums, marketplaces, archives of domain records, registries of legal entities, judicial acts, publications in the media, services for posting vacancies, open cartographic information, records on the movement of goods, images of objects, traces of digital advertising and other arrays, which individually may seem neutral, but in the aggregate reveal hidden forms of criminal coordination. The power of open data lies in the fact that criminal structures, no matter how carefully they disguise themselves, are forced to leave traces of their activities in the space of public communication. They need to announce a set of performers, maintain the recognition of illegal sites, move the audience between channels, respond to the actions of competitors and law enforcement agencies, confirm the "reliability" of their intermediaries, and maintain trust in the criminal environment. All this creates an array of features to be identified, compared and legally evaluated.

No less important area is intelligence on social media platforms and platform communications. This direction requires the security forces to deeply understand that criminal communities today build their influence not only through direct contact, but also through the management of attention, emotions, loyalty and audience habits. In a networked environment, crime acts as a special influence system: it spreads symbolism, forms speech clichés, cultivates rituals of "trust," imposes legends about its own invulnerability, creates a false picture of mass and stability, normalizes criminal behavior through everyday language of communication. The study of this environment should include not only tracking specific messages, but also analyzing the dynamics of communities, user migration between channels, the rhythm of publication activity, changing methods of disguise, ways to involve minors and socially vulnerable persons, as well as the features of digital self-description of criminal intermediaries and coordinators. The key scientific and practical conclusion is that criminal communication is almost never chaotic: even with external fragmentation, it is subject to stable rules of signaling, admission, confirmation, role distribution and execution control.

A special place should be occupied by the analysis of connections between subjects, communication channels, automated accounts, electronic wallets, domain names, technical devices and other digital entities. It is this approach that makes it possible to move from the study of an individual object to the understanding of the criminal network as a functional system. For law enforcement practice, this means the need to identify not only direct, but also indirect connections: coincidences in the time of activity, intersections in the used speech templates, repeating details for calculations, common technical features of the infrastructure, typical user transition routes, similar forwarding

chains, coinciding publication intervals, uniform style of announcement design, synchronism of actions in response to external pressure. Link analysis is especially important because organized crime deliberately crushes its structure, seeking to make each link seemingly autonomous. However, functional dependencies remain between these links, and the analyst's task is not to succumb to the illusion of fragmentation, but to restore a hidden system of coordination. Where criminals see conspiracy through role splitting, the state should see integrity through reconstruction of ties.

A necessary element of modern analytical work is the identification of repeated criminal scenarios. Organized crime is vulnerable not at the points where it claims to be the loudest, but where it is forced to constantly reproduce the same organizational actions. She needs to transfer the audience from one channel to another after blocking, publish signals about the availability of goods or services, collect payment through chains of intermediaries, coordinate couriers or mortgagees, check the loyalty and discipline of performers, resolve conflicts, maintain a reputation, build up a customer base, respond to emergency situations, hide traces of failures and losses. All these forms repeated criminal cycles that can be described, classified and formed the basis of predictive models. When law enforcement agencies identify such cycles, they are able to act not only after the crime has been committed, but also at the previous stages - at the time of preparing the infrastructure, recruiting performers, testing new channels, changing settlement mechanisms, and restructuring communication routes. In other words, the analysis of repeated scenarios translates law enforcement from late fixation to proactive intervention.

This is directly related to the establishment of coincidences between different digital identities. In conditions of network crime, the same subject can act under many names, use different platforms, change methods of self-presentation, use separate channels to communicate with customers, others to communicate with intermediaries, third to calculate, fourth to recruit new participants. The offender seeks to break the unity of his own image, to turn his activities into a set of unrelated masks. Therefore, it is critical for law enforcement agencies to develop methods to establish that several seemingly independent digital profiles can have the same person, the same group, or a single control center. The basis for such a conclusion can be not only technical features, but also features of speech behavior, repetitive communication patterns, typical spelling errors, stable time intervals of activity, familiar methods of message design, repetitive models of financial behavior, similarity of details, a single set of used images, intersections in contact chains. The significance of such work can hardly be overestimated: as long as the criminal network successfully multiplies fictitious personalities, it retains mobility, stability and the ability to quickly recover from local losses. When these masks are analytically reduced to real subjects and coordination centers, the criminal environment loses its main advantage - anonymized multiplicity.

An extremely important area is the restoration of the chronology of criminal activity. It is not enough to know who acted where and how to uncover organized forms of crime. It is necessary to understand when and in what sequence the events unfolded, which actions were preparatory, which were masking, which were coordination, which were calculated, which were a reaction to external influences. Chronological reconstruction allows you to see the logic of the criminal operation: from the appearance of primary signals and trial activity to the deployment of a stable scheme, its expansion, crisis, transformation and possible decay. In practical terms, such a reconstruction makes it possible to establish causal relationships between episodes, identify initiators, distinguish the decision-making center from ordinary performers, determine the phases of the greatest network vulnerability, and also prove the consistency of the actions of participants within the framework of a single criminal plan. The time dimension is not secondary here: it is this that turns a set of disparate digital traces into a provable history of criminal activity.

No less significant is the analysis of the disorganization of the criminal network, that is, the identification of such key nodes, the elimination of which maximally weakens its viability. The mistake of many law enforcement approaches is that efforts focus on the most visible participants or on the noisiest channels of information dissemination. However, the most visible is not always the most important. A criminal network can easily be sacrificed by an external distributor, a secondary intermediary, a public channel or a replaced performer, if its settlement mechanisms, trust contours, coordination routes and technical administrators are preserved. Consequently, the task of law enforcement agencies is to identify not just network participants, but its structurally critical elements: those nodes through which flows of trust, money, commands, admission, confirmation, redirection of the audience, recovery after blocking pass. The impact on such nodes can not only reduce visible activity, but cause a system failure, increase the internal costs of a criminal organization, undermine its ability to reproduce itself, sow distrust between participants and make further functioning risky and expensive.

A broader methodological conclusion follows from this: the modern fight against organized crime should be focused not only on the detection of prohibited content or individual perpetrators, but also on the study of the repeated organizational functions of the criminal environment. The criminal network does not live only by crimes as such; she lives by procedures without which crimes cannot be constantly reproduced. It needs to attract new participants, check old ones, provide calculations, maintain communication channels, compensate for losses, form reputation guarantees, manage the fear of exposure, distribute roles, document internal obligations in informal forms, transfer the audience to reserve resources, erase traces of errors and leaks. It is these mandatory functions that, repeated over and over again, create an analytically vulnerable contour. Where there is repetition, there is a pattern. Where there is a

pattern, detection, measurement, forecasting and targeted suppression are possible there.

To achieve these goals, law enforcement agencies need not episodic modernization, but a deep institutional restructuring of analytical work. First of all, the creation of sustainable interdepartmental mechanisms for combining information is required, since digital traces of criminal activity are almost always distributed between different bodies, levels of management and subject areas. If one service sees financial signs, another - network infrastructure, the third - migration of communication channels, the fourth - the movement of performers, but this information is not reduced to the big picture, the state itself reproduces the fragmentation on which the criminal network parasitizes. Therefore, interagency analytical data cross-linking should become a mandatory principle, not an exception. In this case, we are not talking about the mechanical accumulation of information arrays, but about the development of uniform rules for describing objects, events, connections and timestamps so that heterogeneous information can be compared in a single evidence and operational logic.

A qualitatively different level of personnel training is also needed. Digital intelligence and criminal analysis require specialists who are able to think at the same time legally, operationally, technically and sociologically. It is not enough to own individual methods of finding information; it is necessary to be able to distinguish between genuine signal and noise, to understand the methods of self-organization of network communities, to recognize masking techniques, to work with incomplete and contradictory data, to build testable hypotheses, to separate the probabilistic conclusion from the proven fact, to take into account the limits of permissible interference in the sphere of citizens' rights. A new type of professionalism in law enforcement is the ability to combine rigorous evidence with analytical foresight. Without this, the digital environment will continue to give criminals an advantage in speed, plasticity and stealth.

Of particular note is the question of the legal and ethical framework for such activities. Increased digital intelligence should not turn into an arbitrary invasion of privacy, into indecipherable accumulation of information, or into substitution of evidence by assumption. On the contrary, the more powerful the analytical tools of the state, the stricter the legal guarantees for its application should be. A scientifically based and socially legitimate model of digital criminal analysis implies a clear distinction between open information, promptly significant information, permissible verification procedures, procedurally significant evidence and measures to restrict rights. Only in this case, the analytical strengthening of law enforcement agencies will work not against the rule of law, but in its defense. A state fighting online crime should not be like it in its pursuit of opacity and arbitrariness; its advantage must be legality, accuracy and responsibility.

Finally, it is fundamentally important to realize that in the fight against organized crime, digital analytics cannot be reduced to the role of a service tool. It should become the core of a proactive state action. Where the criminal environment uses digital platforms to disperse traces, the state is obliged to learn how to collect them into a single evidence tissue. Where criminal communities crush identities, the state must restore the subject behind many masks. Where crime relies on repetition of covert organizational procedures, the law enforcement system must turn that repetition into a map of vulnerability. Where the criminal network hopes to survive the blocking of one channel due to the backup infrastructure, the state should hit not on the surface, but by a self-healing mechanism.

Ultimately, it is here that one of the most important lines of modern confrontation between the state and organized crime passes. The winner is not the one who records more individual episodes, but the one who understands the structure of the criminal environment more deeply, faster reveals its patterns and more accurately determines the points of decisive influence. Organized crime must be struck not only by the power of restraint, but also by the power of understanding. And the sooner law enforcement agencies turn digital intelligence and criminal analysis into a priority for state security, the less space criminal networks will have to disguise, reproduce and expand.

3.3. Standardization of digital evidentiary fixation

One of the most acute and at the same time the most underestimated problems of modern law enforcement remain not so much the detection of digital traces of a crime as their proper, legally flawless and technically reliable fixation. In conditions when a significant part of the illegal activity has moved to the electronic environment, the question of the fate of the evidence is decided not only at the time of its identification, but primarily at the time of its fixation. Where there is a lack of uniformity of action, where mandatory rules for handling digital objects have not been developed, where employees act at their own discretion, a justice-damaging gap inevitably arises between the actual detection of a trace and the possibility of its judicial use. In other words, a digital footprint that has not been correctly captured ceases to exist in a procedural sense. This truth should be the basis of the entire departmental policy in the field under consideration.

Digital evidence-based fixation does not require private improvements, but the construction of a holistic, nationwide, normative and methodically verified system. Such a system should be based on the nature of the electronic environment itself, which is characterized by variability, layering, distribution of storage, dependence of content on the time of circulation, the difference between the displayed and actually existing content, as well as the constant threat of automatic deletion, rewriting, hidden change or loss of data. Any message, any correspondence, any posted file, any entry about the time of entry, any clicking

on a link, any list of participants in the conversation, any trace of user interaction with the information platform - all this can have evidentiary value. However, in the absence of standardized fixation rules, the same object can in one case be recognized as admissible evidence, and in the other - rejected by the court as improperly fixed, unverifiable or allowing doubts about authenticity. This situation is incompatible with the principles of legality, equality of law enforcement and the effectiveness of criminal prosecution.

First of all, it is necessary to develop uniform protocols for recording messages, channels, conversations, files, service information about data and reference transitions. We should not talk about departmental memos of a general nature, but about strictly formalized rules that are mandatory for operational units, investigative bodies, expert institutions and other participants in procedural evidence. In these rules, it is necessary to determine which information is subject to mandatory fixation when a digital object is detected: the name of the site or messaging service; Account information the exact name of the channel, conversation, or group; identification designations of participants; date and time of discovery; Date and time displayed in the environment itself Full network hop address Description of the employee's sequence of actions list of technical means used during fixation; Network connection information signs of availability or limitation of content; the presence of deletion, editing, self-destruction of messages or other signs of data instability.

Of particular importance is the distinction between content and its digital context. It is not enough to pin only the text of the message or the image on the screen. It is necessary to record exactly where this object was located, how it was received, in what environment it was displayed, what information accompanied its appearance, what was the position of the object in the general structure of the conversation, whether there were indications of the time of sending, sending, editing, deleting, response message, attaching files, reactions of participants, read status. For the court, it is important not only what is said, but also by whom, when, where, in what sequence and under what circumstances it was done. Therefore, the fixation protocol should cover not only the content itself, but also the entire evidentiary framework that makes this content legally significant.

The need for uniform rules is particularly evident for reference transitions and their associated objects. In a modern electronic environment, content is often placed not directly in a conversation, but through external transitions, temporary pages, distributed storage, hidden invitations, and one-time access addresses. If the employee is limited only to preserving the appearance of the message, without fixing the exact address of the transition, the time of access to it, the sequence of redirects, signs of content availability and its condition at a particular point in time, the evidence loses a significant part of its certifying power. Therefore, national protocols should provide for mandatory fixation of the full resource address, all subsequent redirects, access parameters, opening

time, displayed header information, information about the owner or hosting party, if they are available legally, as well as the results of repeated access to the same address within a reasonable period of time. This is the only way to show the court that the discovered content is not random, artificially created or unidentified information.

Equally important is ensuring that time data is documented in a legally sound manner. Time in digital forensics is not an auxiliary detail, but one of the central elements of evidence-based construction. It is time binding that allows you to establish the sequence of actions, coordination of participants, the moment of formation of intent, the connection between the message and the committed act, the presence of a preliminary conspiracy, the duration of participation in criminal activity, the fact of hiding traces, deleting materials or changing accounts. Meanwhile, temporary information in the electronic environment is often vulnerable: they depend on the device settings, time zone, display features in the site itself, differences between local and server times, synchronization delays, manual adjustment of the system clock, as well as the fact that some sites display time approximately, abbreviated or changes the way it is shown as the record becomes obsolete.

This implies the need to create strict rules for documenting time, in which each fixed value must be accompanied by an indication of the time source, time zone, technical environment in which it is displayed, and how it is compared with the reference time. For law enforcement, it is fundamentally important that the employee does not just rewrite the time designation seen, but certifies exactly what time he records: the system time of the device, the time displayed by the site, the time from the connection log, the time from service records, the time of receiving a response from a remote resource. In each case, a separate reflection of the method of establishing the time value and the degree of its reliability is required. It is advisable to fix the mandatory comparison of the device time with state reference time sources immediately before and after the fixation actions, as well as the mandatory documentation of any discrepancies. If such a procedure is not standardized, the defense will inevitably question the entire time line of events, and with it the reliability of the conclusions of the investigation.

The immediate preservation of rapidly disappearing data requires special consideration. The electronic environment lives according to the laws of fluidity: information that exists at one moment can be irretrievably lost in a few minutes. This category includes not only so-called self-destructing messages, but also displayed for a limited period of browsing history, user presence information, connection records, temporary access keys, intermediate buffers, temporary copies of files, the contents of device RAM, information about current communication sessions, rapidly changing pages and other unstable digital objects. In conditions when such data can disappear automatically, law enforcement agencies do not have the right to act as if in front of them an

ordinary material object that can lie in the storage chamber for months unchanged. Here delay means the loss of truth.

In this regard, a mandatory procedure should be introduced to immediately respond to the identification of rapidly disappearing data. This procedure should determine what actions should be performed first, which employees are authorized to perform them, in what sequence should be recorded, what information should be saved first of all, how the source environment is maintained, how all manipulations are reflected, and how the risk of data changes is minimized by the fact of their discovery. For some situations, the first priority will be to save the current state of the screen, for others - to unload the message log, for the third - to remove information from RAM, for the fourth - to fix the current communication session and network environment. But in all cases, the principle must be one: first - the preservation of the most fragile, then - more stable; first, loss prevention, then in-depth analysis. Any other logic will inevitably lead to the fact that valuable information will be destroyed in the interval between their discovery and the beginning of the procedural design.

The next cornerstone is the use of certified means of calculating checksums, time verification and recording the chain of custody of evidence. In the digital sphere, one cannot limit oneself to referring to the employee's conscientiousness. Technical confirmation is required that the object has not been changed after removal, copying or unloading, that the time of its fixation is verified that each stage of its handling is reflected in a continuous and verifiable sequence. The checksum of a digital object should be calculated according to the approved rules immediately after its receipt and, if necessary, again at subsequent stages. The results should be entered into protocols, supporting documents and evidence storages. This is not a formality, but a foundation of trust in digital evidence.

The identity of the commit time is equally important. In conditions where the defense can declare that the file was created later, the upload was made at a different moment, and the screen image was made retroactively, simply indicating the employee about the date and time of the protocol is no longer enough. A legally significant consolidation of the very fact of the existence of a particular digital object at a certain moment is required. Therefore, departmental standards should provide for the mandatory use of time certification tools recognized by the state and allowing subsequent verification. This practice will strengthen the evidentiary power of the materials, eliminate disputes about the time of their origin and significantly increase the stability of the prosecution in court.

Particular attention should be paid to the chain of custody of evidence, that is, the continuous documentation of all actions with a digital object from the moment it is discovered until it is presented in court. For an ordinary material proof, this problem has long been realized, but in relation to digital objects, it acquires many times greater complexity. The same file can exist in multiple copies; The working

copy may be different from the original copy. Service information may change automatically when you open a file. when transferring to another media, data corruption is possible; When investigating without following the rules - unintended content change. Therefore, national standards should require mandatory demarcation of the original object, its bitwise copy, working copy for research and copy for judicial review. It should be clear and verifiable who, when, on what basis and for what purpose gained access to each copy, what actions he performed with it, what means he used, where the object was stored, under what conditions its safety was ensured and by whom the invariability was confirmed at each stage. If this chain is broken, the evidence is threatened with exclusion, and with it the entire evidentiary system in the case may collapse.

Hence the need to form national standards for obtaining images from the screen, unloading and checking digital objects. At first glance, it may seem that the image from the screen is the easiest way to secure information. But this is where enforcement is especially often confronted with procedural helplessness. The image from the screen is often performed without specifying the device, without fixing the address bar, without displaying the system time, without a visible source structure, without confirming that the image belongs specifically to the account under study, and not to an artificially created imitation. This practice should be recognized as unacceptably primitive. The national standard should strictly define what exactly should be contained in the screen image and in the accompanying protocol: full display of the interface; Application or page name account details; System date and time navigation elements; visible signs of source authenticity; a sequence of transitions preceding the acquisition of the image; information about the facility that was saved; Checksum of the generated image file information on further storage.

However, this is not enough. In a scientifically and procedurally mature system, the image from the screen should not be considered a self-sufficient means of fixation where it is possible to obtain a more complete digital trace. If technically and legally possible, priority should be given to uploading source data, log records, file copies, service information about data and other forms of fixation that allow you to check the origin, integrity and internal structure of the object. The image from the screen should be used either as an initial urgent measure in case of a threat of loss, either as an additional means of visual demonstration of the detected content, but not as the only support for the prosecution in complex cases of criminal community activities, coordination of illegal actions, involvement of new participants, illegal circulation of prohibited items, extremist and terrorist propaganda, blackmail, extortion, fraud and other acts, where electronic correspondence forms the very nerve of the criminal mechanism.

Standardization of uploading digital objects also requires deep regulation. It is necessary to determine in what formats it is permissible to save correspondence,

files and accompanying information; how to ensure the completeness of unloading; how information about non-downloaded or unavailable elements is recorded; how errors, omissions, access restrictions, automatic content reductions are documented; how to verify that the uploaded array matches the content displayed in the source environment. It is critical to have procedures in place to re-verify the upload and match it to visually observed content. This is the only way to avoid a situation where there is only a fragmentary or partially distorted copy of the digital interaction in the case, and key messages, dates or attachments are lost or disputed.

The fundamental component of standardization is the verification of digital objects, that is, the establishment of their authenticity, integrity, relatability and reproducibility. Verification cannot be reduced to the subjective belief of the employee that "he saw it with his own eyes." Need a set of verification actions: mapping multiple sources of information; establishing a logical relationship between the content and the account; Analysis of editing or installation characteristics assessment of compliance of time marks; verification of service data information; comparison with seized devices, information of telecom operators, testimony of persons, results of inspection and expert research. The state standard should consolidate the minimum mandatory set of such checks for various types of digital objects. Otherwise, in one region and even in one division, authenticity will be considered established on the basis of a superficial visual inspection, and in another, it will require full expert confirmation. Such inconsistency undermines the unity of law enforcement and directly damages the authority of the state.

Finally, this whole system will remain a dead letter without purposeful training of investigators and operational employees in the correct work with disappearing content. The electronic environment is merciless to unprofessionalism. One careless touch of the screen, one automatic opening of a conversation, one login to an account without following procedures, one incorrectly performed copy - and the evidence either disappears or turns out to be infected with a doubt about its purity. Consequently, training should cease to be an episodic acquaintance with technical innovations and turn into a systemic professional specialization.

Such training should not be abstract, but applied. Employees should be able to distinguish the types of digital objects according to their degree of stability; understand which data disappears immediately, which - after a limited time, and which are saved for a long time; know signs of edited and self-destructing messages; own the method of initial recording of correspondence, images, sound messages, video recordings, files, placement information, lists of participants, time stamps and network transitions; be able to preserve the digital environment without destroying it; competently draw up procedural documents; interact with specialists and experts; Understand the limits of what your device and account can be affected by. In addition, training should include modeling of typical errors

and their legal consequences. The employee is obliged to clearly realize: violation of the fixation procedure is not just a technical flaw, but the potential death of the entire case, the result of many months of work, crossed out at the hearing with one reasonable doubt about the reliability of the evidence.

Personnel training should be accompanied by the creation of departmental training centers, unified advanced training programs, mandatory periodic certification and the formation of a stable practice of joint work of investigators, operational employees, computer forensics specialists and proceduralists. Moreover, it is necessary to overcome the dangerous misconception that digital fixation is a matter of narrow technical specialists, to whom the main composition of law enforcement agencies can turn only in exceptional cases. On the contrary, in modern conditions it should be one of the basic competencies of each employee in contact with the disclosure and investigation of crimes. Where the digital footprint has become an everyday form of a criminal footprint, its competent consolidation should become an everyday skill of the state.

In a broader sense, the standardization of digital evidentiary fixation is a matter not only of procedural technology, but also of the legal civilization of the state. Justice cannot depend on the case, the personal knowledge of a particular employee, or the technical ingenuity of an individual unit. It should be based on uniform, reproducible, verifiable and binding rules for dealing with digital reality. Only with this approach is it possible to ensure both the effectiveness of criminal prosecution, and the observance of individual rights, and the sustainability of court decisions.

It should be emphasized that digital forensics in the modern era has ceased to be an auxiliary area. She became one of the decisive lines of the struggle for proof. It is possible to identify a criminal network, establish its participants, trace coordination channels, reveal mechanisms for financing and disseminating illegal content, but in the absence of a reliable digital fixation system, all this work can crumble in the judicial stage. The court does not reach a damning conclusion based on guesswork, professional intuition, or operational conviction; it requires evidence whose origin, integrity and admissibility are beyond reasonable doubt. That is why standardization in this area should not be considered as a private technical reform, but as one of the priority state tasks in the field of ensuring the rule of law.

So, for law enforcement agencies, the following should be approved as an unconditional guideline: uniform protocols for fixing digital objects, legally stable documentation of time, immediate preservation of rapidly disappearing data, mandatory use of certified integrity controls, certification of time and storage chain management, national standards for obtaining images from the screen, unloading and verification of digital objects, as well as systemic training. Only a combination of these has begun to turn a disparate practice into a truly state system of digital evidence. And only such a system can prevent the detected

trace of a crime from disappearing not in the abyss of electronic space, but in the gaps of law enforcement helplessness.

3.4. Implementation of risk-oriented prioritization model

One of the most significant mistakes in the activities of law enforcement agencies in countering crime in the digital environment remains the desire to respond to all detected manifestations of illegal activity as equivalent in terms of the degree of public danger. Such an approach may outwardly create the impression of high official activity, but in reality it leads to a dispersion of forces, overloading of investigative and operational units, loss of controllability and, which is especially dangerous, to a strategic weakening of the state in the face of really large and systemic threats. Not all illegal activity in the digital environment has the same level of danger, the same consequences and the same potential for destructive effects on society, the economy and government institutions. That is why modern practices to counter digital crime should not rely on a mechanical increase in the number of checks, detentions and initiated cases, but on a verified, scientifically based, legally stable and organizationally disciplined model of prioritization based on risk assessment.

The essence of the risk-based approach is that the state deliberately abandons the illusion of total and equally intensive control over all digital offenses and instead focuses its main forces on those segments of the criminal environment, which cause the greatest damage, have a high degree of reproducibility, are associated with organized structures, affect the critical interests of the individual, society and the state, and are also able to scale rapidly, evading traditional preventive measures. Priority should be determined by the visibility of the crime, not by the volume of public outcry and not by the simplicity of the reporting result, but by the depth of the threat and the severity of the consequences. If a department directs basic resources to episodic, insignificant or technically primitive violations just because they are easier to document and faster to bring to a procedural result, it thereby leaves in the shadows complex, hierarchically organized, financially secure criminal networks that in reality form the core of modern digital crime.

Building a risk-oriented model involves the creation of a multi-level threat matrix, in which each identified object of operational interest is evaluated according to a set of criteria. Such criteria include the scale of the harm caused or potential, the number of possible victims, the degree of organization of the group, the presence of cross-border ties, the stability of the criminal infrastructure, the volume of illegal income, the connection with violent forms of crime, the impact on minors, involvement in corruption, the possibility of quick recovery after suppression, the use of concealment means, as well as the likelihood of destabilizing public security and undermining state interests. The threat matrix should not be a formal list of categories, but a working tool for the distribution of forces, powers, time, technical means and procedural attention. Without this,

any declaration of priorities will remain departmental rhetoric that cannot change the real state of affairs.

Such a model should prioritize transnational criminal networks. Their danger is determined not only by the geographical scope, but also by the special quality of the criminal organization. We are talking about structures that use the difference in legal regimes, discrepancies in national procedures, territorial dispersal of performers and intermediaries, as well as complex chains of financial and technical concealment. Such networks are able to coordinate the illegal circulation of goods, data, funds and criminal services in several jurisdictions at once, making it sharply difficult to identify organizers, seize assets and consolidate evidence. The transnational network is dangerous because it does not attack an individual citizen or even a separate region - it tests the very ability of the state to protect its rule of law in the context of the digital interconnectedness of the world. If law enforcement agencies do not classify such structures as the highest risk category, they inevitably find themselves in the position of a catch-up party responding to the consequences instead of destroying the center for coordinating criminal activity.

Recruitment channels for violent and extremist structures should have a special place in the priority system. Here we are talking not just about the distribution of prohibited materials, but about a criminal impact on human consciousness, about the targeted formation of readiness for violence, about involvement in activities directed against public security, interethnic peace and constitutional order. In the digital environment, recruitment has acquired new forms: it can disguise itself as communication of interests, ideological discussions, emotional support, a false sense of belonging to a "chosen circle," and the rhetoric of the struggle for justice. A particularly alarming circumstance is that such channels are often aimed at young people, people with an unstable psyche, socially isolated citizens and those who are experiencing a personal crisis. Where the state does not recognize digital recruitment on time, tomorrow it is no longer faced with text on the screen, but with violence on the street, in an educational institution, at a transport facility or in a place of mass stay of people. Therefore, the identification, documentation and suppression of such channels should be considered as one of the unconditional highest priorities.

The segments of the digital environment that ensure the illicit trafficking of weapons, drugs and forged or stolen documents are also reasonably classified as the most dangerous threats. These phenomena cannot be perceived in isolation as "separate markets" for criminal activity. In reality, they are closely intertwined and form a mutually supportive criminal ecosystem, where one type of illegal activity fuels another. Arms trafficking increases the likelihood of violent crime and terrorist acts; the sale of narcotic drugs destroys the health of the nation, fuels organized crime and creates stable corruption ties; shadow circulation of documents facilitates the legalization of other crimes, concealment of identity,

illegal border crossing, fraud and penetration into economic and state structures. When the digital environment becomes a service space for such flows, we are no longer talking about private episodes, but about the shadow logistics of destroying public safety. Therefore, any nodes connecting sellers, intermediaries, carriers, custodians, manufacturers and financial operators should receive increased priority in operational and investigative work.

An equally important area of prioritization is the fight against fraudulent networks that cause massive damage. The traditional underestimation of such schemes as allegedly "non-violent" crimes is a serious misconception. Massive fraud in the digital environment can affect hundreds of thousands of citizens, deprive them of their savings, destabilize trust in financial institutions, undermine respect for law and create an atmosphere of universal vulnerability. The seeming multiplicity of "small" episodes often hides highly organized structures with a rigid distribution of roles: legend developers, communication operators with victims, technical performers, fundraisers, cashing intermediaries, coordinators and cover persons. Mass fraud is dangerous not only by stolen amounts, but also by the destruction of public trust as the basis of civil trafficking. When a citizen ceases to believe a call, a message, a banking operation, a digital document, not only an individual victim suffers - the very mechanism of public communication suffers. Therefore, priority should not be given to individual performers, but to identifying and defeating the entire network, including control centers, financial channels and schemes for redistributing the stolen.

Strategic threats include trading in personal data and restricted information. In modern society, data about a person, his movements, property status, professional activities, family ties, habits, biometric signs, contacts and digital traces become the most valuable resource of criminal influence. Their illegal circulation serves as the basis for subsequent fraud, extortion, blackmail, identity theft, pressure on officials, penetration into protected systems and preparation of other crimes. A particular danger is that the leakage and illegal sale of such information often remains underestimated due to the lack of immediately visible damage. However, it is from such, at first glance, "auxiliary" arrays that the infrastructure of future crimes is formed. Data trading is not a secondary accompaniment to crime, but its breeding ground, its raw material base, its tool for a pinpoint blow to a person, organization and state. Therefore, law enforcement agencies are obliged to consider the identification of channels of theft, accumulation, systematization and sale of data as activities directly related to the prevention of more serious crimes.

Particularly tough and uncompromising prioritization is necessary in relation to criminal schemes affecting minors. Here the state has no moral right to half-heartedness, procedural relaxation or departmental competition. Any digital environment in which minors are involved in criminal activity, sexual

exploitation, distribution of materials that infringe on sexual integrity, inducement to self-destructive behavior, psychological suppression, blackmail, extortion or manipulative management should be considered as a space of increased criminal danger. The vulnerability of children and adolescents is due not only to age, but also to the specifics of digital communication: high gullibility, desire for recognition, insufficient life experience, inability to assess the hidden motives of the interlocutor, as well as psychological dependence on the opinion of the virtual environment. Crimes against minors in the digital environment are especially dangerous because they affect the personality in the formation stage, leaving a mark not for one day, but for years, and sometimes for life. In the system of state prioritization, such episodes should be automatically transferred to the category of highest significance with mandatory interdepartmental interaction, immediate protection of the victim and accelerated adoption of procedural decisions.

In a special group of priority prosecution, it is necessary to allocate the infrastructure of financial support for organized crime. Organized crime lives not only by force of intention, conspiracy and discipline, but above all by the movement of funds. Where it remains possible to quickly receive, move, split, mask and extract criminal proceeds, the criminal network is able to survive the detention of individual participants, the loss of individual sites and even local operational strikes. On the contrary, the destruction of the financial basis often turns out to be more effective than the suppression of individual performers. The infrastructure of financial support should be understood as a combination of persons, schemes, intermediary links, settlement channels, fictitious business transactions, shell accounts, illegal funds transfer services and other mechanisms that ensure the viability of a criminal organization. To follow only the performer is to fight the shadow; to cut off funding is to strike at the heart of the criminal system. That is why the risk-oriented model should invariably raise any identified links between digital crime and the channels of laundering, redistribution and preservation of illegal income to the top lines of priorities.

Networks related to corruption, sabotage and undermining national security should receive the highest level of attention. Here, digital crime ceases to be a purely criminal problem in the narrow sense and reaches the level of a direct threat to the stability of the state. Corruption networks that use the digital environment to coordinate actions, hide ties, transfer information, distribute rewards and destroy traces, undermine the very basis of legality, since they deprive the state apparatus of internal integrity. Diversionary forms of activity - be it encroachment on life support facilities, transport, communications, management, supply or information systems - can cause panic, disrupt the functioning of territories and cause damage incommensurable with ordinary criminal statistics. Undermining national security can be expressed both in direct coordination of hostile activities and in covert assistance to them through communication channels, financing, recruitment, data collection and

destabilization of social processes. When a criminal network comes into contact with corruption and threats to the security of the state, the issue of prioritization ceases to be a matter of official efficiency - it becomes a matter of political and historical responsibility.

However, listing priority categories alone does not solve the problem if there is no clear mechanism for assessing them. Departments need to fix a system of signs by which the object of operational interest belongs to a particular level of risk. This system should include signs of organization, stability and reproducibility of the scheme; availability of role distribution; signs of professional conspiracy; the use of dummies; links to violence; involvement of minors; damage to critical infrastructure; the amount of stolen or legalized funds; the number of regions or States covered by the activity; the presence of patronage by officials; use of stolen data; the ability to quickly recreate channels after blocking; as well as the potential for public resonance if it is associated with massive damage or destabilization. Priority should be assigned on the basis of measurable and verifiable features, and not by intuition, personal preferences of the manager or pressure of the current agenda. Otherwise, the system will inevitably slide either to subjectivity or to the pursuit of outwardly spectacular, but strategically secondary results.

The practical value of the risk-oriented model lies in the fact that it allows you to build a reasonable distribution of powers between departments. Cases and materials of a high degree of risk must comply with a special regime of analytical support, increased requirements for operational penetration, accelerated interregional interaction, enhanced prosecutorial and investigative coordination, special measures to protect witnesses and victims, priority access to technical and expert resources. In contrast, low-risk episodes can be resolved in a simplified manner, without excessive distraction of personnel and funds. The point of prioritization is not to ignore insignificant violations, but to prevent them from absorbing a resource designed to combat truly dangerous crime. The state, which spends the same effort on the secondary and vital, ultimately loses both there and there.

It is fundamentally important that the risk-oriented model is built not only into operational activities, but also into the procedural support of cases. If a priority object is identified, but its documentation is carried out superficially, without a well-thought-out strategy for collecting, securing and checking evidence, the result will not be a victory for the state, but a collapse of the case in court. For this reason, high priority should mean not only accelerating actions, but also improving their quality: carefully establishing the entire network structure, the role of each participant, funding channels, communication methods, data sources, coordination facts, cross-border elements, connection with other crimes and ultimate beneficiaries. Strong prioritization without a strong evidentiary basis is dangerous as it turns a high-profile case into a high-profile defeat.

Therefore, departments must combine risk-based selection of objects with impeccable compliance with the rule of law, procedural purity and standard of proof.

It is also necessary to emphasize the fact that a risk-oriented model cannot be once and for all approved by the scheme. The criminal environment is changeable, flexible and prone to quickly rebuild under the actions of the state. There are new ways of anonymization, new forms of role distribution, new financial mechanisms, new channels of psychological influence, new forms of disguise for legal activities. Therefore, the threat matrix should be constantly updated on the basis of judicial practice, investigation materials, operational accounting information, the results of interdepartmental exchange, criminological research and analysis of the consequences of already suppressed schemes. Prioritization, which is not capable of updating, inevitably turns into an archive of yesterday's threats and skips the threats of tomorrow. In this matter, the state does not need a one-time campaign, but a sustainable culture of strategic observation, analysis and correction.

Ultimately, the introduction of a risk-oriented prioritization model is not a private organizational measure, but an expression of the maturity of state thinking. It shows whether the department is able to see not only a single episode, but also the entire threat architecture; whether it knows how to distinguish a symptom from the source of the disease; whether it is ready to act not for the sake of a formal indicator, but for the sake of a real reduction in criminal potential. The resources of the state should concentrate on the most dangerous nodes, and not be sprayed on secondary manifestations. This is not just a managerial principle - it is a requirement of common sense, legal responsibility and strategic self-preservation. Where forces are focused on the main thing, the state strengthens sovereignty, protects citizens and destroys criminal systems at their core. In the same place where priorities are blurred, imitation, departmental bustle and belated response to an already ripe threat inevitably triumph.

3.5. Active use of financial intelligence

In the fight against organized crime operating in a digital environment, financial intelligence should not be considered as an auxiliary direction, but as one of the central ways to identify, prove, suppress and subsequently destroy criminal activity. Modern criminal communities can carefully hide communications, change technical platforms, use multi-stage conspiracy schemes, replace the personalities of participants and split the organizational structure into isolated links. However, for all the sophistication of such measures, they almost inevitably leave a monetary footprint, since any sustainable criminal activity requires the receipt, distribution, accumulation, concealment and legalization of material resources. Money feeds the criminal network, ensures its stability, creates opportunities for expansion, bribery, recruitment, technical equipment and evasion of responsibility. That is why the defeat of the financial basis of the

criminal structure in some cases turns out to be more destructive for it than the point seizure of individual technical means or the detention of individual performers.

With regard to organized crime in the digital environment, financial intelligence is also of particular importance because criminal activity here is rarely limited to one territory, one type of income or one transfer scheme. On the contrary, there is a constant interweaving of electronic settlements, settlements through virtual assets, the use of dummies, fictitious contractual grounds, the multiplicity of settlement channels and the fragmentation of flows into many, at first glance, unrelated operations. Behind the external chaos of such a movement of funds is quite rational logic: to complicate the restoration of the chain, to make it difficult to establish a beneficiary, to give criminal income the form of legal turnover. Hence the fundamental conclusion follows: financial analysis should not be an episodic investigative action, but a continuous, systemic and proactive process that accompanies all stages of countering organized crime - from initial detection to execution of a court decision.

First of all, a significant strengthening of interaction with financial monitoring units is required, since it is they who accumulate information that makes it possible to detect non-obvious connections between persons, accounts, payment instruments, business entities and operations that are not formally related to each other in the materials of the initial audit. It should not be about a formal exchange of individual requests and answers, but about building a stable interdepartmental architecture, in which information about suspicious transactions, splitting transfers, transit of funds, atypical behavior of accounts, the use of nominal participants and the appearance of signs of money laundering are immediately included in the general array of evidence-significant information. In conditions when criminal proceeds can move with exceptional speed, delay in the transfer of information actually plays on the side of criminals. Consequently, the efficiency of interdepartmental interaction becomes not an organizational detail, but a condition for real success.

Such interaction should be based on uniform approaches to financial and analytical work. It is important not only to record individual suspicious transactions, but also to establish patterns: the frequency of counterparties, abnormal payment times, the use of the same type of details, the coincidence of access devices, the geographical disproportion of operations, the unusual speed of turnover of funds, the presence of artificial fragmentation and signs of transit. Together, these data make it possible to move from scattered facts to the reconstruction of the criminal financial model, and then to the disclosure of the structure of the criminal network itself. In other words, financial monitoring gives the investigation and operational units not only information about money, but also information about people, roles, dependencies, discipline within the group, its control centers and support channels.

A special place in modern conditions should be occupied by the analysis of transactions with virtual assets, electronic wallets and cashing schemes. A common misconception is that settlements in a distributed accounting environment provide criminals with complete invulnerability. In fact, such operations, although they make it difficult to establish the identity of the owner without additional data, leave a trace in the form of an unchangeable sequence of transfers that allows you to identify the routes of movement of property, clusters of addresses, probable nodes for the concentration of funds and points of transition from an anonymized environment to traditional money turnover. The main task of law enforcement agencies here is to combine the technical analysis of the movement of virtual assets with the procedurally significant identification of specific persons who disposed of the relevant funds.

This requires consistent work on comparing data on the time of transfers, devices used, information from exchange sites, materials of operational-search activities, traces of business correspondence, information on the purchase of equipment, payment for communication services, rental of premises, movement of funds on bank accounts and property costs. Only in such a combination of heterogeneous sources is it possible to overcome the appearance of impersonal digital calculations. The financial footprint in the virtual asset environment does not disappear; it only changes shape and requires a higher analytical culture. Therefore, it is fundamentally important for law enforcement agencies to form specialized groups capable of understanding not only the criminal legal side of the issue, but also the economic logic of operations, the features of the multi-stage movement of digital property values, methods of disguising the origin of funds and ways to bring them into cash or property expression.

No less significant area is the identification of intermediaries, exchange points, dummy holders of means of payment and shadow settlement nodes that ensure the transformation of criminal income into a resource suitable for further use. Any organized crime lives not only at the expense of the organizers and performers of the main acts, but also at the expense of a large service layer. This layer includes those who provide details for transfers, open accounts, register wallets, withdraw cash, draw up fictitious contracts, conduct money through imaginary economic activities, create the appearance of legal grounds for moving funds and help the criminal environment come into contact with legal financial turnover. It is these figures that often become the weak link through which you can penetrate the depths of the criminal network.

In law enforcement practice, it is unacceptable to underestimate the role of dummy participants in financial schemes. The external secondary nature of their position often hides enormous significance: they provide a gap between the organizer and the final monetary result, serve as a buffer between the criminal source of income and its subsequent legalization, assume the formal appearance of ownership of funds and create a false investigation horizon for the

investigation. Meanwhile, competent financial analysis allows you to reveal their function. It reveals the lack of real economic independence of such persons, the disproportion of operations to their income and lifestyle, the regularity of the receipt and rapid disposal of funds, the synchronism of actions with other participants in the scheme, the repeatability of money routes. Therefore, finding financial intermediaries is not a peripheral task, but a path to establishing hidden centers of criminal control.

The financial profile should be used as a tool for the reconstruction of a criminal network, and this is one of the most important areas of modern law enforcement. Under the financial profile, it is advisable to understand a systematic description of income, expenses, sources of receipt of property, methods of its distribution, spending habits, characteristic counterparties, rhythm of operations, property environment, debt obligations, assets under direct and indirect control of the person, as well as those channels through which it influences economic processes within the criminal group. Such a profile allows you to restore not only the financial situation of the defendant, but also his real role in the community hierarchy.

Organizer, curator, treasurer, recruiter, technical executor, holder of funds, legalizer of income, dummy owner of property - they all leave different financial drawings of behavior. In some, the concentration and distribution of funds prevails, in others - the reception of small transfers from many sources, in the third - disguising cash flows as legal activities, in the fourth - the acquisition of property by third parties. If the investigation is limited only to the content of negotiations or data on joint participation in episodes, it can only see the outside of the organization. But when financial profiling gets involved, the structure of the criminal network begins to manifest itself in its internal logic: who gets the main benefit, who ensures the stability of the scheme, who performs the functions of a distributor, who depends on whom in monetary terms, who has reserve resources, and who is used as consumables.

It should be emphasized that parallel financial investigations should be conducted simultaneously with the main criminal case, and not after all the factual circumstances of the underlying crime have been established. Delayed financial analysis almost always means loss of time, which means loss of assets, loss of documents, concealment of beneficiaries, destruction of chains of movement of funds and the creation of new covering structures. The criminal environment adapts extremely quickly to the threat of seizure of property: funds are split, transferred to proxies, withdrawn to other jurisdictional spaces, turned into property, rewritten to relatives and affiliated structures, transformed into hard-to-track assets. Therefore, a financial investigation should unfold from the very first stages of identifying criminal activity.

The parallel nature of such an investigation is also of significant evidentiary importance. Firstly, it allows you to timely record the origin and movement of

funds while the traces are not yet blurred. Secondly, it makes it possible to identify additional episodes of criminal activity that are not covered by the original qualification. Thirdly, it contributes to the establishment of other community members who are not formally present in the direct commission of the main act, but derive systematic benefits from it. Fourth, it allows you to reveal the mechanisms of legalization of criminal proceeds, which in themselves form an independent sphere of public danger. Finally, fifth, the financial investigation serves as the basis for the adoption of interim measures, without which even a proven crime risks ending only with a symbolic punishment while preserving the material base of criminals for further activities.

That is why a more active application of the seizure of assets and confiscation mechanisms is required. The state, limited only to a conviction without a real seizure of the criminally acquired, actually leaves the criminal environment the main resource for its reproduction. Organized crime is dangerous not only by committed acts, but also by the ability to recreate itself again and again on the basis of previously accumulated capital. As long as this capital is preserved, it remains possible to pay for protection, corrupt individual officials, recruit new participants, purchase technical means, finance evasion from the investigation and trial, and support the families of detained accomplices to maintain their loyalty. Depriving the criminal environment of a property base is not an addition to criminal prosecution, but its strategic completion.

At the same time, the seizure of assets should not be understood narrowly, only as blocking bank accounts. In modern conditions, assets can be distributed between cash, real estate, transport, expensive equipment, property rights, shares in business entities, luxury goods, funds on electronic wallets, digital property values, receivables, objects formally owned by third parties, but actually under the control of the defendants. Therefore, law enforcement agencies must proceed from an expanded understanding of the property base of the criminal network. It is necessary to timely establish not only what belongs to the suspect legally, but also what he actually disposes of, what was acquired by controlled persons, what assets were paid for by criminal income and what property chains were created to conceal their true origin.

Of particular difficulty is proving the connection between the asset and criminal activity in cases where the property is registered with relatives, proxies or controlled business entities. Here, the totality of indirect, but mutually confirming circumstances acquires decisive importance: the absence of legal sources of income, the disproportion of expenses to official earnings, the participation of the same persons in the movement of funds, the coincidence of the time of acquisition of property with the receipt of suspicious sums of money, payment for the maintenance of property at the expense of the defendants, their use of the corresponding objects contrary to the formal title of ownership. Financial reconstruction of the origin of property in such cases becomes the

central evidence bridge between the main crime and the property result, subject to arrest and subsequent withdrawal to the state.

It should be noted that the active use of financial intelligence is not only repressive, but also preventive. When the criminal environment is faced with a steady practice of quickly identifying cash flows, blocking accounts, opening cashing schemes, seizing property, turning into state revenue assets hidden behind nominal owners, and the inevitable destruction of the system of financial services for crimes, it loses its most important advantage - confidence in the safety of criminal income. Namely, the expectation of an unpunished material result is for many participants the main motive for inclusion in criminal activity. Therefore, financial pressure weakens not only the existing criminal communities, but also their ability to attract new participants, expand spheres of influence and penetrate the legal economic turnover.

Consequently, for law enforcement agencies, financial intelligence should not become a highly specialized function of individual units, but an end-to-end principle of all work to counter organized crime in the digital environment. It requires training in financial analysis techniques; establishment of interdepartmental exchange of information; timely access to data on the movement of funds; developing common methods for assessing suspicious transactions; combination of operational-search, investigative and analytical capabilities; constant interaction with financial and control structures; technological equipment for the study of complex chains of calculations; and also a clear understanding that money in a criminal environment is not just the result of a crime, but its blood, nerve and will.

Ultimately, the most effective way to weaken organized crime is to destroy not only its connection, not only its organizational mechanisms, but above all its monetary infrastructure. You can replace an individual performer, you can create a new closed communication channel, you can transfer activities to another site. But if the flow of funds is blocked, if the income distribution chain is broken, if the schemes of concealment of property are destroyed, if the accumulated resources are seized, if it becomes clear to each participant that the criminal income will neither be preserved, nor legalized, nor transferred to heirs and accomplices, then the criminal organization loses the main thing - its material basis, and with it the ability to survive. This is precisely the true power of financial intelligence: it does not hit the external manifestations of crime, but at its core.

4. RECOMMENDATIONS FOR STATE SECURITY AUTHORITIES

4.1. Consider platform criminalization as a factor of national security

In modern conditions, crime operating in the digital environment can no longer be considered as a set of scattered episodes of illegal trafficking, fraud, extortion,

illegal access to information or organization of shadow settlements. Platform criminalization is a qualitatively different level of threat, in which the digital environment turns not only into a crime scene, but into a full-fledged infrastructure for managing, coordinating, disguising, financing and expanding criminal activity. It is in this regard that it is fundamentally important for the bodies responsible for state security to recognize that the state is not facing a private criminal law problem, but a phenomenon that can affect the foundations of public stability, manageability, sovereignty and security of the most important state and public systems.

The traditional perception of criminal activity as a sphere limited by the tasks of criminal prosecution is rapidly losing explanatory power today. Digital criminal networks act not as rigidly formed associations, but as flexible, rapidly rebuilding structures capable of uniting participants from different regions and states, distributing functions between anonymized performers, hiding decision-making centers and transferring activity to new technical sites as soon as possible. This means that the criminal network operating through digital platforms is increasingly acquiring properties characteristic not only of organized crime, but also of subjects of covert subversive influence. It can provide sustainable logistics of prohibited goods and services, manage cash flows, influence mass behavior, create hotbeds of social destabilization, form channels of illegal cross-border interaction and be used as a cover for much more dangerous forms of activity.

Of particular importance is the fact that platform criminalization undermines social stability not always through direct violence. In many cases, its action is dispersed, accumulative and outwardly inconspicuous. The massive involvement of citizens in shadow settlement schemes, the spread of drug markets through digital channels, the coordination of illegal migration assistance, the involvement of minors in criminal missions, the systematic information impact on alarming social groups, the stimulation of distrust of state institutions - all this separately may seem to be the task of law enforcement response. However, taken together, such processes create a long-term erosion effect that erodes the rule of law, the rule of law and the very ability of the state to ensure the predictability of public life. When significant groups of the population begin to perceive the digital criminal environment as a familiar, accessible and vulnerable order of meeting demand, not just a criminological, but a political and security problem arises.

The aspect of illegal cross-border influence is no less significant. A digital platform is inherently capable of crossing state borders with such ease that traditional criminal structures have never been able to move people, resources, or organizational signals. The cross-border nature of platform criminalization means the loss of the previous locality of the threat. Coordination channels, data storages, settlement participants, organizers of information impact, suppliers of malicious means and executors of specific orders can be located in different

jurisdictions, use legal gaps between states and consciously rely on the difference in national legal regimes. As a result, criminal activity ceases to be an internal matter of one territory: it becomes part of external pressure, in which the criminal interest is intertwined with geopolitical, intelligence or ideological calculation. For state security agencies, this means the need to consider each stable digital criminal network not only from the point of view of corpus delicti, but also through the issue of external relations, management routes, foreign centers of technological support and the potential interest of foreign structures in maintaining and using such a network.

Hidden financing of destructive activities deserves special attention. One of the most dangerous features of digital criminal platforms is their ability to mask the origin, purpose and movement of funds, split transactions, distribute them over many links, use dummy participants, and create the illusion of unrelated transactions. Under these conditions, a criminal platform can act not only as a source of profit for illegal enrichment, but also as a mechanism for financial support of subversive activity, including extremist, sabotage, recruitment, corruption and other activities directed against the interests of the state. The danger here lies not only in the money itself, but also in the opaque architecture of their movement. The more anonymized, dispersed and technologically mediated financial channels, the easier it is to hide the connection between the organizers of the criminal platform and the ultimate beneficiaries, including those outside the state. Consequently, the task of state security agencies is not to formally record the fact of illegal circulation of funds, but to identify the entire chain of their functional purpose: who accumulates resources, who redistributes them, what actions they are directed to, what political, extremist or intelligence interests may be behind the seeming "ordinary" criminal activity.

The issue becomes even more acute where platform-based criminalization intersects with **critical infrastructure**. This should be understood as encompassing not only **energy, transport, financial, telecommunications, and governance systems**, but also the entire complex of facilities and processes whose disruption may cause **large-scale public harm, disorganization of everyday life, economic shock, or a crisis of confidence in the state**. The penetration of criminal digital networks into such spheres cannot be treated as an ordinary offense against information or property. In conditions of high systemic interdependence, even a limited breach of their integrity, availability, or controllability may have **cascading consequences**. A criminal platform may be used to identify insiders, acquire official information, organize unlawful access, procure technical means for bypassing security, coordinate attacks on vulnerable nodes, conceal traces of interference, and subsequently monetize the damage inflicted. Even more dangerous, however, is the fact that such activity may serve not as an end in itself, but as a **preparatory phase for more serious operations**. In this context, the criminal environment is transformed into a zone of preliminary penetration,

resilience testing, and the establishment of covert human or technical support structures.

It is precisely for this reason that the proposition that criminal networks may be used as a **proxy instrument of foreign actors** should be regarded not as a theoretical hypothesis, but as a **working analytical model**. In contemporary practice, sharply demarcated forms of hostile activity are extremely rare. On the contrary, what is observed is their deliberate entanglement, whereby **state-hostile influence seeks to operate through third parties, by proxy, with the direct connection between initiator and executor blurred as much as possible**. Under such conditions, a criminal digital network becomes a convenient **layer of concealment**, enabling several objectives to be achieved simultaneously: preserving plausible deniability, exploiting already existing channels of illegal logistics, relying on established schemes of shadow financing, recruiting operatives without fully informing them of the ultimate purpose, and shifting activity into a domain outwardly resembling "ordinary" crime. This substitution is especially dangerous because delayed recognition of it leads to the **misclassification of the threat**. In situations where counterintelligence analysis and interagency response mechanisms should be activated, the state risks limiting itself to procedural measures addressing isolated episodes, without affecting the organizing center or neutralizing the strategic design.

It follows that it is fundamentally important to proceed from the premise that the **hybrid combination of criminal, extremist, intelligence, and information-destructive activity** is becoming not an exception, but one of the likely forms of development of platform-based criminalization. Today it is no longer sufficient merely to identify the fact of a crime; it is necessary to determine whether the relevant digital network performs broader functions-**mobilizational, propagandistic, intelligence-gathering, recruitment-related, or destabilizing**. The principal danger of hybridization lies in the fact that different forms of threat **mutually reinforce one another**. Criminal profit sustains extremist structures; an extremist agenda facilitates recruitment into the criminal environment; information influence creates an atmosphere of distrust and confusion in which illegal operations are easier to conceal; and intelligence interests use criminal channels as a ready-made illicit infrastructure for penetration. When all these elements converge, the state is no longer confronted with an isolated criminal scheme, but with a **multilayered system of concealed influence on national security**.

From this follows a key practical conclusion: if a digital criminal network begins to perform functions of **logistics, influence, financing, and covert coordination**, it must become an object not only of police attention, but also of **counterintelligence concern**. This proposition is not merely declaratory; it has **methodological significance**. It requires a reassessment of the criteria of dangerousness. It is insufficient to analyze only the object of the crime, the

amount of illicit income, or the number of episodes. What must be identified is the **functional role of the network within a broader threat environment**. In other words, the state must ask not only what exactly has been violated, but also what **infrastructural, financial, communicative, or subversive role** the detected digital platform plays within the system of other covert processes. If a network provides stable anonymous communications, conducts covert distribution of resources, links participants from different countries, and displays signs of discipline, secrecy, technical adaptability, and a stable management core, then what stands before us is no longer merely a criminally punishable group, but an **object of heightened attention for the national security system**.

Accordingly, the bodies responsible for state security must institutionally establish an approach under which **platform-based criminalization is regarded as an independent factor of national security threat**. This implies, first and foremost, the development of a common conceptual framework that eliminates departmental fragmentation and conflicting interpretations. So long as some agencies see in a digital network exclusively a market for prohibited services, others a scheme for the illegal circulation of funds, and still others a channel of informational influence, the state will continue to respond in a fragmented manner. Yet the very nature of the threat requires a **holistic, synthetic perspective**, in which the digital platform is assessed simultaneously as an environment of crime, a system of control, a financial mechanism, a channel of influence, and a potential instrument of external interference. Only in this way is **early diagnosis of the transition from criminal danger to a national security threat** possible.

Moreover, there is a need to shift from predominantly event-driven reaction to the **proactive identification of infrastructural indicators of threat**. Too often, state attention is concentrated on acts that have already been committed, whereas digital criminal networks reveal their true danger long before their most destructive manifestations. Heightened concern should be triggered by signs of **stable anonymous coordination**, the existence of distributed financial channels, the use of technical means to conceal communication routes, active reliance on intermediaries, attempts to recruit persons with access to officially significant information or facilities, as well as the combination of criminal activity with directed informational influence. The early detection of such indicators can prevent the transformation of a criminal network into an instrument of **systemic destabilization**. Here it is especially important to overcome the inertia of departmental thinking, in which each identified function of the network is considered separately and never assembled into a unified picture.

No less important is the strengthening of the **analytical component** of the activity of state security bodies. The issue of platform-based criminalization cannot be exhausted by operational support and procedural documentation alone. What is needed is a **deep strategic analysis** capable of discerning the evolution of

networks, the patterns of their growth, the ways in which they adapt to state pressure, and their interconnection with social crises, cross-border conflicts, and changes in the international environment. Without a developed analytical capacity, the state will inevitably fight consequences rather than the mechanism of the threat itself. Analysis must encompass not only technical and legal aspects, but also **social, economic, ideological, psychological, and geopolitical dimensions**. A criminal digital platform does not exist in a vacuum: it feeds on social fractures, institutional weaknesses, deficits of trust, technological vulnerabilities, and gaps in coordination among agencies. That is why countering it requires not a mechanical tightening of control, but an **intellectually rich, multilayered strategy of state protection**.

Finally, it must be emphasized that recognizing **platform-based criminalization as a factor of national security** does not mean replacing the criminal-law approach with emergency or arbitrary intervention. On the contrary, it is a matter of increasing the precision of the state's perception of the threat and aligning legal and organizational mechanisms with the real nature of the phenomenon. The state is obliged to perceive the threat as it actually is, rather than as it is more convenient to describe it within outdated classifications. When a criminal network assumes functions of **covert logistics, financial intermediation, coordination, informational influence, and cross-border alignment of interests**, it ceases to be exclusively an object of criminal prosecution. It becomes an element of the environment within which a **complex, composite, and deeply clandestine threat to state security** may take shape.

That is precisely why, for bodies responsible for state security, the issue of **platform-based criminalization** must be framed with the utmost clarity and principle. This is not a matter of fashionable terminology or of expanding familiar forms of reporting. It is a matter of the state's capacity to recognize in a digital criminal network the embryonic form of the infrastructure through which **covert influence, the undermining of resilience, the financing of destructive forces, and penetration into the country's internal processes** may be carried out. Delay in such recognition comes at a high cost to the state: it is paid for through the growth of shadow governance, the penetration of criminality into the fabric of society, and the expansion of the space in which external and internal opponents of legal order find common ground. Therefore, the recognition of **platform-based criminalization as a factor of national security** should be regarded not as a narrow recommendation, but as one of the **basic conditions of modern state self-preservation**.

4.2. Establishment of a national early warning system

In contemporary conditions, the issue of creating a national early warning system for the criminalization of the digital environment has ceased to be a matter of narrow professional discussion and has become one of the central tasks of state self-preservation. This is not merely about improving departmental

surveillance, nor about technically expanding the capabilities of individual units. It is about forming an integrated state mechanism for the anticipatory detection of threats, capable of recognizing emerging criminal processes before they acquire stability, institutional completeness, and a destructive social scale. It is precisely here that the fundamental boundary lies between a state that manages a threat and a state that merely belatedly records its consequences.

The digital environment has long ceased to be merely a space for communication, information exchange, and economic activity. It has become a complex, multilayered, highly dynamic environment in which unlawful structures are able to form rapidly, camouflage themselves, disperse, and then regroup in new configurations. Their strength is determined not only by the number of participants, but also by their ability to use anonymization, dispersion, the interchangeability of communication channels, coded vocabulary, closed and semi-closed communities, systems of intermediaries, false pretexts for presence, as well as financial and organizational mechanisms hidden from superficial observation. Under these conditions, the traditional reactive model, based on detecting acts that have already been committed, is manifestly insufficient. State security requires a transition from delayed recording to anticipatory recognition.

A national early warning system should be created as a permanent, interagency, scientifically grounded, and legally regulated system for identifying signs of the criminalization of the digital environment. Its principal purpose is not simply to collect fragmented information, but to detect the dynamics of dangerous processes, uncover hidden links between individual manifestations, recognize the early signs of the formation of criminal infrastructure, and ensure the development of timely managerial decisions. In other words, such a system should be oriented not toward registering an already-formed body of crime, but toward recognizing pre-criminal and early-criminal states of the digital environment.

The first crucial element of this system is the identification of indicators of the growth of dangerous networks. Such indicators cannot be reduced to formal metrics such as the number of messages, the number of subscribers in a given community, or a sharp increase in traffic on certain digital platforms. Quantitative growth in itself does not yet mean criminalization. Therefore, the indicative model must be constructed as a multifactor system of features that takes into account the speed at which new connections are formed, the nature of their density, the emergence of intermediary nodes, the recurrence of information transmission routes, the distribution of roles among participants, the appearance of stable chains of subordination, as well as the synchronicity of behavioral actions across different segments of the digital environment. Of particular importance is the recognition of cases in which previously disconnected bodies of users begin to display signs of hidden organizational unity: reproducing common verbal formulas, using a unified set of coded

designations, redirecting audiences along similar trajectories, and forming a stable system of internal specialization. The growth of a dangerous network is not a mechanical expansion of presence, but a complication of structure, the strengthening of internal ties, and an increased capacity for self-reproduction. It is precisely such processes that an early warning system must detect.

No less significant is the monitoring of new channel migration schemes. The criminal environment in digital space is distinguished by exceptional adaptability. When state attention intensifies, unlawful structures rarely disappear; much more often, they shift their platforms of presence, fragment their channels of communication, move into closed modes of interaction, create chains of intermediate nodes, and use camouflage communities and temporary gathering points. Consequently, the task lies not only in observing specific digital resources, but above all in understanding the patterns of their movement, fragmentation, and renewed concentration. A national early warning system must record typical scenarios of transition from the open dissemination of information to semi-concealed forms of interaction, from mass agitation to targeted recruitment, and from a single notification channel to a distributed network of small groups linked by internal intermediaries. It is especially important to identify migration not in its technical but in its organizational sense: who initiates the transition, how roles are redistributed, how manageability is preserved during a change of environment, which categories of participants remain in the open field, and which are transferred into the closed circuit. Anyone who does not track the routes by which criminal communication moves inevitably loses sight of the very logic of the threat's development.

One of the most alarming early signs of the criminalization of the digital environment is a surge in recruitment activity. In today's digital space, recruitment is rarely carried out in a direct and open form. More often, it is concealed under the guise of ideological engagement, pseudo-solidarity, promises of material support, rhetoric of belonging to an "elite" community, the romanticization of violence, the display of false social protection, or the exploitation of personal vulnerability. For this reason, an early warning system must be able to distinguish between ordinary informational activity and directed involvement in unlawful practices. This requires taking into account a combination of signs: a sharp increase in appeals to certain age, social, or professional groups; the systematic use of psychologically vulnerable themes; the emergence of successive stages of rapprochement with the audience; the transfer of communication from the public sphere into an individualized mode; the formation of circles of trust; promises of reward, status, protection, or revenge; and the appearance of verbal constructs that blur moral and legal prohibitions. It must be understood that recruitment is not a one-time act, but a process of gradually breaking down an individual's inner resistance. Consequently, early warning must be able to detect not only the final stage of inducement, but also

the preceding phase shifts in rhetoric, targeting, and the emotional intensity of interaction.

An exceptionally important task is the analysis of abrupt changes in vocabulary and semantic codes. Criminal structures operating in the digital environment constantly transform the language of their communication. They replace direct designations with veiled expressions, use slang euphemisms, deliberately distort words, introduce ambiguous formulas, combine every day and specialized vocabulary, create symbolic markers of belonging, and employ verbal signals for identifying "their own." Moreover, a change in language often precedes a change in the organizational model. When a community begins to develop new designations, this often indicates either a transition to a more concealed mode of activity, or an expansion of membership, or preparation for the commission of new kinds of acts. Accordingly, the state early warning system must include a deep semantic analysis of linguistic changes, capable of identifying not only the frequency of individual words, but also transformations of semantic fields, shifts in emphasis, the emergence of new contexts of use, and the intensification of aggressive, conspiratorial, mobilizational, or dehumanizing rhetoric. Particularly dangerous are those cases in which the previous language of discussing every day, cultural, or quasi-political topics begins to fill with references to violence, shadow financial operations, illicit movement, concealment of identity, coded arrangements, and rituals of internal loyalty. It is precisely in such transitional zones that the future criminal contour is often formed.

A special place in the architecture of early warning belongs to the assessment of the concentration of suspicious ties between digital nodes. Under conditions of complex network organization, crime is less and less likely to manifest itself through linear hierarchies and increasingly acts through distributed, polycentric, multi-level structures. This means that the threat may emanate not from a single visible center, but from a set of seemingly insignificant nodes that, when connected, form a stable infrastructure. Therefore, it is fundamentally important to measure not only the existence of ties, but also their density, recurrence, stability, role in the transmission of information, degree of intermediation, and function in the redistribution of flows. A high concentration of suspicious ties may be expressed in a sharp intensification of interactions between previously weakly connected communities, in the emergence of intermediary nodes through which a disproportionately large volume of coordinating signals passes, and in the formation of closed circuits where information spreads at high speed with a low level of leakage to the outside. It is critically important for the state to learn to see precisely these structural condensations, because it is often within them that the core of a future unlawful network crystallizes. Danger arises not only from the content of messages, but also from the architecture of their dissemination.

Directly related to this is the automatic detection of signs of coordination between outwardly unrelated communities. This point is of particular importance because the contemporary criminal environment seeks to avoid obvious organizational unity. Different communities may declare different goals, use different symbols, appeal to dissimilar audiences, and even appear to be in conflict with one another, while in fact remaining elements of a single hidden system. Their unity may be manifested in the synchronicity of actions, the identity of semantic turns, repetition of route patterns in participant movement, coordinated dissemination of certain directives, the use of common intermediaries, a shared temporal discipline of publication, parallel changes in speech codes, or the concentration of the same financial and organizational ties. Therefore, the early warning system must be aimed specifically at recognizing latent coordination-that hidden organizational unity which does not lie on the surface and is therefore especially dangerous. Otherwise, the state will see fragmented pieces where in reality an entire system is already operating.

However, even the most advanced surveillance system will not be able to fulfill its purpose if it is not integrated with law-enforcement databases, customs information, border analytics, financial monitoring, cyberincident data, and analytical materials on organized risk groups. It is necessary here to emphasize a fundamental point: the criminalization of the digital environment is never confined solely to the digital environment. It almost always extends into physical space, logistics, the movement of persons and goods, illicit financial flows, the use of front structures, corrupt contacts, the organization of cross-border links, and the technical support of unlawful activity. Consequently, a digital signal acquires genuine operational and analytical value only when it is correlated with other state-held information and incorporated into a unified threat picture.

Integration with law-enforcement records is necessary to establish links between new digital manifestations and already known persons, methods, routes, objects of criminal encroachment, as well as previously identified episodes. Not infrequently, one and the same subject, while formally changing means of communication, linguistic masks, and circles of contact, retains a stable behavioral signature that becomes discernible only through comparison with accumulated bodies of information. Customs information makes it possible to identify correlations between surges of activity in the digital environment and the movement of certain categories of goods, equipment, components, monetary surrogates, data carriers, or dual-use items. Border analytics makes it possible to detect the spatial dimension of the threat: overlapping entry and exit routes, short-term visits to sensitive zones, repeated travel patterns, atypical mobility of certain groups, as well as signs of coordinated movement by persons linked through informal digital contacts. Financial monitoring makes it possible to uncover the material basis of hidden networks, identify atypical transactional chains, the splitting of payments, the use of intermediaries, the concentration of funds at nodal points, and the connection between recruitment activity and the

financial incentivization of operatives. Cyberincident information is necessary to understand the technical dimension of the threat: which resources are being attacked, which tools are being used to conceal traces, how malicious effects are being propagated, and how infrastructure reconnaissance and penetration into significant systems are being prepared. Finally, analytics on organized risk groups provides strategic depth of assessment, making it possible to connect current digital signals with criminal formations that have been developing over time, their specialization, economic base, personnel reserve, territorial influence, and cross-border contacts.

At the same time, integration must not be understood as the mechanical merger of all data into a single repository without legal differentiation, scientific methodology, or organizational discipline. On the contrary, the effectiveness of a national early warning system depends on a clear legal regime of access, a strict distribution of powers, source verification, differentiation of degrees of reliability, preservation of the procedural usability of information, and the development of uniform rules for interagency exchange. A strong state is not a state of disorderly accumulation of information, but a state of intelligent, lawful, and purposeful handling of it. Otherwise, there arises a risk either of paralysis due to information overload or of abuses that discredit the very idea of threat prevention.

A necessary condition for the effectiveness of such a system is also the creation of a unified methodological framework for assessing danger. If different agencies proceed from inconsistent criteria, use different risk scales, define suspicious ties differently, and interpret signs of coordination inconsistently, the system will lose coherence and turn into a set of incompatible fragments. Consequently, there is a need to develop a nationwide conceptual apparatus, standardized indicator models, a typology of threat levels, procedures for interagency confirmation of signals, and uniform regulations for transferring materials for further response. The problem of false positives and false negatives deserves particular attention. The former generate unjustified burdens on state bodies and may affect law-abiding persons; the latter, on the contrary, create an illusion of well-being where a dangerous network is already taking shape. Therefore, the national early warning system must be built on the principles of continuous scientific validation, retrospective assessment of the accuracy of conclusions, adaptation of indicators to changing forms of crime, and constant comparison of predictive conclusions with actual outcomes.

It should be emphasized separately that the creation of such a system is impossible without a serious scientific and personnel foundation. Its full functioning requires specialists capable of combining legal reasoning, criminological analysis, linguistic sensitivity, an understanding of network structures, skills in handling large bodies of information, knowledge of cross-border crime, financial schemes, migration processes, and the psychological

mechanisms of involvement. In other words, this is not simply about the technical support of a state function, but about the formation of a new security culture in which prevention is built at the intersection of law, science, strategy, and administrative will. Without such a personnel foundation, even the most advanced computational means will remain mute: they will be able to register noise, but they will not be able to recognize the meaning of the threat.

Another essential requirement is the phased organization of response to early warning signals. It is inadmissible for every recorded indicator automatically to generate a reaction of the same intensity. The system must distinguish levels of danger: from weak harbingers of disorder to signs of a formed coordination network. Each level must correspond to its own measures-from deeper observation and additional verification to interagency notification, preventive intervention, operational support, and the initiation of procedural mechanisms. This is especially important in conditions where the criminalization of the digital environment develops unevenly: in some cases it is expressed in the initial accumulation of hostile rhetoric, while in others it is already manifested in the distribution of roles, logistics, financing, and the preparation of specific unlawful acts. The state must be able to calibrate the force of intervention to the degree of maturity of the threat, while retaining the capacity to escalate its response rapidly when dangerous tendencies are confirmed.

Finally, it is fundamentally important to understand the strategic meaning of early warning. Its purpose is not exhausted by the technical detection of suspicious digital processes. It consists in preventing disparate signs of disorder from turning into a full-fledged criminal infrastructure-stable, self-renewing, economically sustained, socially rooted, and protected by internal mechanisms of conspiracy. When the state does not possess an early warning system, it inevitably acts only after the threat has already strengthened, acquired a personnel reserve, backup channels, financial supports, and legal cover. In such a situation, the cost of response increases many times over: greater forces are required, harsher measures become necessary, the restoration of compromised security becomes prolonged, and the level of social costs rises. By contrast, anticipatory detection makes it possible to suppress a dangerous process at the phase of its least stability-when the network has not yet acquired internal discipline, has not formed durable sources of financing, and has not yet taken root in the social fabric.

Thus, the creation of a national early warning system for the criminalization of the digital environment should be regarded as one of the key pillars of modern state security. Such a system must identify indicators of the growth of dangerous networks, track channel migration schemes, record surges in recruitment activity, analyze abrupt changes in vocabulary and semantic codes, assess the concentration of suspicious ties between digital nodes, and automatically recognize signs of coordination between outwardly unrelated communities. At

the same time, its effectiveness is possible only with deep integration with law-enforcement records, customs information, border analytics, financial monitoring, cyberincident data, and analytical materials on organized risk groups. Without early warning, the state is doomed to lag behind. With early warning, it gains a chance not to chase the threat, but to outpace it. It is precisely in this that the true meaning of responsible state policy in the digital age resides.

4.3. Regulatory Update

In the context of the rapid technologization of criminal activity and the growing interconnectedness of the digital environment with economic, political, and social processes, the issue of updating the regulatory framework ceases to be a purely sector-specific task of lawmaking. It becomes a matter of preserving the effectiveness of the state, its ability to protect society, suppress the activities of organized criminal structures, and at the same time maintain the legal order within the bounds of constitutional legality. Where the law lags behind, crime gains not merely a temporary advantage-it acquires space for entrenchment, institutionalization, and subsequent pressure on state mechanisms. For this reason, modern regulatory policy in the sphere of state security must be not fragmented, but systemic, anticipatory, and internally coherent.

A particularly dangerous situation arises when the digital environment develops faster than the legal instruments designed to regulate it. In such cases, a gap emerges between the actual capabilities of criminal actors and the legal capabilities of the state. This gap is especially visible in the investigation of serious transnational offenses committed through the use of distributed network infrastructures, anonymized accounts, remote data storage tools, and sophisticated methods of concealing digital activity. Criminal communities deliberately exploit inconsistencies among national legal regimes, differences in evidentiary admissibility standards, the lack of regulation concerning the preservation of electronic traces, and the slowness of intergovernmental procedures. Accordingly, updating the regulatory framework should not be aimed at a merely symbolic “modernization” of legislation, but at genuinely closing those legal voids that have already become an operational resource for the criminal world.

First and foremost, the legal status of digital traces and the procedures for their preservation must be clarified. To this day, in a number of law enforcement contexts, electronic information continues to be viewed through the prism of outdated categories of physical media, even though its nature, mechanisms of creation, methods of alteration, and conditions of loss differ fundamentally from those of traditional material objects. A digital trace does not exist in the simplified form of a “file” or a “message”: it constitutes a complex aggregate of metadata, event logs, network identifiers, timestamps, information on the sequence of actions, indicators of user interaction with a system, routing parameters, and other technically significant elements. For this reason, the legal definition of a

digital trace must be broad, technologically neutral, and at the same time procedurally specific.

It is necessary to establish by law that digital traces constitute an independent category of evidentially significant information requiring a special procedure for detection, recording, seizure, copying, authentication, transfer, examination, and storage. At the same time, the law must account for their high mutability, their dependence on the settings of the information environment, and the possibility of their automatic deletion, overwriting, or distortion as a result of the ordinary functioning of technical systems. The preservation of a digital trace is not a technical formality, but a legal guarantee of truth. If information is not recorded in a timely and proper manner, the state risks losing the ability either to prove the very fact of the criminal act or to identify the persons involved.

In this connection, detailed regulation is needed for procedures aimed at the urgent preservation of digital information prior to the final procedural decision on its seizure or examination. The law should clearly define the grounds, limits, time frames, and procedure for issuing binding orders on the temporary preservation of data by telecommunications operators, owners of information resources, information transmission intermediaries, and other entities possessing the technical capacity to prevent the destruction of information. Of particular importance is the establishment of requirements for the continuity of the chain of custody, for certifying the integrity of information, for documenting every action involving digital objects, and for differentiating access by officials to the relevant materials. Without such norms, any significant electronic evidence may be called into question, and the very criminal-procedural prospects of the case may be undermined.

No less urgent is the task of improving the regimes governing international exchange of electronic evidence. Modern crime recognizes no state borders, yet borders often become its most reliable shield. Information concerning correspondence, posted materials, financial transactions, connection data, accounts, and digital routes may be located simultaneously in several jurisdictions, subject to different standards of information protection, and disclosed only in compliance with multilevel procedures. As a result, investigators face a paradox: the necessary information technically exists, but legally remains inaccessible, or arrives only when its evidentiary value has already been lost.

Resolving this situation requires not only bilateral and multilateral agreements, but also a reconsideration of the very logic of international legal cooperation. It is necessary to develop mechanisms that make it possible to expedite the transmission of requests, unify minimum standards for the content of applications, establish maximum response times in cases involving serious crimes, recognize the legal significance of duly certified electronic data packages, and agree in advance on categories of data subject to priority preservation. Today,

delay in the international exchange of evidence is tantamount to the loss of evidence. While states are agreeing on the form of a request, criminal actors change devices, delete accounts, transfer assets, and sever the digital links leading to the organizers of criminal acts.

A special place should be given to the regulatory framework for direct, yet strictly controlled, interaction between competent authorities and foreign holders of technically significant information in cases where delay objectively creates a threat to life, public safety, the stability of critical systems, or the investigation of particularly serious transnational crimes. At the same time, such interaction must not turn into legal improvisation. It is possible only where there is a clear definition of competence, grounds for urgency, the procedural form for confirming the request, the procedure for subsequent judicial or prosecutorial review, and the rules governing the use of the information obtained. The strength of the state lies not in arbitrary intrusion into the information sphere, but in its ability to act swiftly, lawfully, and in a provable manner.

The next fundamental direction is the establishment of platforms' obligations to cooperate within lawful procedures. In today's digital space, major online platforms, messaging services, data storage services, information dissemination intermediaries, and other owners of information infrastructures effectively function as nodal points through which flows vast amounts of information of interest for suppressing criminal activity. However, in the absence of clearly formulated obligations, this role becomes a source of legal uncertainty. Some entities invoke internal rules, others refer to foreign jurisdiction, still others cite the lack of technical capability, and yet others point to the unclear status of the requested information. The result is always the same: law enforcement encounters procedural delays, fragmented responses, and the loss of investigative prospects.

Therefore, it is necessary at the legislative level to establish an exhaustive list of obligations for such entities upon receipt of a lawful and properly formalized request from competent authorities. Such obligations should include the timely preservation of specified categories of information, the provision of identifying and technical information within the limits established by law, the maintenance of continuous communication with authorized units, the existence of an official representation or an appointed responsible person for interaction with state authorities, and compliance with requirements to restrict access to materials directly connected with serious crimes where such requirements are based on a judicial or other legally prescribed decision. A platform that derives profit from organizing the informational communication of millions of persons has no right to evade lawful participation in the protection of public security.

At the same time, the duty to cooperate must not be understood as permission for the arbitrary seizure of any and all information. On the contrary, the broader the technical capabilities of private data holders, the more precisely the limits of state

interference must be defined. The legislature must establish lists of the categories of information that may be requested, grounds for differentiating access to them, requirements for judicial authorization in the most sensitive cases, notification rules where permissible, and the procedure for subsequent appeal. Only such a combination of imperative force and legal certainty can prevent two extremes at once: the helplessness of the state in the face of criminal networks and the erosion of guarantees of private life.

The development of criteria for expedited response procedures in relation to serious transnational crimes is acquiring particular relevance. Here, legislation must proceed from the understanding that not all crimes require the same procedural speed or the same scope of urgent measures. Where the acts in question are associated with terrorist activity, illicit arms trafficking, the exploitation of minors, human trafficking, the coordination of mass unrest, interference with critical facilities, the creation of networks for the dissemination of especially dangerous materials, large-scale theft of financial assets, or the activities of stable transnational criminal associations, delay measured in hours or even minutes may have irreversible consequences. Precisely for this reason, special legal regimes of accelerated response are required.

Such regimes must be based on clearly established criteria. First, it is necessary to define the nature of the public danger of the act, including the scale of potential harm, the number of potential victims, the threat to life and health, and the capacity of the criminal activity for rapid expansion. Second, the transboundary character of the criminal infrastructure, the multiplicity of network nodes used, the distributed nature of data storage, and the risk of the immediate transfer of traces to other jurisdictions should be taken into account. Third, an important criterion should be the high probability of irreversible loss of evidence if the ordinary, longer procedure is applied. Fourth, the stability of the criminal structure, its organization, the presence of role distribution, a financial base, and a mechanism for concealing traces must be assessed. An expedited procedure should be an exception, justified only where the ordinary procedure no longer protects the law but in fact serves the offender through its delay.

At the same time, expedited procedures must be accompanied by special procedural safeguards. Mandatory written reasoning, the shortest possible time limits for subsequent judicial review, heightened requirements for documenting every action, a special procedure for storing the information obtained, the possibility of reviewing the proportionality of the measure applied, and-where permissible without prejudice to the investigation-subsequent notification of the persons concerned are all needed. Such an approach makes it possible to ensure not only operational efficiency, but also legitimacy. For state decisiveness that is not grounded in law sooner or later turns into a crisis of trust; yet law that is incapable of acting in a timely manner becomes a ritual of impotence.

An independent direction consists in the regulatory definition of highly dangerous digital criminal ecosystems. Law cannot effectively counter what it is unable to describe precisely. In practice, digital formations are becoming increasingly visible that cannot be reduced to a single crime, a separate participant, or a specific technical resource. What is at issue are complex, self-reproducing systems that combine anonymization tools, infrastructures for the dissemination of prohibited materials, illegal payment mechanisms, recruitment channels, means of teaching criminal skills, databases of stolen information, tools for coordinating attacks, intermediaries for concealing the origin of digital assets, and mechanisms for circumventing state control. Such formations function as a full-cycle criminal environment: they recruit, train, equip, finance, protect, and reproduce unlawful activity.

A normative definition of such ecosystems is necessary so that law enforcement can respond not only to isolated manifestations, but also to the infrastructural basis of criminality. The law should identify the characteristics by which such an environment is recognized as highly dangerous: the systematic facilitation of serious crimes; the unification of multiple participants into a stable structure; the use of special means of concealing identity and information transmission routes; the existence of services supporting unlawful operations; the involvement of an indefinite circle of persons in criminal activity; transnational reach; and a high rate of recovery after the blocking of individual elements. Crime prevails where the state sees only episodes and fails to notice the system. Consequently, the legal norm must make it possible to classify, restrict, block, and examine precisely the system itself as a source of ongoing threat.

However, it is especially important here to ensure precision in legislative wording. It is unacceptable for broad definitions to encompass neutral technical tools, lawful research communities, professional associations of information security specialists, or other entities whose activities are not directed toward the commission of crimes. The definition of a highly dangerous digital criminal ecosystem must be based not on outward signs of complexity or technological sophistication, but on a provable set of functional characteristics demonstrating its instrumental orientation toward supporting serious unlawful activity. Here the legislature must exercise the highest degree of precision, since any ambiguity will equally benefit both criminals hiding behind legal vagueness and unscrupulous law enforcement officials inclined toward excessive expansion of interference.

Finally, exceptional importance attaches to the regulation of interagency access to data within the framework of procedural guarantees. The modern system for ensuring state security includes numerous bodies and units possessing information of various kinds: operational-search, investigative, border-control, customs, financial, migration, tax, registration, judicial, and other data. The fragmentation of these data sets, departmental insularity, and the absence of

uniform access procedures create not merely inconvenience, but a direct threat to the effectiveness of the state. Criminal groups have long learned to exploit institutional gaps: while one agency verifies information, another lacks grounds to request it, a third lacks technical compatibility, and a fourth is constrained by restrictions unsupported by a clear mechanism for lawful override. As a result, fragments of information do not coalesce into an evidentiary picture, and time works against the law.

The legislature must create a regime of interagency access under which information may be transferred quickly, specifically, and only where proper legal grounds exist. This requires clear categories of data, differentiation of access levels, legislative consolidation of the purposes for which information may be used, mandatory logs of access to information, the establishment of personal responsibility of officials for the unlawful obtaining, dissemination, or use of data, and procedures for independent review of the lawfulness of access. Interagency exchange must be neither chaotic nor paralyzed. It should be built as a strictly organized system in which each operation is justified, traceable, and subject to subsequent oversight.

It is especially important to determine the rules for the interaction of different legal regimes governing information. Some data fall under the secrecy of communications, others under personal data protection, still others under banking secrecy, others under tax secrecy, a fifth category consists of operational accounting information, and a sixth comprises materials of the preliminary investigation. Until the legislature develops a clear mechanism for correlating these regimes, officials will either act with excessive caution for fear of exceeding their powers or, conversely, will be inclined toward an expansive interpretation of their competence. In both cases, the rule of law suffers. Therefore, the law must not merely declare the possibility of interagency cooperation, but must describe in detail the legal grounds, conditions, limits, time frames, methods of request authentication, and procedures for subsequent review. Only in this way is it possible to combine investigative effectiveness with the inviolability of procedural guarantees.

The full set of the above measures requires a unified methodological approach. Updating the regulatory framework in the sphere of state security cannot be limited to the introduction of scattered amendments into separate legislative acts. What is needed is an integral concept of a legal response to the digitalization of crime, based on several fundamental principles. First, technological neutrality: the law must be applicable not only to already known means of committing crimes, but also to new forms that have not yet become widespread. Second, certainty: every power of the state must have clear boundaries excluding arbitrary interpretation. Third, proportionality: the depth of interference in the information sphere must correspond to the seriousness of the threat and the procedural purpose. Fourth, verifiability: any action involving the obtaining,

preservation, transfer, and use of digital information must be documented and available for subsequent legal assessment. Fifth, coherence: norms from different branches of law must not enter into destructive contradiction with one another.

This is precisely the key imperative of modern legal policy: the state must be faster than the criminal, but it must not become more arbitrary than the law. Excessively lenient regulation creates a refuge for criminal networks in legal loopholes; excessively vague and overbroad regulation undermines public trust, weakens the legitimacy of law enforcement activity, and provokes abuses. Accordingly, the updated regulatory framework must combine strictness with precision, operational speed with accountability, and power with legal culture. Only such an approach will make it possible not merely to respond to individual crimes in the digital environment, but to build a stable system of legal counteraction capable of protecting state security, the interests of society, and the rights of citizens against threats of a new historical scale.

4.4. Training a new type of personnel

The rapid escalation in the complexity of organized crime amid the universal digitalization of social relations necessitates a fundamental reassessment of prevailing approaches to staffing the bodies responsible for state security. Criminal communities are no longer confined to stable hierarchies, territorial attachment, and traditional methods of concealing traces. They now operate in distributed environments, use anonymized financial transactions, employ closed communication channels, substitute identity with digital masks, construct multi-layered schemes for moving assets, and create sophisticated spheres of influence in which criminal conduct, financial operations, information manipulation, and international intermediation merge into a single criminal mechanism. Under these conditions, state security can no longer rely on a narrowly specialized operative trained solely within the boundaries of one discipline. The present historical moment urgently calls for the formation of a new type of specialist - a complex, interdisciplinary professional capable of thinking simultaneously in legal, technological, operational, financial, and behavioral dimensions.

It is for this reason that the central task becomes the training of personnel who combine legal education, an understanding of the structure of digital platforms, skills in intelligence work within the digital environment, experience in financial and analytical inquiry, knowledge of the nature of transnational crime, as well as the ability to work with digital linguistics and the patterns of network behavior. What is at issue is not the mechanical aggregation of disparate areas of knowledge, but the formation of a qualitatively new professional integrity. Such a specialist must not merely know individual legal provisions, but must understand the limits of evidentiary admissibility, the peculiarities of national and international jurisdiction, the procedures for obtaining information from foreign digital service providers, the legal regimes governing data retention and

transfer, and the distinction between operationally significant information and evidence capable of withstanding judicial scrutiny. Their legal training must be not formal but profound, since any error in the procedural handling of a digital trace is capable of destroying even an impeccably conducted operational development.

However, knowledge of the law alone is no longer sufficient. A modern officer responsible for ensuring state security must understand the internal logic of digital platforms, their architecture, the order in which information is disseminated, the mechanisms for ranking materials, the ways communities are formed, the principles of user anonymization, the nature of digital intermediation, and the behavioral patterns of participants in network communications. It is essential that such a professional clearly understand how criminal structures use marketplaces, messengers, gaming communities, file repositories, anonymous forums, cryptographically protected communication channels, and other digital environments to recruit participants, distribute roles, coordinate actions, conceal supply routes, launder funds, and exert pressure on witnesses. Without such understanding, the state will repeatedly lag behind, reacting only to acts already committed, whereas the task of a genuinely modern security system should be prevention in advance.

No less important are the skills of intelligence work in the digital environment. Today, the identification of a criminal network increasingly begins not with physical surveillance, but with the detection of a weak digital signal that only an experienced specialist is capable of distinguishing from the general informational noise. The training of this new type of personnel must include the ability to establish connections between fragmented digital traces, identify hidden nodes of communication, recognize coordinated actions, reconstruct the structure of criminal contacts, determine centers of decision-making, and distinguish the true managerial apex of a criminal community from front figures. At the same time, it is particularly important to cultivate in personnel the capacity to work not only with explicit information, but also with indirect indicators: the timing of publications, repeated turns of phrase, the distribution of roles in correspondence, changes in the habitual behavioral patterns of participants, routes of asset movement, and the coincidence of digital events in time. It is precisely from such seemingly insignificant elements that the evidentiary picture of contemporary organized crime is assembled.

Financial and analytical training likewise deserves particular emphasis. Organized crime has long understood that power in the criminal environment rests not only on violence, but also on the ability to move, fragment, disguise, and legalize proceeds covertly. Anyone who does not understand the movement of financial flows sees only the outward shell of a crime, but not its economic heart. Accordingly, the new type of officer must command methods for analyzing transactional activity, be able to trace chains of asset movement through

multiple accounts, intermediary structures, virtual assets, sham contractual arrangements, and foreign jurisdictions. Such an officer must be able to distinguish signs of payment fragmentation, identify the artificial complication of settlements, determine the beneficial owner behind formally independent persons and organizations, and understand the connection between the financial architecture of a criminal group and its operational resilience. Under contemporary conditions, financial analysis ceases to be merely auxiliary; it becomes one of the principal avenues for exposing organized structures, because money, unlike legends and false names, always leaves a trace.

A necessary element of the new training is also a deep understanding of transnational crime. A modern criminal community crosses state borders with ease - not necessarily physically, but almost always organizationally, financially, and informationally. In the digital age, a crime is often committed in one country, organized in another, financed from a third, and produces consequences in a fourth. Accordingly, the officer responsible for state security must understand differences in legal regimes, the specifics of international cooperation, forms of mutual legal assistance, the grounds and limits for sending interstate requests, as well as typical methods of evading international prosecution. Such a professional must know how criminal networks exploit legal differences between states, which jurisdictions become convenient for concealing data, registering sham organizations, storing criminal proceeds, and hosting controlling infrastructure. Only this kind of training makes it possible to move from the sterile acknowledgment of a “foreign trace” to the real overcoming of cross-border barriers.

A crucial component in training personnel of the new type is work with digital linguistics and network behavior. This field is often underestimated, although it is precisely language, communicative style, speech habits, rhythm of communication, and patterns of digital presence that make it possible to penetrate the deep structure of the criminal environment. A criminal network speaks not only through words, but also through pauses, repetitions, silences, conventional designations, shifts in tone, and rituals of digital communication. A next-generation specialist must be able to identify hidden semantic structures, distinguish linguistic markers of allegory, understand methods of concealing meaning through the coding of ordinary expressions, record indications of the speaker’s managerial status, recognize attempts artificially to alter linguistic appearance, and establish probabilistic links between different digital accounts on the basis of linguistic and behavioral indicators. In addition, knowledge of the regularities of network behavior is required: methods of entering closed communities, mechanisms for earning trust, the roles of intermediaries, the recruitment of operatives, the formation of reputation in unlawful environments, and methods of intimidation and maintenance of internal discipline. Without understanding these processes, the state risks combating

isolated episodes rather than the logic by which the criminal system reproduces itself.

In light of the foregoing, it appears necessary to introduce specialized training programs aimed not at the abstract "mastery of digital technologies," but at solving specific state security tasks. Such programs should be built on the principle of substantive unity between law, operational activity, financial analysis, international cooperation, and the study of digital communications. Training should be not descriptive but applied; not bookish but practice-oriented; not institutionally closed but directed toward genuine cross-sectoral coordination. It would be advisable to include in the educational process the analysis of real criminal schemes, the modeling of crisis situations, the study of complex arrays of digital data, the reconstruction of chains of international cooperation, the examination of judicial practice concerning the admissibility of digital evidence, and the assessment of typical procedural errors. The specialist of the new type is formed not through lecture-based instruction, but through repeated passage through intellectually demanding and reality-based professional situations.

A special role should be played by departmental master's programs and advanced training courses structured in accordance with the needs of serving personnel. It should be emphasized here that personnel update cannot be reduced merely to the recruitment of young specialists. The state security system requires not simply an influx of new personnel, but a deep re-equipping of the professional corps already in service. Investigators, operatives, experts, prosecutorial personnel, analysts, and officers of financial control units must all be given the opportunity systematically to deepen their knowledge in adjacent fields. In this context, a departmental master's program should serve not as a formal educational stage, but as a space for cultivating a professional elite capable of integrating scholarship, practice, and strategic thinking. Advanced training courses, in turn, should not be general in nature, but specialized; short-term in format, yet intensive in substance; and promptly updated in light of new criminal schemes, shifts in judicial practice, and the development of means for concealing digital activity.

The practice of joint exercises appears no less significant. Modern organized crime defeats the state above all where state authorities act in isolation, where information is fragmented, competences collide, and the professional languages of different agencies do not coincide. Joint exercises are necessary in order to transform institutional adjacency into genuine professional interaction. Within the framework of such exercises, situations should be modeled involving the exposure of multi-episode criminal schemes, the detection of cross-border financial flows, the obtaining of data from foreign service providers, the seizure and fixation of digital media, the disruption of coordinated criminal campaigns, as well as the protection of witnesses and victims under conditions of

informational pressure. It is especially important that such exercises involve not only representatives of law enforcement and security bodies, but also specialists in financial monitoring, forensic expertise, international law, linguistic analysis of texts, and behavioral analysis. Only in such a composition is it possible to develop a unified understanding of the sequence of actions, the boundaries of competence, and the mechanisms for transferring results among participants in the process.

Training in international data request mechanisms must also become mandatory. This issue cannot be left on the periphery of professional education, because it is precisely ignorance of procedures, deadlines, formal requirements, and the specifics of interaction with foreign competent authorities that often leads to irretrievable loss of information. In digital investigations, time often determines everything: a delayed request may mean vanished event logs, deleted accounts, destroyed correspondence traces, and assets moved beyond reach. Personnel must therefore be trained both in the basic principles of international legal assistance and in practical issues: identifying the proper addressee, substantiating urgency, complying with requirements concerning the content of a request, ensuring the preservation of the information obtained, translating and legalizing documents, and coordinating international procedures with the requirements of national criminal procedure. Of particular importance is cultivating in personnel the skill of early recognition of situations in which a foreign element is present already at the initial stage, even though outwardly the case may appear domestic.

Training in digital evidentiary hygiene is of exceptional importance as well. By this should be understood the body of professional rules aimed at preventing the loss, distortion, contamination, or procedural devaluation of digital information. Digital evidence is fragile not in a material sense, but in a legal and informational one: it is easily compromised by careless action, improper documentation, incorrect extraction, the absence of a documented chain of custody, inaccurate interpretation of metadata, or the use of unverified methods of examination. Personnel training must include stable skills in handling electronic media, remote storage, event logs, geolocation data, correspondence, multimedia files, and information concerning network activity. It is necessary to teach the rules for documenting every operation, distinguishing between original and working copies, ensuring reproducibility of results, coordinating the interaction of investigator and expert, and identifying procedural risks in advance. Without such a culture, it is impossible to ensure either the reliability of an investigation, or the court's trust in the materials submitted, or ultimately the lawfulness of state intervention.

At the same time, training personnel of the new type must not be reduced merely to expanding the list of disciplines. A change in educational philosophy itself is required. The principal goal must be the formation of a professional capable of

systemic thinking, lawful action, profound analysis, and anticipation of the development of a criminal situation. Such a specialist must be able rapidly to move from a legal norm to a digital trace, from a digital trace to a financial scheme, from a financial scheme to an international element, and from an international element to a strategy for dismantling the entire criminal network. Such a professional must not only possess knowledge, but also intellectual discipline, resilience in the face of informational overload, the ability to engage in interagency cooperation, a habit of testing hypotheses, attention to detail, and responsibility for every procedural decision. The training of such personnel is complex, costly, and time-consuming; however, any alternative would mean the state's conscious acquiescence in chronic lag behind criminality.

From both a scholarly and practical perspective, it is evident that the contemporary fight against organized crime requires not merely an investigator and not merely a computer specialist, but a professional of a hybrid profile. Yet even this definition requires clarification. The matter at hand is not "hybridity" as a random combination of functions, but an integral professional model of a new defender of the state, in whom are united a jurist, an analyst, a researcher of the digital environment, a connoisseur of international mechanisms, a specialist in financial flows, and a subtle interpreter of linguistic and behavioral material. It is precisely such a professional who is capable not only of reacting to crime, but of recognizing its emergence; not only of collecting information, but of transforming it into evidence; not only of seeing an individual episode, but of uncovering the entire infrastructure of a criminal community.

Consequently, the issue of training personnel of a new type is not a secondary matter of educational policy, but one of the central questions of national security. Whether the state is able to create such a personnel system will determine not only the effectiveness of investigations into individual cases, but also the country's ability to preserve sovereignty under conditions of the digital transformation of crime. The personnel question here is a strategic one, a question of legal order, a question of citizens' trust in the state, and a question of the historical viability of the security system itself. Where specialists of yesterday are trained, the state is doomed to fight crime with yesterday's means. Where, however, a specialist of the new type is formed, there arises the possibility not of chasing the threat, but of outpacing it; not of patching consequences, but of dismantling criminal structures at their foundation. It is precisely toward such a model that the will of state institutions, the scholarly community, and the entire system of professional education must be directed.

5. INTERNATIONAL COOPERATION: RECOMMENDATIONS WITHIN THE FRAMEWORK OF INTERPOL AND OTHER INTERNATIONAL STRUCTURES

5.1. Strengthening Interpol's Role in Coordinating Platform-Oriented Investigations

In the current era of the transnational digitalization of crime, the issue of international cooperation in countering criminal communities that use communication platforms as an environment for operation, recruitment, coordination, concealment, and the redistribution of roles has acquired not merely practical but **fundamentally civilizational significance**. It is no longer sufficient to regard international police cooperation as a set of formal procedures for transmitting requests, obtaining reference information, or assisting in the search for particular individuals. Such an understanding of international cooperation, largely archaic in nature, is rapidly losing its adequacy in the face of a new criminal reality in which criminal activity is increasingly organized not around a stable geographical location, but around the digital architecture of platforms, distributed communication channels, pseudo-anonymous accounts, temporary online communities, and rapidly shifting clusters of participants.

It is precisely for this reason that, under contemporary conditions, Interpol must be conceptualized and employed not only as a channel for the interstate exchange of information, but above all as an **international coordination and analytical center** capable of identifying, correlating, and interpreting the cross-border patterns underlying the existence of digital criminal ecosystems. What is required is a transition from reacting to offenses already committed to creating a system of **proactive analytical support for investigations**, in which special attention is devoted not to an isolated episode, but to the criminal infrastructure as such: its nodes, channels of resilience, mechanisms of reproduction, rules of adaptation, and methods of evading national criminal prosecution.

In this connection, it appears advisable within the Interpol framework to initiate the establishment of a specialized area dedicated to criminal ecosystems operating on digital communication platforms. Such a field should not be oriented toward the study of individual categories of crime in their traditional sectoral isolation, but toward identifying the broader organizational environment within which illicit drug trafficking, human trafficking, extortion, fraud, the unlawful trade in personal data, extremist and terrorist propaganda, the involvement of minors in unlawful activities, and other forms of criminal conduct converge. Practice convincingly demonstrates that the same platform, the same communication channel, and the same anonymization model may simultaneously serve several distinct areas of criminal activity. Consequently, analytical work must be conducted not only by reference to the legal classification of the offense, but also according to the type of digital environment in which the criminal network arises and reproduces itself.

The creation of such a specialized area must be endowed not with declaratory functions, but with **strictly institutional powers**. Its mission should include the development of methodological approaches to identifying platform-based

criminal organization, the accumulation of typical operational scenarios of digital criminal communities, the elaboration of a conceptual apparatus suitable for uniform interstate use, and the formulation of coordinated procedures for operational and investigative response. The particular importance of this area is due to the fact that criminal communities have long learned to exploit differences between national legal systems as a source of their own resilience. While one state may classify certain conduct as preparation for a serious crime, another may treat it as an administrative offense or even as lawful conduct; while one jurisdiction retains records of online activity, another irreversibly deletes them upon the expiry of short data-retention periods; while some authorities perceive only an isolated digital trace, the criminal network has already dispersed across several states. Within this asymmetry of procedures and approaches, crime finds for itself a space of near-impunity. Accordingly, Interpol must become the institution capable of containing this asymmetry and transforming fragmentation into a coordinated system of knowledge and action.

One of the most important dimensions of such activity should be the development of **international threat profiles** for standard criminal models emerging in the digital platform environment. An international threat profile should be understood not as a brief description of a dangerous phenomenon, but as a complex analytical document reflecting the structural characteristics of a criminal model, the stages of its life cycle, the typical role composition of its participants, the means of concealment employed, the indicators of network expansion, the methods of recruiting new members, the patterns of profit distribution, the channels for laundering criminal proceeds, and the factors indicating the imminent transformation of one criminal form into another. Such profiles must be based on the comparison of materials from different states, since only a transnational perspective makes it possible to detect recurring configurations that remain invisible within the confines of a single national criminal statistic.

The importance of threat profiles is difficult to overstate. They make it possible to shift the fight against crime from a mode of fact-description to a mode of **model recognition**. In other words, investigators and operational units gain the ability to see not only what has already occurred, but also what the observed communication activity may develop into in the near future. If a characteristic combination of signs is detected-for example, a sharp increase in the number of closed groups, the emergence of intermediary accounts, the unification of speech formulas, a transition to short interaction windows, the synchronized migration of participants between platforms, and the use of multiple digital personas-this should be treated not as an accidental accumulation of circumstances, but as a symptom of the formation of a specific criminal model. This is precisely the advantage of analytically mature international cooperation: it enables authorities to recognize criminality before it becomes entrenched in its most dangerous organizational form.

Alongside this, it is necessary within the Interpol framework to develop **uniform indicators of digital criminal networks**. Without a common set of indicators, any international interaction risks remaining captive to terminological fragmentation. Today, one state emphasizes the content of messages, another the routes of digital data movement, a third financial traces, and a fourth the peculiarities of online coordination. Yet a criminal network exists as a combination of interrelated features, and its reliable detection is possible only through the integration of substantive, structural, behavioral, temporal, technical, and transactional indicators.

Uniform indicators should encompass at least several dimensions. First, there are **structural indicators**, reflecting the presence of stable coordination nodes, hierarchy, or, conversely, a distributed network organization with backup centers of control. Second, **behavioral indicators**, making it possible to record typical scenarios of digital activity: synchronization of publications, repetition of coded formulas, algorithms for onboarding newcomers, discipline in deleting traces, and cyclical changes of communication channels. Third, **content-related indicators**, pointing to the use of a specific vocabulary, conspiratorial designations, euphemistic constructions, and masking speech strategies. Fourth, **technical indicators**, associated with the nature of accounts, registration patterns, device uniformity, means of concealing location, connection features, and methods of circumventing restrictions. Fifth, **transactional indicators**, revealing the connection between communication activity and the movement of funds, digital assets, payment substitutes, prepaid instruments, and other forms of settlement. Finally, sixth, **evolutionary indicators**, enabling the assessment of a network's capacity for adaptation, fragmentation, reassembly, and the transfer of activity to new platforms following the blocking of previous ones.

The development of such indicators has not only methodological but also **evidentiary significance**. In circumstances where criminal communities increasingly refrain from leaving direct inculpatory traces and instead operate through hints, coded constructions, fragmented digital episodes, and distributed roles, it is precisely the totality of indicators that makes it possible to construct a substantiated picture of organized criminal activity. Here it is especially important to emphasize that international law enforcement cooperation must aspire not to the mechanical exchange of masses of unprocessed information, but to the coordinated use of indicators that possess stable interpretative value across jurisdictions. Only then does international cooperation cease to be a mere accumulation of fragmented information and become a genuine production of legally and criminologically significant knowledge.

Particular attention should be paid to the proposal to establish **secure channels for the rapid exchange of platform artifacts and analytical materials**. In this context, platform artifacts should be understood not only as messages, images, audio recordings, video materials, account data, and digital links between

accounts, but also as considerably more complex objects: timestamps, editing sequences, indicators of data deletion or restoration, patterns of interaction with posts, user transition schemes between channels, digital traces of community administration, moderation features, indicators of distributed governance, and other elements capable of revealing the internal structure of a criminal network.

The need for specifically rapid, and not merely formally secure, exchange is explained by the fact that the digital criminal environment operates within temporal regimes wholly different from those of traditional interstate legal assistance. Where a criminal group is capable, within a matter of hours, of deleting a body of data, changing platform, renaming channels, redistributing roles, and dissolving into a new communication contour, a month-long wait for an interstate response effectively means the loss of evidentiary prospects. Therefore, what is required is the creation of a special mechanism-procedurally and technologically secured-for the transmission of critically important information in a mode as close as possible to real time. Otherwise, international cooperation will inevitably lose to crime not in substance, but in tempo; and in the digital environment, **tempo is no longer a technical detail, but the very essence of effectiveness**.

At the same time, the creation of such channels is impossible without **strict legal regulation**. Neither legal vagueness nor the temptation to substitute legality with considerations of momentary expediency can be permitted. On the contrary, what is required is a carefully designed system of authorization, differentiated levels of access, accounting for the purposes of data use, logging of all actions involving received information, verification of the provenance of digital materials, preservation of their integrity, and compliance with national and international legal requirements concerning the protection of individual rights. Otherwise, the legitimate goal of strengthening the fight against transnational crime risks entering into a dangerous contradiction with the principles of legality, proportionality, and judicial oversight. The strength of international cooperation must be measured not by arbitrariness of instrument, but by the precision of its legal design.

No less important is the publication of **international analytical bulletins** devoted to new methods of concealment, migration, and reorganization used by criminal communities in the digital environment. Such bulletins should not be reduced to general surveys or to the mere statement of known threats. Their function is to provide states with timely, scientifically processed, and practically applicable information on new methods of concealing criminal activity, the transformation of linguistic codes, the use of lawful digital services for unlawful purposes, the evolution of recruitment pathways, the transition from open channels to semi-closed and fully closed communication environments, methods of network fragmentation after exposure, and techniques for redeploying communities under new names and with new visual identities.

The scientific and practical value of such bulletins lies in the fact that they transform isolated national experience into a **collective international resource**. If a criminal group has developed an effective concealment scheme in one country, there is no reason to doubt that this scheme will be reproduced in another jurisdiction within a very short time, especially where continuous exchange of experience already exists among members of the criminal milieu. Crime has long internalized the lesson of international cooperation-and in some respects has internalized it better than states themselves. For that very reason, every delay in the analytical dissemination of information about newly detected schemes objectively contributes to strengthening transnational criminal adaptability. In this sense, an international analytical bulletin is not merely an informational product, but a means of preventing institutional blindness, whereby public authorities in different countries encounter the same model in sequence, yet each time as if for the first time.

It should also be emphasized that strengthening Interpol's role in coordinating platform-oriented investigations must be based on engagement with a broader circle of international structures. Depending on the nature of the threat and the subject matter of the investigation, close coordination is required with regional police associations, international judicial and supervisory mechanisms, specialized bodies combatting the laundering of criminal proceeds, institutions dealing with child protection, the suppression of human trafficking, the fight against illicit drug trafficking, and the prevention of terrorist activity. However, Interpol's coordinating role in this system appears especially important precisely because it is capable of linking diverse areas of enforcement into a **single picture of the platform-based criminal environment**. Where sector-specific international mechanisms see only separate fragments of the threat, Interpol is potentially capable of perceiving its architecture.

This gives rise to another conclusion of principle. In order to enhance the effectiveness of international cooperation, Interpol must develop not only channels of interaction between states, but also **common analytical standards**, uniform approaches to the description of digital artifacts, agreed forms for the presentation of information, compatible models for threat categorization, and a shared methodology for interpreting platform-based criminal activity. Without this, information exchange will remain quantitatively abundant but qualitatively fragmented. Put differently, states may transmit enormous volumes of data to one another while remaining unable fully to extract from them their evidentiary and predictive significance. In the age of digital crime, value lies not simply in the volume of information received, but in the ability of the international community to read within that information the hidden organizational logic of the criminal network.

Ultimately, the strengthening of Interpol's role in coordinating platform-oriented investigations must be regarded as an **urgent necessity**, dictated by the

very nature of contemporary criminality. Digital criminal communities strive for boundlessness, for dissolution within transnational communication space, and for the use of differences between legal systems as a means of self-protection. The response to this strategy cannot be local, slow, or fragmented. It must be as systemic as the threat itself; as dynamic as criminal migration between platforms; and as intellectually sophisticated as the methods of digital concealment themselves.

Accordingly, Interpol must be reconceptualized as a space for the **strategic analysis of transnational digital criminal architectures**, in which international cooperation ceases to be a secondary adjunct to national investigation and becomes an autonomous condition of its effectiveness. Only on this basis can one speak of a genuine, rather than merely declaratory, strengthening of international criminal-police coordination. And if states truly intend to confront the criminality of the twenty-first century, they must acknowledge the obvious: today the struggle is no longer only for the detection of an individual offense, but also for the ability of the international legal order to understand, anticipate, and dismantle digital forms of organized criminal power. It is precisely this that constitutes the key task of contemporary international cooperation and one of the most important directions for the further development of Interpol as an institution of global human-rights and law-enforcement responsibility.

5.2. Joint International Task Forces

In contemporary conditions, the fight against transnational organized crime can no longer be conducted through the instruments of national criminal prosecution alone. Criminal networks long time ago ceased to coincide with state borders, and therefore efforts to counter them cannot remain confined within a single jurisdiction. Where a criminal organization distributes functions among organizers, intermediaries, technical operatives, financial operators, transporters, recruiters, and money launderers across multiple countries, any fragmented investigation will inevitably remain partial. It may identify a low-level perpetrator, disrupt an individual channel, or seize some material traces, but it will be incapable of dismantling the system itself. An isolated national investigation all too often strikes only at the periphery, leaving untouched the command center, the financial core, the technical infrastructure, and the mechanisms by which criminal activity is reproduced. **It is precisely for this reason that joint international operational task forces, established under the coordination of Interpol and other intergovernmental and regional law-enforcement cooperation mechanisms, assume particular importance.**

Such task forces are not merely a vehicle for the exchange of information among agencies of different states; rather, they represent a qualitatively different level of coordinated action, in which an investigation is structured from the outset as a single process rather than as a mechanical aggregation of parallel national proceedings. Their purpose is to bring within a single operational and legal

framework the capacities of the law-enforcement authorities of several states, financial intelligence units, specialized cybercrime divisions, experts in the circulation and concealment of digital assets, digital forensic specialists, and prosecutors and other officials responsible for ensuring the admissibility, relevance, and proper procedural form of international evidence. **Only such an integrated concentration of capabilities makes it possible to move from episodic reaction to the systematic dismantling of a criminal network.**

The participation of law-enforcement agencies from several states within a joint task force is dictated by the very nature of transnational crime. One state may possess information concerning transportation, another concerning banking operations, a third concerning the location of computing infrastructure, a fourth concerning the whereabouts of the organizer, and a fifth concerning the ultimate laundering of proceeds through property, controlled business entities, or nominees. So long as this information exists in isolation, the criminal organization retains the advantage: it sees the entire chain, whereas state authorities perceive only separate fragments. **A joint international operational task force removes this asymmetry** by creating the conditions for the synchronized correlation of data, the development of a unified evidentiary theory, the coordinated distribution of tasks among national segments of the investigation, and the simultaneous execution of procedural and operational measures. The point of such a task force lies not in diplomatic courtesy between agencies, but in restoring the lost wholeness of law-enforcement vision.

A fundamentally important element of such task forces is the participation of financial intelligence units. Within the structure of contemporary organized crime, the flow of money has long ceased to be merely a consequence of crime; it has become its organizational foundation. Through the movement of funds, one can identify beneficial owners, intermediaries, payment-splitting schemes, conversion points, routes of capital transfer, links between outwardly unrelated episodes, and the true scale of the network's activity. Where accomplice testimony may be incomplete, false, or self-serving, financial trails possess a particular evidentiary resilience. They reflect the objective logic of criminal circulation. For that reason, the involvement of financial intelligence is necessary not only to identify suspicious transactions, but also to map the financial architecture of the criminal organization: from the initial receipt of criminal proceeds to their concealment, dispersal, transformation into assets, fictitious liabilities, loans, securities transactions, precious metals, luxury goods, and digital asset units. **To deprive a criminal network of income is to deprive it of its capacity to expand, corrupt, recruit, and recover after coercive disruption.**

No less significant is the role of specialized cyber units. A substantial portion of transnational criminal activity is now coordinated through distributed communications tools, closed online communities, anonymization mechanisms, remote data storage, dummy accounts, technically concealed access nodes, and

complex schemes of digital intermediation. Even where traditional crimes are concerned-human trafficking, narcotics trafficking, arms trafficking, illicit trade in cultural property, rare biological resources, tobacco smuggling, fraud, extortion, and the laundering of criminal proceeds-the digital environment becomes the space for recruitment, coordination, financing, concealment, and the allocation of roles. **Accordingly, without cyber units it is impossible** to identify the infrastructure of a criminal network in a timely manner, establish the technical dependencies among participants, detect the encryption tools employed, determine the points of administration of closed platforms, prevent the remote destruction of data, and ensure operational responsiveness to the rapidly changing configuration of digital traces. Where crime seeks refuge behind technical complexity, the state must respond not with delay, but with superior expertise.

A special place within joint international operational task forces belongs to specialists in digital assets and their circulation. The use of such instruments in the criminal sphere is connected not only with attempts to disguise the origin of assets, but also with the creation of a parallel financial ecosystem in which traditional banking controls are insufficient. The conversion of criminal proceeds into digital form, the fragmentation of funds across multiple addresses, the use of mixing services, intermediary exchange platforms, sham transactions, multistage transfers, and distributed-ledger instruments enables criminal networks to complicate the identification of beneficial owners and the geography of control. Yet it would be mistaken to regard this environment as wholly opaque. On the contrary, where there is appropriate specialist training, access to analytical tools, international information-sharing, and timely judicial and procedural action, it is possible to trace a substantial portion of digital asset flows, identify key addresses, uncover links between transactions, and subsequently freeze or seize the corresponding assets. **For the criminal, digital property may appear to be a refuge; for a properly equipped investigation, it may become a map of that person's own movements and connections.**

Within such task forces, digital forensic specialists perform a function without which the reliable transformation of electronic traces into a judicially significant system of evidence is impossible. Their role is not confined to the technical extraction of data from seized devices. Rather, it encompasses the scientifically grounded capture, preservation, analysis, and interpretation of digital objects in compliance with strict requirements relating to chain of custody, reproducibility of results, verifiability of methodology, identification of the source of information, and the exclusion of uncontrolled alteration of content. In the context of an international investigation, the significance of this work increases many times over, since any error in the extraction, copying, verification, or description of a digital dataset may result in the loss of evidentiary value in a foreign jurisdiction. **It is the digital forensic specialist who converts the chaos of electronic fragments**-correspondence, connection logs, navigation data, login

records, residual files, deleted entries, image metadata, and document metadata-into a coherent system of facts suitable for judicial scrutiny. If modern crime leaves traces in device memory and network infrastructure, then digital forensics becomes the language through which those traces begin to speak in court.

Prosecutors, or other procedural supervisors capable of guiding international evidentiary work from the formulation of the investigative theory to the presentation of materials in court, must also be indispensable members of a joint international operational task force. Their presence is necessary because transnational investigations fail not only from a lack of information, but also from the incompatibility of legal regimes. Evidence lawfully obtained in one country may prove unusable in another because of differences in the authorization of investigative acts, documentation requirements, standards for the protection of individual rights, the scope of judicial oversight, the admissibility of special methods of obtaining information, or the certification of digital materials. A prosecutor within the international task force must construct a procedural strategy in advance: determining what information should be requested and in what manner, which actions should be carried out simultaneously, where prior judicial authorization is required, how to maintain the chain of custody for physical evidence, how to formulate international requests, and how to avoid duplication or, conversely, gaps in the evidentiary record. **Operational success that is not converted into admissible evidence is not a victory, but merely a conspicuous and fruitless episode.**

The effectiveness of joint international operational task forces depends to a large extent on the analytical model according to which their work is organized. One of the central models is the approach conventionally described by the formula **"follow the money."** Its essence lies in recognizing the financial flow as the principal guide for identifying organizers, beneficial owners, and the mechanisms through which criminal proceeds are laundered. Under this model, the starting point is not limited to the facts of theft, smuggling, human trafficking, or illicit trafficking in prohibited goods, but extends to any anomalous property-related processes: a lifestyle disproportionate to lawful income, payments routed through chains of nominees, unexplained asset accumulation, transfers to jurisdictions lacking transparency, abrupt fragmentation of receipts, atypical transactions between affiliated structures, and the conversion of funds into hard-to-trace forms of property. Consistent movement along this trail makes it possible to identify centers of income distribution, the individuals who make key decisions, and the infrastructure that preserves and reproduces criminal capital. In a number of cases, it is financial analysis that destroys the false picture constructed by criminal networks, which push minor operatives into the foreground while carefully concealing those who derive the principal benefit. **Money rarely lies; it moves according to the logic of power, subordination, and interest, and therefore reveals the true structure of the criminal organization.**

The second model-**"follow the administrators"**-is aimed at identifying the persons who in fact manage the network, maintain its stability, allocate roles, control communications, and make decisions concerning the movement of people, funds, goods, documents, and data. The transnational criminal environment is characterized by the deliberate blurring of leadership: a formal organizer may be absent, while management functions are distributed among several individuals, some responsible for logistics, others for finance, others for security, others for recruitment, and still others for technical infrastructure. Nevertheless, every durable criminal network has points of administration: actors with privileged access to communication channels, databases, task-distribution systems, payment-verification mechanisms, closed platforms, and internal conflict-resolution procedures. Identifying them makes it possible to strike not at interchangeable operatives, but at the coordinating nerve center of the entire structure. This requires the correlation of digital, financial, migration, transportation, telecommunications, and behavioral data in order to determine who sets the rules, who confirms transactions, who authorizes movements, and who imposes measures of secrecy. **To decapitate a network is to deprive it of its capacity for self-preservation, even if some peripheral elements formally remain at liberty.**

The third model-**"follow the infrastructure"**-proceeds from the understanding that a criminal network exists not only as a collection of persons, but also as a collection of the material and digital conditions that sustain it. This includes transport routes, warehouses, transit premises, sham enterprises, banking and payment instruments, computing capacity, servers, domain names, anonymization services, forged documents, means of communication, cryptographic mechanisms, logistics intermediaries, channels of corruption, legal shells, and assets used to conceal traces or launder proceeds. So long as this infrastructure remains functional, the criminal organization is capable of replacing personnel losses and rapidly restoring turnover. For that reason, the task of the international operational group must not be confined to the arrest of individual participants, but must extend to dismantling the supporting structures that make criminal activity stable and repeatable. This requires simultaneous pressure on all elements of the infrastructure: asset seizures, confiscation of servers and communication devices, blocking of payment channels, closure of front companies, revocation of licenses and registrations, restriction of access to storage and production facilities, identification of corrupt intermediaries, and neutralization of technical administrators. **Crime is not defeated when yet another operative is apprehended, but when the environment in which crime can regenerate the next day has been destroyed.**

The fourth model-**"follow the routes of movement"**-is of particular significance in cases involving human trafficking, irregular migration, smuggling, narcotics offenses, the movement of weapons, cultural property, rare animals and plants, and other forms of criminal activity based on border-crossing. Here the central

object of analysis is the route: the geography of recruitment, transit, placement, transfer, storage, intermediate stops, crossings of checkpoints, changes of transport and documents, and the use of border infrastructure and logistics intermediaries. The study of movement routes makes it possible to identify not only the factual trajectory of persons or goods, but also the hidden organizational structure of the network: who ensures border crossing, who prepares documents, who receives the cargo or victims, who organizes onward distribution, who provides security, who exercises coercion, debt collection, detention, and concealment. Of crucial importance here is the combination of border-control data, transport analytics, surveillance, telephone and network connection records, financial transactions, victim and witness testimony, device examinations, and navigation data analysis. **A route is not merely a line on a map; it is the scheme of power of a criminal network manifested in space.**

At the same time, none of these models should be applied in isolation from the others. A truly effective international investigation is built on their combination. Financial flows may lead to an administrator; the administrator may lead to technical infrastructure; the infrastructure may lead to movement routes; and the routes may reveal new financial nodes and previously unknown intermediaries. **A joint international operational task force is superior to fragmented forms of cooperation precisely because it allows the entire system of interconnections to be maintained within a single analytical field.** The modern criminal network is multilayered; accordingly, the response of the state must likewise be multilayered, simultaneous, and continuous.

In order to ensure the effectiveness of such task forces, clear organizational and legal foundations for their functioning are required. Above all, there must be a predetermined procedure for the exchange of information, including the classification of information by level of access, rules for the protection of personal data, conditions for the use of intelligence information in criminal proceedings, mechanisms for confirming its provenance, and permissible limits on onward transfer to third states. It is no less important to establish uniform standards-or standards subject to mutual recognition-for the recording of evidence, especially digital evidence, in order to prevent subsequent challenges. Questions of jurisdiction, priority of forum, parallel prosecution, extradition, transfer of criminal proceedings, and cross-border confiscation of assets must also be resolved in advance. **Without such normative and procedural predictability, even a well-equipped task force risks finding that operational material cannot be transformed into judicial results.** Criminal networks prevail whenever states delay over formalities; the law must not become a shelter for those who systematically destroy the legal order itself.

It is also necessary to emphasize the importance of synchronized action. A transnational network adapts rapidly to localized strikes: if arrests and searches are carried out in one country without simultaneous measures in other

jurisdictions, the organizers gain time to flee, destroy data, transfer assets, re-register property, alter routes, and recruit new operatives. For that reason, joint international operational task forces must plan the decisive phase of intervention as a single operation, in which temporal windows, target objects, addressees of procedural acts, measures for freezing assets, seizing data carriers, blocking digital services, and apprehending key persons are agreed upon in advance and executed simultaneously. **In the fight against transnational organized crime, delay is measured not in hours, but in lost opportunities to disrupt an entire system.**

The issue of trust among the participants in a joint task force also deserves separate consideration. International cooperation in the criminal-law sphere cannot be reduced to the formal exchange of requests. It requires institutional trust, grounded in predictability, professional integrity, observance of confidentiality, willingness to share sensitive information, and readiness to assume obligations of timely response. Such trust does not arise spontaneously; it is formed through regular joint exercises, professional training, the development of common methodological approaches, the exchange of analytical practices, reciprocal secondment of specialists, the creation of secure communication channels, and continuous evaluation of the quality of completed operations. **Where states act as competing observers, the criminal network remains master of the situation; where they act as a single legal organism, the space of impunity narrows rapidly.**

Finally, it is critically important that the activity of joint international operational task forces not be limited exclusively to a repressive function. Their work should also generate strategic knowledge: identifying typical schemes for concealing proceeds, new methods of using digital assets, vulnerabilities in border regimes, nodes of corruption, regulatory gaps, deficiencies in procedures for identity verification and property registration, patterns in the recruitment and movement of victims, and changes in logistical routes. That knowledge must be transformed into recommendations for legislatures, financial-control authorities, migration services, border and customs agencies, the judiciary, and bodies responsible for international cooperation. **If an operation ends only with a conviction, but does not alter the environment in which crime feeds and hides, then the state has won a battle, but has not yet turned the course of the struggle.**

Thus, joint international operational task forces should be regarded as one of the key instruments of modern counteraction to transnational organized crime. Their value lies not in the formal aggregation of representatives from different agencies, but in their ability to create a unified framework for detection, analysis, disruption, proof, and the subsequent dismantling of criminal infrastructure. Their composition should include law-enforcement authorities from several states, financial intelligence units, cyber divisions, specialists in digital assets, digital forensic experts, and prosecutors capable of ensuring the procedural

soundness of international evidence-gathering. Their work should be based on a combination of models focused on financial flows, network administrators, infrastructure, and routes of movement. **Only such an approach makes it possible to strike not at an incidental fragment, but at the very mechanism of transnational criminal reproduction.** Organized crime is global in its mode of existence; accordingly, the response to it must be equally integrated, swift, and resolute.

5.3. Standardization of international exchange of electronic evidence

One of the most acute and, at the same time, systemic problems of contemporary criminal proceedings in the cross-border environment remains the disproportionality between the speed with which electronic traces disappear and the slowness of international legal assistance. This contradiction has long since ceased to be a mere procedural difficulty of a particular kind. It has assumed the character of a fundamental challenge to justice as such. Where connection data, subscriber registration data, user activity logs, location data, network interaction data, and other forms of electronic evidence may be altered, lost, overwritten, or destroyed within hours or even minutes, the execution of an international request over the course of weeks or months in fact signifies not merely delay, but the loss of evidence as a legal reality.

Under these circumstances, the issue of standardizing the international exchange of electronic evidence should be regarded not as a purely technical or departmental task, but as a necessary condition for preserving the State's capacity to uphold legality. If criminal activity is carried out in an environment of instantaneous data movement across multiple jurisdictions, while State mechanisms continue to operate at the pace of the paper era, law enforcement begins to lose to the criminal environment not accidentally, but structurally. It is precisely for this reason that, within the framework of Interpol, regional intergovernmental associations, mutual legal assistance treaty regimes, as well as specialized platforms for inter-agency cooperation, the creation of uniform, pre-agreed, and binding rules for handling electronic evidence must be consistently advanced.

First and foremost, expedited data preservation procedures are required, that is, such legal and organizational mechanisms as would make it possible to immediately transmit to an authorized foreign entity a request for the temporary preservation of the integrity of a specific body of data pending receipt of a full request for disclosure or production. This does not mean the immediate transfer of data content without observance of national safeguards and judicial oversight; rather, it concerns the minimum necessary measure aimed at preventing the loss of such data. In the contemporary digital environment, it is the preservation stage that is decisive. If data have not been secured in a timely manner, subsequent procedural efforts often lose their meaning. International recommendations should therefore establish a uniform list of grounds for urgent

preservation, define the circle of competent authorities, prescribe permissible periods for initial preservation, regulate the extension of such a regime, determine the procedure for certifying the moment of receipt of the request, and impose on the recipient an obligation to confirm that measures to preserve the integrity of the data have been taken. Without such unification, every request will encounter discrepancies in procedural forms, departmental instructions, and national conceptions of the permissible scope of urgency.

No less important is the introduction of uniform formats for describing digital objects subject to preservation, examination, and transfer. One of the causes of refusals, delays, and erroneous execution of international requests lies in the differences in how States describe the same object: a user account, a network node, a communication device, cloud storage, an event log, a video surveillance recording, correspondence, a file, a forensic image, connection data, or subscriber registration data maintained by a communications service. Where there is no uniformity in terminology, ambiguity inevitably arises; where ambiguity exists, the evidentiary value of the material obtained inevitably suffers. Accordingly, international standardization must include the development of uniform terminological glossaries, mandatory descriptive fields for each object, rules for indicating temporal parameters, time-zone references, methods for identifying device and account identifiers, and common principles for documenting the links between the digital object, its carrier, the source of extraction, and the specific procedural act. Such a measure is not merely an improvement in records management. It eliminates legal uncertainty upon which the admissibility and reliability of evidence in court depend.

Of particular importance is the development of standard templates for urgent requests, since it is precisely at the stage of initial contact that precious time is most often lost. At present, urgent requests are frequently drafted in a free-form manner, contain incomplete information, fail to reflect the procedural basis of the request, and do not permit a rapid determination of the nature of the offence, the scope of the measures sought, or the permissible limits of interference with individual rights. As a result, the foreign recipient is compelled to spend time on clarifications, follow-up requests, and interdepartmental approvals. Yet in cases involving terrorism, organized crime, human trafficking, illicit drug trafficking, offences against the sexual integrity of minors, crimes against critical information infrastructure, serious violent offences, and other acts associated with the rapid concealment of traces, delay amounts in practice to facilitating impunity. A standardized urgent request should contain information on the requesting authority, the legal basis of the request, the legal classification of the offence, an indication of the degree of urgency, a precise list of the data to be preserved or produced, a justification of the relevance of those data to the event under investigation, an indication of the risk of their imminent loss, and details of acceptable means of communication for immediate confirmation of execution. Such templates should be translated in advance into the working languages of the

relevant organizations and accompanied by uniform instructions for completion so as to exclude semantic discrepancies.

A key element of international evidentiary interoperability is the harmonization of metadata requirements. Electronic evidence derives its value not only from its content, but also from information concerning its origin, structure, time of creation, modification, transmission, method of extraction, and conditions of storage. It is precisely this information that makes it possible to establish the authenticity of the object, detect interference, trace the chain of custody, and assess its fitness for judicial proceedings. In practice, however, States differ in their approach to the set of mandatory accompanying information: in some jurisdictions, a general indication of the source is sufficient, while in others a detailed description of the carrier, software version, time of extraction, copying method, integrity-control tools employed, and all persons who had access to the object is required. In the absence of uniform requirements, evidence obtained in compliance with the standards of one country may prove disputable or even unusable in another. It is therefore necessary to achieve international agreement on the minimum mandatory metadata set for different categories of electronic evidence. Such a set should include the object identifier, the source from which it was obtained, timestamps of all significant actions, information on the person and authority that performed the extraction, characteristics of the original carrier or remote storage, information on the methods of copying and preservation employed, data relating to integrity control, as well as a continuously documented chain of lawful custody. Without this, international exchange will produce not procedurally robust evidence, but merely information whose legal value is easily called into question.

Another crucial area is the mutual recognition of certain technical forms of verification, since it is precisely at this stage that different national approaches to certifying the authenticity and integrity of electronic data come into conflict. In some legal systems, decisive significance is attached to hash values; in others, to judicial certification procedures; in still others, to the involvement of an authorized expert; and in others again, to departmental standards of digital copying. If the international transfer of electronic evidence is not based on at least a minimally agreed set of mutually recognized methods of confirming data integrity and provenance, every cross-border case will begin with doubt as to the very evidentiary foundation. A particularly balanced approach is required here. The aim should not be the complete elimination of national procedural autonomy. On the contrary, what is needed is the development of a list of such technical forms of certification as are regarded as sufficient **prima facie** to establish that the object has not been subjected to unauthorized alteration after its extraction or preservation. International recommendations could provide for agreed rules on the generation of hash values, the logging of copying operations, the certification of the time of fixation, the preparation of extraction records, the documentation of the tools used, and the maintenance of a continuous chain of

custody. Such mutual recognition does not deprive the court of the right to assess the evidence on the merits, but it eliminates the destructive situation in which cross-border exchange is halted at the threshold by distrust of basic technical procedures.

Particular attention must be paid to the establishment of emergency freezing and preservation procedures for serious crimes, that is, a regime under which the competent authority of one State could, in strictly limited cases, promptly initiate the urgent preservation of specific electronic data in the possession of a foreign service provider, another data holder, or a competent authority of another country. It should be emphasized clearly here: such a mechanism must not become a means of circumventing judicial safeguards, expanding surveillance, or arbitrarily interfering with private life. Its purpose is strictly functional-to preserve evidence until the proper legal procedure for requesting and transferring it has been carried out. Yet that very purpose requires the highest degree of promptness. Where offences involve a real threat to life, personal security, national security, the protection of children, the prevention of a terrorist act, the exposure of organized criminal networks, or the interruption of large-scale malicious interference with vital systems, the State is not entitled to justify inaction by reference to the complexity of interstate correspondence. International instruments of both a recommendatory and treaty nature should establish the categories of cases in which such emergency measures are permissible, the limits on the volume of data to be preserved, the duration of the freezing regime, the procedure for subsequent judicial or prosecutorial review, the grounds for terminating the measure, and the guarantees of notification and legal protection for affected persons to the extent compatible with the purposes of the investigation.

It should be emphasized that the standardization of the international exchange of electronic evidence cannot be confined to the issuance of abstract recommendations. Legal form is sterile without organizational substance. For such mechanisms to function in reality, there must be permanent contact points operating on a round-the-clock basis; uniform secure channels for the interstate transmission of requests and confirmations; pre-established lists of competent authorities; agreed time limits for initial response; model guidance on the classification of urgency; as well as regular interstate training for investigators, prosecutors, judges, experts, and staff of international cooperation units. Otherwise, even the most sophisticated normative instrument will founder on the realities of interdepartmental disunity, linguistic errors, imprecise identification of the addressee, and the elementary lack of awareness among practitioners of the tools already available.

It is equally important that international standardization be built upon a balance between effectiveness and human rights guarantees. Electronic evidence is almost always directly linked to private life, secrecy of communications, freedom

of expression, personal data protection, the inviolability of professional secrecy, and other constitutionally significant interests. Therefore, the acceleration of procedures must not be understood as a renunciation of legality. On the contrary, standardization is capable of becoming an instrument for enhancing legal certainty and protecting the individual. When the grounds, limits, timeframes, forms of request, content requirements, rules of storage, and permissible methods of using data are clearly and uniformly determined in advance, the space for arbitrariness narrows, while the possibilities for subsequent judicial review increase. In other words, a properly designed international framework for handling electronic evidence serves both the interests of criminal prosecution and the interests of the legal protection of the individual.

From both scientific and practical perspectives, it appears justified to establish a multilevel model of standardization. At the first level, basic concepts, general principles of urgency, data integrity requirements, and the minimum metadata set should be agreed. At the second level, model request forms, uniform lists of mandatory details, and classifiers of digital objects should be developed. At the third level, a framework should be created for the mutual recognition of certain procedures of technical certification and data preservation. Finally, at the fourth level, implementation control should be ensured: statistical monitoring of response times, identification of typical reasons for refusal, analysis of judicial assessment of the evidence obtained, and periodic revision of standards in light of technological development and the transformation of criminal practices. Without such a multilevel structure, international standardization risks remaining merely a set of good intentions that do not alter the everyday reality of investigation and adjudication.

It must also be said that the absence of uniform international rules is particularly advantageous to those actors who deliberately structure criminal activity around the gaps between jurisdictions. Organized criminal groups, terrorist networks, persons disseminating child sexual exploitation material, fraudulent associations, and entities engaged in extortion through the use of malicious software have long learned to exploit not only anonymization and technical obfuscation, but also the legal fragmentation of the global space. They know that where the State must spend weeks formalizing a paper request, where translation takes longer than the lifespan of connection logs, and where one authority does not recognize the technical preservation performed by another, a refuge for impunity emerges. Consequently, the standardization of the international exchange of electronic evidence is not a matter of bureaucratic convenience, but a matter of closing the loopholes that legal disunity itself opens to criminality.

In this connection, recommendations adopted within Interpol and other international organizations should not be declaratory, but substantive. They should provide for model rules on immediate data preservation, uniform descriptions of digital objects, mandatory forms for urgent requests, uniform

metadata requirements, minimum standards for certifying integrity, emergency procedures for freezing data in cases of serious crime, as well as rules governing the subsequent transfer, examination, and judicial verification of the material obtained. Mechanisms for assessing compliance with such recommendations are likewise necessary: comparison of States' response times, analysis of the causes of non-execution, preparation of consolidated reports, compilation of best-practice lists, and the creation of platforms for the coordination of disputed issues. International cooperation must cease to be a space of polite formulas and become a space of measurable effectiveness.

The concluding proposition here is entirely clear. If data disappear within hours while an international request takes months to execute, justice suffers defeat before judicial proceedings even begin. In the digital age, preserving evidence means preserving the very possibility of establishing the truth. Therefore, the standardization of the international exchange of electronic evidence must be recognized as one of the central tasks of contemporary criminal policy, international procedural cooperation, and legal scholarship. Whether a uniform, rapid, legally sound, and technically reliable framework for handling such evidence is created will determine not only the effectiveness of the investigation of individual cases, but also the State's overall ability to uphold the rule of law in the face of criminality operating at the speed of an electronic signal.

5.4. Interaction with INTERPOL, EUROPOL, the United Nations Office on Drugs and Crime and regional structures

In the contemporary environment, the fight against transnational crime can no longer be structured according to outdated paradigms in which a criminal act, its preparation, commission, concealment, and monetization were confined to a single territory, a single legal system, and a single body of evidence. The digital environment has dismantled those boundaries. Today, a criminal network may recruit operatives in one state, host its command infrastructure in another, employ concealment mechanisms in a third, channel criminal proceeds through distributed payment chains in a fourth, and target victims simultaneously across several continents. In these circumstances, international cooperation must be understood not as a diplomatic adjunct to a national investigation, but as its **integral, foundational, and continuously operative basis**.

Alongside Interpol channels, particular importance attaches to the systematic use of the capabilities of the **United Nations Office on Drugs and Crime (UNODC)**, Europol, mechanisms aligned with the requirements of the **Financial Action Task Force (FATF)**, regional counterterrorism and anticrime centers, as well as networks of national computer emergency response teams where conventional criminal threats intersect with digital ones. The objective should not be the mechanical expansion of the list of international partners, but the creation of a **single operational and analytical environment** in which information,

methodologies, indicators of criminal activity, investigative alerts, and legal decisions are correlated in a manner commensurate with the speed of crime itself.

The United Nations Office on Drugs and Crime possesses exceptional potential in developing international approaches to combating **digitally enabled organized crime**. Its significance lies not only in providing expert support to states seeking to improve their legislation, but also in its ability to integrate criminal-law, criminological, procedural, and institutional agendas. It is precisely within this forum that progress can be made toward unified definitions of emerging forms of criminal activity, common criteria for classifying conduct as transnational organized digital crime, model frameworks for defining the powers of investigative authorities, and coordinated approaches to the collection, preservation, examination, and international transfer of digital evidence. Without such a **theoretical and normative foundation**, efforts to combat crime will inevitably be eroded by legal fragmentation: the same conduct will be treated in one jurisdiction as a serious criminal offence, in another as an administrative violation, and in a third as conduct not properly classified at all. Where there is no unity of concepts, there can be no durable unity of action.

Within the European space, Europol occupies a special place as a structure capable of providing **advanced criminal intelligence analysis** of large data sets, coordinating multilateral investigations, consolidating fragmented episodes into a single criminal picture, and supporting joint operations against complex networked entities. Its importance is particularly great in cases where criminal activity is serial, distributed, clandestine in nature, and accompanied by active use of encrypted communications, anonymizing infrastructure, fraudulent accounts, multi-layered payment chains, and remote orchestration of criminal conduct. In such circumstances, a single state almost never sees the crime in its entirety; it sees only a fragment. Only supranational analytical consolidation makes it possible to identify links among seemingly unrelated facts: matching digital fingerprints, recurring criminal techniques, common control nodes, the migration of the same actors across different criminal schemes, and the synchronization of attacks with the subsequent movement of funds. For that reason, analytical engagement with Europol should not be episodic, but **embedded in the day-to-day practice** of detecting, documenting, and suppressing criminal activity.

No less significant are mechanisms compatible with international standards in the field of **anti-money laundering and countering the laundering of criminal proceeds**. In the context of digitalization, illicit income increasingly takes forms that hinder its immediate recognition: distributed units of value, payment surrogates, transactions through gaming and trading platforms, multi-stage transfers via nominal intermediaries, structuring of amounts, the use of transnational payment corridors, and fictitious commercial transactions. If the financial dimension of crime remains outside the scope of international control,

the fight against it is reduced to addressing consequences rather than causes. A criminal network may lose operatives, individual server capacities, or distribution channels, but so long as the mechanism for extracting, moving, and legitimizing proceeds remains intact, it will reproduce itself. Therefore, cooperation with bodies and platforms implementing approaches to financial transparency should be directed not only at identifying suspicious transactions, but also at developing common criteria of **digital financial risk**, typologies of criminal misuse of new payment instruments, procedures for asset freezing, coordinated models for identifying ultimate beneficial owners, and mechanisms for the rapid interstate exchange of information on the movement of criminal capital. A blow to criminal infrastructure without a blow to criminal proceeds is always incomplete.

Regional counterterrorism and anticrime centers should be regarded as a **critical link** in cases where digital crime intersects with violent extremism, illicit arms trafficking, human trafficking, smuggling, drug trafficking, terrorist financing, and the destabilization of public order. The digital environment increasingly functions not as a separate sphere of crime, but as the connective layer between different forms of illicit activity. It is used to coordinate deliveries, facilitate recruitment, launder proceeds, disseminate instructions, conduct vulnerability reconnaissance, select targets, arrange covert transfers of funds, and construct deceptive informational cover. Accordingly, regional structures should not only accumulate information on traditional threats, but also possess sustainable digital analytical capabilities: correlation of network links, monitoring of communication channels, analysis of illicit platforms, and identification of indicators of preparation for distributed criminal actions. Their value lies in their proximity to the specific criminal environment and in their knowledge of the linguistic, ethnocultural, economic, and geographic characteristics of the region, without which many transborder criminal connections remain undetected. **Global coordination without regional depth is inevitably blind; regional awareness without international integration is equally destined to fragment.**

Networks of national computer emergency response teams should be integrated into anticrime cooperation whenever a technical incident proves to be not merely a disruption of the functioning of an information system, but an element of criminally punishable conduct. In practice, the distinction between the technical and criminal dimensions of a threat is often artificial. Large-scale malicious interference with networks may serve as cover for extortion; compromise of accounts may prepare the ground for theft; dissemination of malicious software may function as an instrument of blackmail, sabotage, or unlawful data collection; blocking of resources may be a means of coercing victims or eliminating competitors in the shadow economy. If response teams operate in isolation from law enforcement, **critically important time is lost**, and with it trace information: event logs are wiped, volatile data disappears, compromised nodes are reinstalled, and offenders have time to dismantle their infrastructure. It

follows that an interaction model is required in which, where indicia of crime exist, technical response and criminal procedural documentation are initiated in parallel rather than sequentially. In the digital environment, delay is not merely an organizational shortcoming; it is a direct path to the irreversible loss of evidence.

Against this background, **joint threat assessments** require particular development. Such documents should not consist of generic declarations about rising danger devoid of practical value. They must be based on verifiable data, account for sectoral and regional specifics, identify stable criminal models, describe the so-called life cycle of a criminal scheme-from preparation to profit extraction and concealment of traces-and include indicators for early detection together with lists of the most vulnerable points for intervention. The value of a joint threat assessment lies precisely in its capacity to transform disparate observations from different states into a common picture of the evolution of the criminal environment. It makes it possible to anticipate the displacement of criminal activity from one sphere to another, understand which tools are gaining popularity, identify vulnerabilities that are repeatedly exploited, determine which intermediary nodes criminals rely upon, and track changes in methods of concealment.

It is also necessary to build common repositories of information on **typical methods of preparing, committing, and concealing crimes**. Such repositories should include descriptions of criminal techniques, recurring sequences of actions, digital and behavioral indicators, anonymization tools employed, models for recruiting perpetrators, cash-out methods, methodologies for deleting traces, methods of pressure applied to victims, and characteristic mistakes made by offenders that facilitate their identification. Such data sets are especially important for identifying serial patterns, attributing criminal groups, and preparing alerts for investigative, operational, and forensic units. A criminal may change account names, communication nodes, and payment instruments, but rarely changes the entire constellation of stable behavioral characteristics overnight.

International catalogues of **digital indicators** should likewise become a mandatory element of such cooperation. This concerns not only IP addresses, domain names, file hashes, or signs of malicious activity, but also more sophisticated indicators: patterns of node interaction, temporal regularities of operations, recurring registration-data templates, traces of automation, linguistic features of messages, the structure of payment routes, parameters of the software used, and indicators of connectivity between different criminal platforms. Properly organized international exchange of such indicators makes it possible not merely to respond to crimes already committed, but to prevent new episodes and to establish quickly that events appearing independent are in fact components of a single organized activity.

There is also a pressing need for the exchange of **practical methodologies for the seizure, preservation, and analysis of data held by digital platforms**. The danger of inconsistency is especially high in this area: one state may be effective at ensuring the urgent preservation of data but encounter difficulties in obtaining it thereafter; another may have strong judicial practice but respond too slowly to short-lived digital traces; a third may possess advanced forensic capabilities but lack well-developed interagency coordination mechanisms. Yet platform data now assumes decisive importance in many cases: it can establish chains of account control, confirm synchronization of participants' actions, identify hidden administrators, recover deleted episodes of communication, trace the movement of funds, and correlate criminal campaigns with one another. International exchange must therefore encompass not abstract discussion, but **concrete, practice-tested operational models**: how to formulate requests, which data to request first, how to justify urgency, how to preserve the evidentiary integrity of the information received, how to describe its provenance, and how to present it in court.

Finally, **joint educational programs** remain one of the most important directions of development. Their purpose should not be the formal conduct of events for reporting purposes, but the development of a common professional language among investigators, operational officers, prosecutors, judges, computer forensics specialists, incident response personnel, financial intelligence units, and international coordination structures. In circumstances where crime develops at the intersection of law, technology, finance, and interstate interaction, narrow institutional training is insufficient. What is needed are educational programs that integrate legal foundations, technical skills, questions of evidentiary admissibility, the specifics of international legal assistance, methods of financial tracing, and techniques of operational analysis. Only under these conditions will international cooperation cease to be an exchange of paperwork and become a **coordinated action of professional communities** united by a common task, a shared understanding of the threat, and an equally high standard of evidentiary practice.

Thus, international organizations and specialized networks should be used not for the outward observance of the requirements of international courtesy, but as an **effective mechanism for building a common operational and analytical environment**. This means continuous data circulation, comparability of methodologies, consistency of legal qualifications, compatibility of technical procedures, speed of emergency response, and trust grounded in professional predictability. Either states will create such an environment, or criminal networks will continue to exploit the advantages of global connectivity more effectively than law and public order.

5.5. Promotion of international standards of responsibility of digital platforms

One of the most acute and, at the same time, fundamentally unavoidable issues of contemporary criminal policy is the determination of the scope of obligations incumbent upon digital platforms to assist in the lawful investigation of serious crimes. This issue cannot be resolved either through the logic of the State's complete withdrawal from the digital environment or through the transfer of law-enforcement functions to private owners of information systems. Both extremes are equally dangerous. The former turns platforms into zones of de facto legal inaccessibility; the latter undermines the foundations of legality by substituting private discretion for public authority. Accordingly, the international community must persistently seek to achieve a balance under which digital platforms do not become punitive actors, yet at the same time do not retain immunity from duties of reasonable, lawful, and timely cooperation with the administration of justice.

First and foremost, there is a need to develop minimum international standards governing platform responses to lawful requests from competent authorities. At present, one of the key problems is the extreme fragmentation of existing practice. Some owners of digital systems respond quickly but incompletely; others require excessively formalized procedures incompatible with the urgency of criminal investigations; others, in substance, create merely the appearance of cooperation by delaying deadlines or invoking internal rules that cannot take precedence over a duly issued legal request; still others apply such inconsistent approaches to similar requests that this undermines the very idea of equality in law enforcement. Yet, in the investigation of serious crimes, what matters is not abstract responsiveness, but time limits, the completeness of the information provided, the clarity of admissibility criteria for requests, the existence of a clear emergency contact channel, and the possibility of verifying what steps the platform has taken to preserve or disclose data. In this regard, an international standard should establish a minimally necessary set of obligations: registration of the request, acknowledgment of its receipt, assessment of urgency, preservation of relevant data pending substantive resolution of the matter, a reasoned response within a reasonable period, the availability of a round-the-clock emergency communication channel, and documentation of all stages of interaction. The rule of law begins where arbitrary discretion gives way to a predictable and verifiable procedure.

Particular importance attaches to the international regulation of retention periods for data relevant to the investigation of serious crimes. In the digital environment, traces are often inherently short-lived. Connection records, session data, message metadata, addressing information, device linkage data, technical logs, internal identifiers, account management history, and other digital parameters may disappear long before a law-enforcement authority completes interstate formalities. Offenders are well aware of this vulnerability and deliberately exploit platforms where the natural rate of evidentiary disappearance is high and the procedure for preserving such traces is difficult.

Consequently, international standards must proceed from a simple yet decisive proposition: in cases involving serious crimes, the retention period for relevant data cannot be determined exclusively by the platform owner's commercial interests or its internal cost-minimization policies. Agreed minimum retention periods are required for certain categories of data, differentiated by the degree of public danger posed by the offence, the nature of the incident under investigation, and the evidentiary significance of the information concerned. At the same time, such periods must be combined with guarantees of legality, purpose limitation, and the inadmissibility of arbitrary retention beyond the bounds of a lawful objective. A trace that the law has failed to preserve too often becomes a trace that can no longer be reconstructed.

Among the immediate priorities is also the creation of internationally agreed procedures for the urgent prevention of the destruction of digital traces. This concerns the so-called emergency preservation of data in situations where there are reasonable grounds to believe that its loss may occur within hours or even minutes. Such a mechanism should operate pending the completion of complex interstate procedures for obtaining information, serving not as a substitute for judicial or other lawful authorization, but as its temporary preservative adjunct. Otherwise, international legal assistance will repeatedly arrive too late, after the object of proof has already disappeared. Here again, however, it is critically important to preserve the legal balance. The emergency preservation procedure must have clearly defined grounds for application, a limited subject matter, fixed periods of validity, mandatory subsequent confirmation by a competent authority, and the possibility of ex post review of the lawfulness of its use. Otherwise, an emergency mechanism risks becoming an instrument of unjustified interference. Properly regulated, however, it becomes the very tool capable of saving evidence in the first hours after criminal activity is detected, when delay is especially destructive.

No less important are the obligations of digital platforms with respect to transparency in their interaction with competent authorities. Transparency here should be understood in two dimensions. The first is external and public: the publication of aggregated information on the number of requests received, the categories of legal grounds invoked, the proportion of requests complied with, average response times, the criteria applied to data localization, and the general principles governing internal review of such requests. The second is procedural and addressed directly to State authorities: a clear description of request formats, the categories of data available, the rules for verification of authority, emergency communication channels, conditions for data preservation, and grounds for refusal. Opacity benefits only those who seek to evade responsibility, obstruct oversight, and present arbitrary conduct as an expression of corporate autonomy. By contrast, transparency creates the conditions for comparability of practice, identification of abuses, protection of users' rights, and increased trust in lawful forms of cooperation. Where there is no transparency, there inevitably

emerges a zone of institutional shadow in which both the interests of investigation and the guarantees of legality suffer alike.

International significance also attaches to notification protocols concerning the detection of large-scale criminal networks operating through digital platforms. In practice, it is not uncommon for a platform owner to identify anomalous activity, the mass creation of interconnected accounts, coordinated use of automated tools, indications of trafficking in prohibited items, systematic involvement of minors, extortion networks, financial fraud, or some other large-scale criminal structure before the State does. Where no internationally recognized procedure exists for notifying the competent authorities, valuable time is lost, while the criminal network succeeds in changing its configuration, deleting information, and migrating to other platforms. It is necessary to establish a framework under which, upon detecting signs of large-scale and socially dangerous criminal activity, a platform is obliged, in the prescribed form, to notify the authorized authorities of the relevant jurisdiction or a specially designated coordination centre. Naturally, such notification must not be transformed into a generalized duty of total denunciation or arbitrary reporting of any unusual activity whatsoever. It must be limited to serious forms of criminality, based on predefined criteria of material significance, and accompanied by subsequent legal assessment by a competent authority. Yet to ignore this area would amount to a voluntary renunciation of one of the few early-warning signals capable of preventing criminal activity before it reaches an irreversible scale.

In developing international standards, it must be emphasized in particular that digital platforms must not substitute themselves for law-enforcement authorities. They are not entitled independently to determine guilt, issue quasi-judicial decisions on criminally relevant circumstances, or, at their own discretion, shape repressive practices beyond the limits of the law. Their function is different: to ensure the preservation of necessary data, comply with lawful and duly formalized requests, provide timely information regarding detected signs of especially dangerous activity, maintain clear and verifiable procedures of interaction, and refrain from creating artificial obstacles to investigations. This position is fundamental. Cooperation with justice is not equivalent to the usurpation of its powers. Yet the converse is equally fundamental: possession of critically important evidence and control over the environment in which serious crimes are committed cannot serve as grounds for evading responsibility under the pretext of technological neutrality.

At the international level, such standards should be advanced consistently and persistently through a combination of substantive criminal-law, procedural, treaty-based, and organizational measures. It is important to secure not merely the adoption of general declarations, but also the incorporation of specific obligations into multilateral agreements, model recommendations, inter-agency

protocols, practical guidance, and standardized forms of cooperation. It is likewise necessary to ensure the compatibility of these standards with human-rights guarantees, the protection of privacy, judicial oversight, and the principle of proportionality of interference. Only then will an international model of platform responsibility be both effective and lawful. If, however, the international community confines itself to calls for voluntary cooperation, without clear rules, deadlines, and verification mechanisms, criminal networks will continue to derive advantage from legal ambiguity, the commercial caution of platforms, and divergences between States.

Ultimately, the question of the responsibility of digital platforms is a question of the law's capacity not to capitulate before a new architecture of criminality. The State cannot permit the space in which recruitment, coordination, settlement, concealment of traces, and dissemination of criminal services occur to be removed from the sphere of reasonable duties to assist lawful investigation. Yet intervention in this sphere must likewise remain strictly subject to law, judicial guarantees, and internationally recognized procedures. Accordingly, the true task of the international community is to construct a clear, binding, and fair regime of interaction under which serious crimes do not dissolve into digital irresponsibility, while the law is equipped with the necessary means for their timely suppression and proof. It is precisely in this that the true meaning of international standards consists: not in multiplying formalities, but in restoring the effectiveness of law where criminality has attempted to place itself above borders, deadlines, and national jurisdictions.

6. PREVENTION AND INFORMATION AND LEGAL IMPACT

6.1. Prevention of demand for criminal services

Preventing demand for criminal services in the digital environment should be regarded not as an auxiliary area of public policy, but as one of the central preconditions for undermining the economic, social, and organizational foundations of criminal activity. For as long as there remains a mass, latent, or semi-open public demand for illegal digital services, any measures of suppression, however technologically advanced, will remain largely reactive in nature. Crime in this sphere is sustained not only by professional organizers, technical operatives, and financial intermediaries, but also by a broad circle of consumers who frequently seek to portray their own participation in unlawful schemes as something insignificant, routine, and almost neutral. This constitutes one of the most dangerous moral and legal distortions of our time: crime begins to disguise itself as a service, while complicity is reframed as convenience.

In this regard, demand prevention requires not fragmented or episodic explanatory efforts, but systematic, scientifically grounded, and continuously reproduced activity on the part of the state, educational institutions, mass media,

law enforcement agencies, civil society institutions, and professional associations. Its subject matter is not limited to formally informing the public of prohibitions; rather, it entails the consistent transformation of public perceptions regarding what is permissible, beneficial, safe, and morally indifferent. What is at issue is a profound influence on legal consciousness, value orientations, and everyday patterns of choice. Wherever an individual ceases to perceive an illegal digital service as a crime, the state is obliged to restore legal clarity, moral certainty, and social responsibility.

First and foremost, it is necessary to reduce tolerance toward criminal digital content and the associated practices of its consumption. The particular difficulty of this task arises from the fact that unlawful material in the digital environment is often presented in a form devoid of any outward signs of danger: as entertainment, as "useful advice," as a means of circumventing restrictions, as a way to accelerate the achievement of a desired result, or as part of an allegedly normal everyday culture. As a result, an extremely dangerous habit of emotional and moral indifference is formed. The unlawful dissemination of personal data, instructions for fraudulent conduct, offers to purchase malicious software tools, information on methods of concealing income, services for unlawfully gaining access to accounts, and material justifying harassment, extortion, illicit trafficking in prohibited substances, or other crimes come to be perceived by a significant part of the audience not as manifestations of public danger, but as a variety of permissible informational background.

Such tolerance does not arise suddenly. It develops gradually: through repeated exposure, through the dulling of emotional sensitivity, and through the spread of a cynical attitude according to which only that conduct is regarded as illegal which is followed by immediate punishment. Therefore, state prevention policy must dismantle the very mechanism by which society becomes accustomed to criminal content. What is needed here is not a dry declaration of prohibitions, but a persistent and persuasive demonstration that behind every digital product of a criminal nature stand specific victims, specific harm, and specific destruction of human destinies, property interests, business reputations, public safety, and trust in the rule of law. Society must regain the ability to perceive, behind an impersonal interface, the living reality of crime. If a citizen perceives an unlawfully obtained database merely as a "convenient set of information," this means that preventive efforts have proved insufficient; it must be made clear that what is actually involved is an intrusion into private life and a threat of blackmail, fraud, personal discrediting, and other grave consequences.

No less important is the clarification of the legal consequences of participation in shadow schemes, and this must be done in the most concrete, substantive, and non-abstract form possible. A significant defect of many preventive campaigns lies in the fact that they are confined to general warnings about "possible liability," without disclosing either the legal nature of the act, the forms of

culpability, or the distinctions among the organizer, principal offender, aider and abettor, intermediary, and consumer of an illegal service. As a result, a substantial portion of the public develops the false impression that the risk of criminal or administrative prosecution concerns only "major players," whereas the ordinary customer, recipient of a service, user of an anonymous data transmission channel, purchaser of stolen information, distributor of unlawful material, or person who provides his or her own account details for dubious transactions supposedly remains outside the ambit of legal assessment. That misconception must be systematically refuted.

Preventive informational and legal outreach must clearly indicate that participation in a shadow digital scheme rarely remains confined to a single role and almost always constitutes a chain of interconnected violations. Citizens must be informed that even the ostensibly "passive" purchase of an illegal service may entail consequences in the spheres of criminal, administrative, civil, tax, labor, and reputational liability. It is necessary to demonstrate in detail how the unlawful acquisition of access to another person's information, the use of nominee accounts, facilitation of cash-out operations, registration of fictitious accounts, transfer of means of communication, issuance of bank cards in the names of third parties, participation in schemes to conceal the origin of funds, or acquisition of stolen digital products each either constitutes unlawful conduct in itself or functions as a link in a broader criminal mechanism. In a form that is both scientifically rigorous and journalistically compelling, one obvious truth must be affirmed: there is no such thing as "harmless" participation in criminal infrastructure. Every link, however minor it may seem, reinforces the system that sustains fraud, extortion, illicit trafficking in prohibited items, theft of funds, invasions of privacy, and other socially dangerous acts.

Particular importance attaches to demonstrating the direct connection between the so-called "convenient service" and the actual crime behind it. It is precisely here that one of the key cognitive distortions of the contemporary shadow environment must be overcome: the tendency to separate consumer interest from the criminal origin of the service. The shadow digital sphere is constructed upon a language of euphemisms, substitutions, neutral designations, and pseudo-technical formulas. Unlawful interference with information systems is presented as "assistance in restoring access"; trafficking in stolen information as "information support"; deception of citizens as "arbitrage schemes"; dissemination of prohibited material as "alternative content"; and participation in financial crime as "remote side work." Such linguistic camouflage destroys society's capacity for proper legal qualification of what is taking place.

For that reason, prevention efforts must consistently expose the real substance of the shadow service. It is necessary to show that behind the promise to "solve the issue quickly" there lies either theft, extortion, unlawful access, aiding and abetting fraud, laundering of criminal proceeds, or some other form of socially

dangerous conduct. Each service must be demonstrably and persuasively linked to the actual chain of harm it causes. If a citizen is offered information about another person's private life, it must be made clear that this is not merely "information," but an instrument of pressure, blackmail, discrediting, and destruction of constitutionally protected interests. If an individual is offered payment in exchange for the use of bank details to "transfer funds," that person must understand that he or she is becoming part of a mechanism for concealing financial flows serving fraud, drug-related crime, corrupt transactions, or other grave offenses. If a teenager is offered remuneration to distribute certain material online, it must be shown that this may amount to participation in extremist, fraudulent, pornographic, narcotics-related, or other criminal activity. Legal education in this sphere must do more than inform: it must strip crime of its mask.

Special preventive work with young people is of exceptional importance, since it is precisely young persons who most often become the targets of staged involvement in shadow digital practices. In this context, the criminal environment acts deliberately, subtly, and ruthlessly. It exploits age-specific characteristics: the desire for recognition, the search for independent income, curiosity toward the forbidden, underestimation of long-term consequences, trust in the authority of an "experienced interlocutor," and a tendency to perceive the digital environment as a space of convention and play. On this basis, mechanisms of recruitment are constructed that often begin with outwardly neutral actions: carrying out minor tasks, registering accounts, transferring means of communication, placing advertisements, delivering items, receiving and forwarding money, disseminating messages, or participating in closed communities. In substance, however, what is taking place is the gradual destruction of the individual's legal barriers and moral sensitivity.

Accordingly, prevention among young people cannot be confined to abstract appeals to "obey the law." What is required is deep, age-differentiated, and pedagogically sound work based on exposing typical recruitment scenarios, indicators of manipulation, methods of psychological pressure, mechanisms of recruitment, and the subsequent exploitation of the dependent position of the recruited person. Adolescents and young adults must be able to recognize not only direct criminal solicitation, but also the initial stages of inducement: promises of "easy money," assurances of "complete anonymity," claims that "nothing serious is happening," references to the widespread nature of the practice, and appeals to need, resentment, feelings of exceptionalism, or protest. It is necessary to explain clearly that the criminal environment never offers equal cooperation: it seeks an operative who can be replaced, used, blackmailed, framed, and, at a critical moment, made the scapegoat. Behind the façade of apparent freedom there is almost always exploitation, and behind the promise of earnings lies the prospect of a criminal record, loss of educational opportunities, destruction of family ties, and collapse of one's social future.

At the same time, preventive efforts directed at young people must rely not only on fear of punishment, but also on the formation of a stable legal identity. It is not enough to tell a young person what must not be done; it is necessary to show why compliance with the law constitutes a form of personal dignity, civic maturity, and genuine freedom rather than an external restriction. Otherwise, any warnings are quickly displaced by the temptation of profit. Here the role of the educational environment, the family, mentorship, and examples of socially approved self-realization is particularly significant. Young people must see before them not merely a list of prohibitions, but a clear alternative: lawful paths of professional growth, creative development, civic participation, income generation, and social recognition. Wherever the lawful space is left vacant, it is immediately occupied by the criminal intermediary.

Targeted work with vulnerable social groups is also of particular importance, since demand for criminal digital services is often intensified not only by legal ignorance, but also by poverty, social isolation, debt burden, low levels of education, addiction, family disorganization, unemployment, migratory instability, digital illiteracy, psychological instability, and other factors of social disadvantage. To ignore these circumstances is to substitute declarative statements for genuine prevention. A person placed in conditions of chronic deprivation is far more likely to accept an offer to participate in a dubious scheme; an individual suffering from loneliness and lack of recognition is more readily drawn under the influence of closed communities; and a citizen with a low level of legal culture is more likely to believe in the impunity of unlawful transactions. Consequently, demand for criminal services must be regarded not only as a product of individual choice, but also as a consequence of accumulated social deformations.

Targeted prevention presupposes identifying those population groups for whom the risk of involvement is especially high and building communication with them that is not generalized, but substantively and socially proportionate. For minors, one set of methods is required; for unemployed young men, another; for elderly persons vulnerable to fraud, a third; and for citizens with prior experience of administrative or criminal offenses, a fourth. At the same time, this must not amount to stigmatization. On the contrary, effective prevention proceeds from recognition of the human dignity of every person and from the need to avert crime before it turns into a personal catastrophe. The state is obliged not only to prohibit, but also to offer a way out: legal aid, social support, employment programs, educational initiatives, psychological assistance, restoration of educational trajectories, and family counseling. Wherever a vulnerable person receives lawful support, demand for criminal services loses a substantial part of its appeal.

Informational and legal influence as a whole must be built on the principles of continuity, evidentiary grounding, and real-life credibility. Episodic campaigns

timed to particular incidents are incapable of substantially changing the situation if they do not develop into a lasting presence of law in public consciousness. It must be assumed that the modern digital environment continuously reproduces new forms of temptation, neutralizes prior warnings, updates methods of disguise, and creates an illusion of normality where criminal calculation is in operation. In response, the state and society must create a stable regime of legal visibility of crime, in which no shadow service is perceived as neutral, technical, or routine. This requires a combination of legal education, public debate, analytical publications, judicial practice, clarifications by competent authorities, scholarly expertise, and the work of educational and cultural institutions.

It is fundamentally important that preventive rhetoric not be reduced to a bureaucratic enumeration of prohibitions. In its scholarly and publicistic dimension, it must possess moral force, intellectual depth, and factual irreproachability. Society must hear not an impersonal notification, but the clear voice of the legal order calling things by their proper names: unlawful access is an attack on security; acquisition of a criminal service is a contribution to the expansion of the criminal market; use of stolen information is participation in the infliction of harm; handing one's details over to criminals is not "helping acquaintances," but opening a channel for further theft and concealment of traces; indifferent consumption of criminal content is a form of social complicity in the degradation of the legal environment. When these meanings are left unarticulated, crime receives its most important advantage: the right to be misunderstood.

Ultimately, one firm conclusion must be acknowledged: it is not enough to combat supply alone; it is necessary to reduce demand for criminal digital services systematically, persistently, and purposefully. Wherever there remains a consumer of an illegal product, its supplier will inevitably emerge; wherever society remains tolerant of shadow profit, crime will reproduce itself again and again in new organizational forms; wherever the citizen seeks convenience at any cost, law will be displaced by calculation and public safety by private self-interest. For that reason, genuine prevention is not a peripheral measure, but a strategy of society's civic self-protection, moral mobilization, and legal self-respect. Only such an approach makes it possible not merely to react to offenses already committed, but to destroy the very environment in which an illegal digital service appears profitable, habitual, and acceptable. It is precisely here that the line is drawn between formal counteraction and the genuine protection of society against contemporary crime.

6.2. Shift from Abstract Advocacy to Evidence-Based Prevention

In contemporary society, crime prevention in the digital environment can no longer remain a matter of general appeals, moralizing formulas, and abstract warnings aimed at an indeterminate audience. Such a mode of informational

influence has lost its effectiveness precisely because the criminal milieu has radically transformed the ways in which it reproduces itself. It no longer operates solely through crude coercion, overt threats, or explicit inducement to unlawful conduct. On the contrary, its power lies in its ability to dissolve into familiar forms of everyday communication, to imitate ordinary modes of employment, to simulate legitimate income, and to disguise itself as routine services, intermediary activity, assistance with payments, delivery, order processing, remote support, investment facilitation, recruitment, training, consulting, and other outwardly innocuous forms of social activity. Under these conditions, the former abstract style of propaganda proves not merely weak but, to a certain extent, helpless, because it combats not the real mechanisms of recruitment and involvement, but rather their simplified and outdated image.

It is precisely for this reason that prevention must be **evidence-based**, that is, grounded in the systematic study of actual methods of recruitment and involvement, in the precise description of criminal scenarios, in the identification of recurring behavioral patterns among recruiters, intermediaries, and organizers, and in the analysis of case law, investigative materials, victim testimonies, statistically corroborated communication patterns, and recurring elements of criminal disguise. What is required is a shift from verbal condemnation to an explanation of danger that is cognitively rich, legally precise, and psychologically accurate. Only then does prevention cease to be external noise and become an instrument for recognizing threats.

Within such a framework, **case-based analytics** assumes particular importance, namely, the study of concrete instances in which individuals are drawn into unlawful activity, followed by the identification of typical indicators, sequences of actions, and stable mechanisms of influence. A concrete case is incomparably more persuasive than any abstract appeal, because it demonstrates not a theoretical possibility of risk but an already realized pathway of criminal entanglement. In one instance, this may take the form of an offer of "temporary part-time work" with minimal requirements and a promise of daily payment; in another, a request to open an account, obtain a payment instrument, or register a means of communication "for the needs of the organization"; in a third, involvement in forwarding parcels, receiving funds, registering accounts, posting advertisements, obtaining confirmation codes, transmitting account details, or formally participating in a chain of payments. Outwardly, such acts are not always perceived as criminally punishable, especially when they are performed in fragments, under the guise of isolated assignments, and without immediate disclosure of the ultimate purpose. Yet it is precisely **case-based analysis** that makes it possible to show how a combination of seemingly neutral acts amounts to full participation in a criminal scheme.

Scientifically grounded prevention should not merely retell isolated examples; it must uncover the **models of involvement** that underlie them. These models

possess a certain internal logic. As a rule, involvement begins with the removal of suspicion. To achieve this, markers of ordinariness are employed: polite communication, a businesslike tone, the absence of direct requests to break the law, a promise of simple duties, a plausible everyday cover story, an indication of urgency but not emergency, and an emphasis on the accessibility of the work to anyone, including students, the unemployed, low-income individuals, migrants, persons burdened by debt, and those seeking a quick way to obtain money without long-term employment. This is followed by a stage of gradual displacement of moral and legal reference points: the person is asked to perform an act that appears insignificant, temporary, technical, and devoid of independent social danger. Thereafter, a mechanism of fragmentation of responsibility is triggered: each individual act is presented as secondary and unrelated to the final criminal outcome. Finally, once the person has been drawn into the chain of operations, they are informed either of part of the true purpose or placed in a situation of factual dependency in which refusal becomes psychologically, materially, or organizationally difficult.

Revealing these **models of involvement** is especially important because crime in the digital environment operates through the normalization of dangerous behavior. A person is made to believe that their participation is merely technical assistance, a temporary formality, or minor support unrelated to any serious offense. In this way, a false distance is created between the executor of an individual task and the ultimate criminal outcome. The law, however, evaluates conduct not according to the subjective verbal packaging imposed by the organizer, but according to the real substance of the acts, their direction, the person's awareness, the nature of their assistance, and their place within the overall scheme. Accordingly, prevention must dismantle in advance the illusion of the legal neutrality of intermediary acts. It is necessary to explain, persistently and on the basis of evidence, that the transfer of account details, the registration of means of identification in the name of a straw person, the receipt and forwarding of funds, the registration of fictitious accounts, the storage and transfer of items of unknown origin, participation in false correspondence with victims, and the processing of orders lacking a transparent commercial purpose may all constitute components of a single criminal mechanism and may each entail independent criminal-law assessment.

An essential element of **evidence-based prevention** is the systematization of standard fraudulent schemes. An offender rarely acts in a state of total improvisation; far more often, they reproduce already tested structures of psychological influence. Some schemes are built on promises of easy income for minimal effort; others exploit trust in supposedly official institutions; still others imitate lawful commercial activity; and still others rely on emotional pressure, pity, fear of losing an earning opportunity, or the desire to solve an urgent financial problem. At the same time, a standard fraud scheme invariably combines several indispensable components: the creation of an appearance of

legality, the selective release of information, the migration of communication into closed channels, the substitution of concepts, the elimination of time for reflection, the shift of emphasis from purpose to procedure, assurances of safety, references to the widespread nature of the practice, and the constant verbal neutralization of doubt. A person is not told, "commit a crime." They are told: "it's just a routine formality," "everyone does it," "you're only helping process a payment," "there's nothing illegal here," "management bears the responsibility," "your task is simply to pass this on," "it's temporary," "it's just a check," "it's an internal procedure," "it's necessary to overcome restrictions," or "it's required for client servicing." The entire rhetoric is built on replacing the substance of the acts with their outward technical shell.

This is why preventive work must not simply enumerate dangerous offers; it must analyze the **language of deception** as an instrument of criminal influence. In such schemes, words serve not a descriptive but a concealing function. They do not communicate the actual state of affairs; they repackage it into a form that is convenient for the victim or intermediary participant to accept. Under the guise of neutral vocabulary lies a redistribution of risk: the entire danger is shifted onto the recruited individual, while the organizer remains in the shadows, preserving distance and therefore a greater degree of protection from immediate detection. Prevention must therefore teach not merely caution, but the recognition of verbal indicators of substitution: excessively vague descriptions of duties, refusal to disclose the substance of the work in advance, demands to use personal documents or payment details for the benefit of third parties, promises of disproportionately high remuneration for primitive actions, evasion of written formalization, the imposition of urgency, and categorical demands not to discuss the assignment with relatives, acquaintances, lawyers, or representatives of state authorities.

An integral component of **evidence-based prevention** is recourse to real judicial consequences. Society must see not only the moment of recruitment, but the full legal outcome of criminal involvement. So long as prevention remains limited to phrases about "possible liability," it stays within the realm of conditional warning and fails to achieve the necessary degree of persuasiveness. What is needed instead is a systematic explanation of how the relevant acts are legally classified, which specific offenses are identified in the conduct of intermediaries, nominal executors, persons who provide their data, couriers, recipients, custodians, go-betweens, persons who communicate with victims, or those who transfer funds, and how courts assess their arguments about ignorance, the supposedly technical character of their participation, or the absence of personal interest in the final outcome. Judicial practice convincingly shows that the assertion that a person "only passed it on," "only registered it," "only received it," or "only transferred it" does not by any means always eliminate criminal liability. On the contrary, where a combination of objective and subjective elements is present, such acts may be treated as aiding and abetting, co-perpetration,

participation in the laundering of criminal proceeds, facilitation of fraud, involvement in the illegal circulation of prohibited substances, offenses against property, offenses in the sphere of computer information, or other crimes depending on the concrete factual structure.

The explanation of judicial consequences serves a **dual function**. First, it destroys the myth of the impunity of peripheral participants in a criminal network, who are often persuaded that all responsibility lies exclusively with the "main organizers." Second, it returns the legal discussion to its true foundation: criminal law responds not to a person's self-justification, but to their actual contribution to a socially dangerous act. In this regard, it is critically important to illuminate not only the fact of punishment, but also the collateral consequences: a criminal record, restrictions in employment, damage to business and personal reputation, financial recovery measures, seizure of property, procedural costs, restrictions on holding certain positions or engaging in certain activities, migration-law consequences for foreign nationals, strain on family life, and the psychological consequences of participation in criminal proceedings. The more concretely the full range of legal and social consequences is disclosed, the stronger the preventive effect.

Yet the true evidentiary character of prevention is not exhausted by a legal description of sanctions. It requires a deeper analysis of the mechanisms by which **trust is manipulated**, because contemporary criminal involvement is built not primarily on the demonstration of force, but on the exploitation of the basic properties of human consciousness and social behavior. Trust is a foundational precondition of normal social life; without it, neither economic exchange, nor professional cooperation, nor family and neighborhood mutual assistance is possible. For precisely this reason, the offender seeks not to destroy trust as such, but to intercept it by inserting themselves into familiar forms of communication. They use symbols of legality, intonations of competence, visual markers of officiality, the sequence of business interaction, the imitation of procedures, references to rules, confirmations, reviews, recommendations, and a false transparency of action. All of this creates in the addressee a sense of a familiar and therefore safe environment.

The manipulation of trust is usually carried out through several successive **psychological mechanisms**. First comes the mechanism of authority: the message is framed in such a way that the recipient experiences the interaction as one with a person possessing status, knowledge, special powers, or organizational resources. Next comes reciprocity: after a minimal "benevolent" contact, the individual is expected to take a return step by providing data, performing a task, confirming an operation, or offering temporary assistance. Then comes gradual involvement: first, an insignificant act is proposed, after which the probability of agreement to the next act increases. An important role is also played by time scarcity: haste deprives a person of the ability to critically verify the

circumstances. Finally, the mechanism of social normalization is particularly dangerous, whereby the potential victim is led to believe that such actions are widespread, ordinary, and generally accepted practice. All this requires prevention not to engage in slogan-like condemnation of gullibility, but to provide a subtle and respectful explanation of the ways in which normal human qualities-responsiveness, the desire to earn money, readiness to help, faith in order, and a tendency to follow formal instructions-are transformed into points of criminal vulnerability.

From this follows another fundamental task: demonstrating how **criminal networks disguise themselves as ordinary services**. This is perhaps one of the most dangerous features of contemporary criminal organization. Criminal activity increasingly ceases to present itself in an overtly unlawful form; on the contrary, it strives to be unrecognizable, to resemble an everyday service, an intermediate support function, logistical assistance, payment intermediation, operator support, assistance with processing, customer acquisition, message handling, or the execution of assignments that do not appear to go beyond the bounds of everyday routine. Here lies the profound social challenge: crime mimics convenience, speed, accessibility, and everyday utility. It promises to remove difficulties, shorten procedures, ease formalities, eliminate restrictions, save time, find a customer, transfer funds, accept an order, confirm identity, arrange delivery, or assist with payments. Yet beneath this shell there often lies a distributed criminal system in which each "ordinary" act functions as an operational element of a broader unlawful result.

Scientifically oriented prevention must expose the very **mechanism of such disguise**. First, the criminal network fragments its structure into numerous inconspicuous roles, each of which appears harmless in isolation. Second, it avoids ensuring that participants are fully informed, so that each sees only their own fragment and does not comprehend the whole. Third, it uses outward signs of ordinary economic or communicative activity: correspondence in a businesslike tone, job titles, instructions, schedules, template responses, and formalized assignments. Fourth, it seeks to shift the legal trace onto the recruited person: documents, payment operations, means of communication, physical receipt of objects, account registration, and confirmation of actions. Fifth, it quickly replaces one performer with another, preserving the resilience of the system even when individual participants are identified. Accordingly, prevention must show not only the isolated risky contact, but the **architecture of the criminal network as a whole**: who receives the benefit, who bears the principal risk, who remains invisible, how roles are distributed, and why the peripheral participant is usually the most vulnerable to criminal prosecution.

What is most effective is not rhetoric of intimidation, but a clear explanation of how **digital everyday life** is transformed into an environment of criminal recruitment. This idea has fundamental methodological significance.

Intimidation works only briefly and often only on those who are already inclined toward caution. Moreover, excessively harsh and schematic warnings often produce the opposite effect: a person fails to recognize in a real situation the threat described in the admonitory message precisely because reality turns out to be outwardly far more prosaic, calm, and ordinary. Digital everyday life is dangerous not because it is exceptional, but because it is familiar. A criminal offer arrives in the form of an ordinary message. An illegal assignment looks like a small favor. Recruitment is disguised as employment. The transfer of details is explained by business necessity. Correspondence with a victim is presented as client communication. The receipt and forwarding of funds is called payment processing. Accepting a parcel is called logistical assistance. Creating an account is described as technical registration. If prevention does not expose this substitution of form for substance, it loses even before legal influence begins.

For this reason, contemporary prevention must be **explanatory and analytical** in character. Its object should not be an abstract image of a "bad act," but a sequence of specific everyday actions which, in a certain combination, form a criminal chain. The citizen must be shown their own life trajectory within the sphere of risk: how an offer of part-time work arrives in a messenger app; how the interlocutor avoids giving direct answers about the employer; how at first the person is asked to perform a harmless task; how this is followed by a demand to use personal documents, an account, a device, or an address; how artificial urgency is created; how a prohibition on disclosure is introduced; how rapid payment is promised; how the person who gave the instructions disappears at the first problem; and how the recruited individual remains the only visible participant in the entire scheme for the victim, the bank, the telecommunications operator, and law-enforcement authorities. Only such a concrete reconstruction gives a person a genuine chance to recognize the threat in real life rather than in abstract didactic form.

To increase the effectiveness of informational and legal influence, preventive messaging should strive for the **maximum possible specificity**. It is not enough to say, "do not trust suspicious offers." It is necessary to explain which specific signs should arouse doubt, why they are dangerous, how they correlate with already known forms of criminal activity, and what legal consequences may follow. It is not enough to state, "do not share your data." It is necessary to explain how personal data, bank details, communication identifiers, delivery addresses, access credentials, and accounts are used for criminal purposes, how they are employed to create a false legal appearance of legitimacy, and why the owner of such information is often the first to fall within the scope of investigative interest. It is not enough merely to mention manipulation in formal terms. One must show it step by step: the establishment of contact, the lowering of critical vigilance, the creation of illusory benefit, the fragmentation of assignments, the substitution of terminology, the formation of dependency, and the severing of feedback once the recruited person has been used.

At the same time, **evidence-based prevention** must remain respectful toward its audience. Public moralizing, reproaches for gullibility, and arrogant opposition between "reasonable" and "unreasonable" citizens are methodologically unsound and socially harmful. They do not strengthen the ability to recognize threats; rather, they intensify shame, push the experiences of victims into silence, and reduce citizens' willingness to seek help. Yet for prevention, the lived experience of those who have already been drawn into a criminal scheme-who initially failed to recognize the danger and then encountered criminal-law, financial, and personal consequences-is of exceptional value. Such experience should not be an object of ridicule, but a source of knowledge. Society has a duty to draw conclusions from it, and state and academic institutions must translate those conclusions into clear preventive formulas.

Accordingly, the transition from abstract propaganda to **evidence-based prevention** is not a minor methodological adjustment, but a profound transformation in the very philosophy of crime prevention. It is a shift from slogan to analysis, from intimidation to understanding, from generalities to a legally and psychologically precise description of threat, and from formal information delivery to the cultivation of an ability to recognize criminal disguise in the everyday digital environment. Such prevention must rely on **case-based analytics**, reveal **models of involvement**, systematize typical deceptive schemes, demonstrate real judicial consequences, expose the mechanisms of trust manipulation, and consistently show how criminal networks hide beneath the shell of ordinary services. Only in this case will informational and legal influence cease to be a ritual and become an effective means of civic protection.

Ultimately, what is at stake is the protection not only of particular individuals, but of the very fabric of **social trust**, which today is subject to deliberate criminal exploitation. If the state, academia, and society do not learn to explain to citizens exactly how crime enters their everyday lives under the guise of convenience, earnings, service, and simple assistance, no external strictness of wording will compensate for the lack of genuine understanding. But if prevention becomes **evidence-based**, concrete, legally precise, and psychologically persuasive, it will acquire the very power that abstract propaganda has always lacked: the power of exposure. And once the mechanism of involvement is exposed, it loses a significant part of its power.

7. PRACTICAL PRIORITIES FOR THE NEAR FUTURE

In the **short to medium term**, state policy aimed at combating organized crime operating in the platform environment cannot be confined to isolated measures designed merely to address crimes after they have already been committed. Law enforcement now faces a **qualitatively new challenge**: not simply to respond to discrete offences, but to build an integrated system for the **early detection**, **evidentiary preservation**, **inter-agency correlation**, **financial tracing**, **international disruption**, and **preventive counteraction** of criminal formations

that use digital infrastructure as a space for recruitment, coordination, concealment, and profit generation. For this reason, the practical priorities for the near future should be understood not as a list of disparate administrative assignments, but as a programme for the **institutional reconfiguration of the state** in the face of a new criminal reality.

First and foremost, it is necessary to establish **unified national centres for the analysis of platform-based crime**. At present, one of the principal weaknesses of the state response lies in **institutional fragmentation**. Information on criminal activity is dispersed among the police, investigative authorities, financial intelligence units, customs bodies, prosecutorial authorities, security services, communications regulators, and other competent institutions. Criminal networks, by contrast, operate as a **single organism**: they rapidly change communication channels, redirect financial flows, divide roles, use proxy accounts, rely on remote access, and exploit cross-border data storage infrastructure. When confronted with this form of organization, the state cannot afford to respond through bureaucratic disunity.

A unified national centre for the analysis of platform-based crime should become not yet another bureaucratic superstructure, but a hub for the **collection, correlation, and predictive interpretation** of criminally relevant information. Its purpose is not to replace criminal investigation or inquiry, but to secure the **analytical superiority of the state**. Such a centre should aggregate information on typical criminal schemes, persistent digital traces, methods of concealment, recurring indicators of coordination, routes of criminal proceeds, and interconnections between platforms distributing illicit content, intermediary actors, and ultimate beneficiaries. Of particular importance is the development of **uniform methodologies for identifying criminal platforms**: from analysing the structure of network interactions to determining indicators of centralized control, role allocation, repeated criminal conduct, and the connection between digital activity and real-world economic or violent crime.

No less significant is the adoption of **standards for the digital preservation of evidence**. Law enforcement practice shows that **evidentiary vulnerability** often turns manifestly criminal conduct into a legally ambiguous picture insufficient for a well-founded procedural decision. The digital environment is characterized by rapid change, the ease with which information can be deleted, the possibility of retrospective editing, the multiplicity of intermediate service providers, and a high degree of dependence on proper procedural preservation. In such circumstances, arbitrary, fragmented, and technically incomparable methods of recording evidence become a direct threat to justice.

The state requires **mandatory uniform rules** for the authentication of digital traces, covering the detection, seizure, copying, description, storage, and presentation of information relevant to criminal proceedings. This includes procedurally robust preservation of correspondence, files, metadata,

timestamps, transmission routes, device identifiers, network logs, payment records, user actions, access parameters, and traces of data alteration. Such standards must establish requirements for the **continuity of the chain of custody**, the verification of data integrity, the documentation of technical tools used, the admissibility of remote examination of information, the authentication of file provenance, and the recording of all manipulations performed on a digital medium. Without such safeguards, the state will repeatedly face the dangerous situation in which an offender prevails not because he is innocent, but because the traces of his conduct were preserved in a legally defective manner.

The next priority is the creation of **inter-agency databases of indicators of criminal networks**. Modern organized crime rarely reveals itself through a single conspicuous event. Far more often, it manifests itself through a constellation of seemingly unrelated signs: similarities in phrasing across different communication channels, matching publication intervals, recurring methods of recruitment, typical transfer routes, common technical parameters of accounts, similar methods of disguising goods and services, recurring intermediary wallets, addresses, devices, and contacts. When these indicators remain scattered, the criminal network remains invisible. When they are systematically accumulated and correlated, the state begins to perceive the **structural map of the criminal enterprise**.

Such databases should contain not only data on specific individuals, but above all a system of **forensically significant indicators**-that is, features enabling separate digital episodes to be linked to a broader pattern of organized criminal activity. It is essential that such datasets be formed on a lawful basis, with clear access controls, strict guarantees of prosecutorial and judicial oversight where required, and the capacity for prompt updating. The practical value of inter-agency databases lies in their ability to shift law enforcement from episodic disruption to exposing the **entire architecture of the criminal network**: organizers, administrators, coordinators, operatives, providers of technical resources, financial operators, and persons facilitating the laundering of proceeds.

Particular attention must be paid to strengthening **financial and crypto-analytics**. It should be stated plainly: in the context of platform-based crime, the movement of funds is no longer a secondary accompanying element, but the **central axis of criminal activity**. It is through financial flows that the internal structure of the criminal association, the distribution of roles, the scale of operations, the territorial reach, and the resilience of the network become visible. **Money is the language of organized crime**, and unless the state learns to read that language in all its complexity, it will remain perpetually behind.

Financial analytics must cover both traditional payment methods and transactions carried out using **digital assets**, **distributed ledger technologies**, and derivative methods for concealing the origin of funds. This requires a combination of legal, economic, and forensic approaches. It is necessary to

develop methods for detecting anomalous transfers, structuring of sums, cascading redistribution of funds, the use of multiple intermediary wallets, the rapid conversion of digital assets into fiat currency, and reverse conversion operations designed to break the traceability of property. Equally important, however, is the ability to interpret these processes in evidentiary terms: to link financial movements to specific criminal episodes, to the persons controlling the transactions, and to the ultimate beneficiaries. Without **deep financial analysis**, no disruption of platform-based crime can be regarded as complete, because removing individual operatives without dismantling the financial circuitry of the criminal network merely creates the conditions for its rapid regeneration.

Among the urgent tasks is the development of procedures for the **expedited international preservation of data**. Digital crime long time ago transcended national jurisdiction not only in its consequences but also in its infrastructure. Information crucial to an investigation may be stored on servers in one country, administered from another, concern victims in a third, and be used by a criminal group dispersed across several states. The key problem lies not only in obtaining such data, but above all in ensuring its **prompt preservation**. While traditional-and often protracted-mutual legal assistance procedures are underway, information is frequently deleted, altered, or becomes effectively inaccessible.

Accordingly, international cooperation must include **accelerated mechanisms for the urgent securing and preservation of digital information**, pending its subsequent formal transfer through procedural and diplomatic channels. Such procedures are necessary in relation to access logs, registration data, connection records, the contents of correspondence within the limits permitted by the law of the relevant state, technical characteristics of accounts, payment information, linked-device data, and other information vulnerable to rapid loss. This requires not only a treaty framework, but also a network of **permanent contact points** capable of responding around the clock, under uniform protocols, and within short timeframes. Otherwise, organized crime will continue to exploit the **asymmetry of time**: states need weeks and months, while criminals need only minutes.

In the same context, it is of fundamental importance to initiate within **INTERPOL** specialized lines of work on **platform-based organized crime**. International policing structures are objectively confronted with the need to update their priorities. Whereas traditional forms of transnational organized crime-drug trafficking, human trafficking, illicit arms trafficking, and money laundering-previously occupied centre stage, today all of these phenomena are increasingly organized, concealed, and scaled through digital platforms. This requires not merely an expansion of existing methods of work, but the creation of a **distinct area of activity** devoted specifically to the platform-based nature of contemporary organized crime.

Such a workstream should focus on the systematization of criminal platform typologies, the exchange of best investigative and analytical practices, the coordination of international operations, the development of common terminology, and the creation of rapid-alert channels for new criminal models. Its most important outcome would be the formation of a **shared international threat picture**, in which individual states no longer see only local episodes, but are able to relate their own data to broader transnational processes. **Platform-based crime does not respect national borders**; accordingly, the response to it cannot remain narrowly national.

However, no organizational reform will be effective without the development of **training programmes for hybrid-profile personnel**. A particularly acute shortage now exists of specialists capable of operating with equal confidence in the legal, forensic, technical, financial, and international-law dimensions. Older professional training models, based on rigid separation of competencies, no longer correspond to the complexity of modern criminal ecosystems. An investigator who does not understand the nature of a digital trace risks overlooking critical evidence. A technical specialist unfamiliar with criminal procedural requirements may obtain information that is inadmissible in court. A financial intelligence officer who does not recognize the organized structure of a criminal network sees only isolated suspicious transactions rather than the system as a whole.

Accordingly, there is a need to develop a **new generation of interdisciplinary specialists** capable of combining legal precision, analytical depth, technical literacy, and a strategic understanding of organized crime. This requires not only advanced training for current personnel, but also a revision of the curricula of departmental academies, universities, and professional training centres. Such programmes should integrate criminal law, criminal procedure, forensic science, the law of evidence, financial monitoring, international cooperation, the fundamentals of digital platforms, methods of network analysis, the psychology of recruitment into criminal communities, issues of laundering criminal proceeds, and the methodology for investigating cross-border crime. A state that fails to prepare personnel for the new criminal era will inevitably wage tomorrow's battle with yesterday's tools.

It is also **strategically important** to incorporate the assessment of **digital criminal platforms** into the system of **national security**. This proposition requires particular insistence, because in many states such crime is still perceived as a narrow specialist issue for law enforcement alone. In reality, platform-based criminal structures affect not only public order, but also economic resilience, trust in state institutions, the protection of minors, information sovereignty, the stability of the payment system, sanitary and pharmaceutical safety, electoral processes, migration governance, and even the country's international reputation. Once a criminal network acquires the capacity to exert mass influence

over social behaviour, to manage shadow markets, and to derive profit from digital anonymity, the issue is no longer a mere aggregate of separate criminal offences, but a **threat of a systemic nature**.

Accordingly, the assessment of criminal platforms should be embedded in **state mechanisms of strategic forecasting**, in security planning documents, in national threat indicator systems, in procedures for inter-agency exchange of significant information, and in crisis-response frameworks. It is necessary to develop methodologies for assessing the scale, resilience, and social danger of such platforms, to identify sectors and social groups at heightened risk, and to account for the impact of criminal digital infrastructure on the lawful economy and public institutions. The recognition of platform-based organized crime as a **national security threat** is not a rhetorical gesture, but a necessary condition for the mobilization of state resources.

Alongside coercive and organizational measures, it is critically important to develop **preventive information-law initiatives**. It is mistaken to assume that the fight against organized crime is exhausted by detection and punishment. The platform environment operates according to the logic of constant audience expansion, and criminal networks therefore seek not only to conceal themselves, but also to **recruit**. They normalize unlawful conduct, portray criminal earnings as an ordinary life strategy, disguise violence as a service, and present participation in criminal schemes as a trivial side job. Particularly vulnerable are young people, persons with limited legal awareness, users in difficult financial circumstances, and citizens unable to critically recognize manipulative practices.

Preventive work must therefore be structured as a **systemic state policy of legal education and public warning**. It should explain the real mechanisms of recruitment into criminal schemes, demonstrate the legal consequences of participation even in so-called low-level roles, clarify indicators of recruitment, methods of psychological pressure, forms of misuse of personal data, the risks of transferring payment instruments to third parties, and the dangers of acting as an intermediary in financial transfers or holding digital assets on behalf of others. Equally important is the need publicly to dismantle the myth of the **impunity** and **facelessness** of platform-based crime. Society must clearly understand that behind the façade of impersonal communication channels stand specific organizers, specific victims, specific ruined lives, and specific harm to the state. In this context, prevention is not an ornament to punitive policy, but its **necessary continuation and foundation**.

Finally, it is necessary to pursue the **international standardization of engagement with platforms**. Where a significant share of communication, trade, and payment activity is concentrated on private digital platforms, the effectiveness of crime control depends to a considerable extent on how consistently and predictably relations between states and such entities are structured. At present, this sphere is marked by fragmentation: different states impose different requirements

regarding response times, disclosure procedures, removal of unlawful content, data preservation, user identification, and compliance with lawful requests from competent authorities. Such divergence creates **legal uncertainty** and enables criminal networks to select the most advantageous jurisdictions and platforms.

International standardization should be directed towards the development of **agreed minimum obligations for platforms** in the areas of data preservation, responses to lawful requests, notification of detected indicators of serious organized criminal activity, protection of the evidentiary integrity of information, and respect for users' rights. It is critically important here to maintain a **proper legal balance**: the state must not transform private platforms into an uncontrolled punitive instrument, but platforms are likewise not entitled to shield themselves behind claims of technical neutrality where their infrastructure is systematically used to coordinate serious crime, traffic prohibited goods, launder proceeds, exploit vulnerable persons, and recruit operatives. What is required is an **internationally agreed model** under which platforms' obligations are clearly delineated, procedures are transparent, oversight is lawful, and individual rights are guaranteed. Only such an approach can overcome the present situation in which cross-border private infrastructure develops faster than the mechanisms of public accountability.

In conclusion, it should be emphasized that the priorities outlined above form a **single architecture of the state's practical response** to platform-based organized crime. National analytical centres without uniform evidentiary preservation standards will be overwhelmed by disputable data. Preservation standards without inter-agency indicator databases will not make it possible to see the network as a whole. Financial analytics without international data preservation will lag behind events. International cooperation without trained personnel will become a formality. Strategic recognition of the threat without prevention will not reduce the social base for recruitment. And engagement with platforms without international standardization will remain uneven and vulnerable.

For that reason, what is required from states in the immediate future is not a cosmetic refinement of isolated procedures, but the **political will for a systemic rethinking** of the very nature of combating organized crime in the digital age. The time for half measures has passed. Criminal networks have already learned to turn the platform environment into a space of **power, profit, and control**. The question now is whether the state can turn that same environment into a space of **legality, evidentiary reliability, international coordination, and inevitable legal accountability**. The answer to that question will determine not only the effectiveness of criminal policy, but also the capacity of the modern state to preserve the **sovereignty of law** in an era of rapidly changing technological reality.

8. CONCLUSION

The current stage in the development of social relations clearly demonstrates that the digital environment has ceased to be merely an auxiliary space for communication, information exchange, and everyday coordination of actions. It has become one of the key environments of social organization, within which stable ties are formed, roles are distributed, patterns of trust are maintained, behavioral stereotypes are reproduced, and practices of collective interaction are consolidated. For this very reason, digital communication platforms used by millions of people in everyday life are increasingly functioning not simply as a backdrop against which crime occurs, but as a fully-fledged environment for its operation. Under these conditions, organized crime acquires qualitatively new opportunities: to conceal the structure of interactions, rapidly redistribute functions among participants, replace lost links, shift activity across different communication channels, and preserve resilience even when individual elements of its network are partially dismantled.

The fundamental danger of this phenomenon lies in the fact that we are no longer dealing with isolated unlawful acts committed through technical means, but with a profound transformation in the very logic of criminal organization. Whereas in the past the criminal environment depended to a considerable extent on the territorial proximity of participants, personal contacts, materially fixed channels of communication, and the relatively slow processes of recruitment, coordination, and resource redistribution, today many of these constraints are losing their former significance. The digital communication environment reduces the costs of criminal interaction, expands geographic reach, increases the speed of decision-making, and makes it possible to preserve relative anonymity under the outward appearance of ordinary everyday communication. This creates a situation in which criminal activity no longer stands apart from social reality as an external force, but becomes ever more deeply embedded in its routine mechanisms.

It must be emphasized that the threat is determined not only by the technical characteristics of the platforms in use. Encryption, distributed server infrastructure, the rapid deletion of information, the ability to create multiple accounts, high-speed message transmission, and the difficulty of establishing the actual location of participants are all undoubtedly significant. However, to reduce the problem solely to these factors would be to narrow its substance unjustifiably. No less important-and in many cases even more important-are the social embeddedness of these platforms, their broad legitimacy in the eyes of the public, the psychological familiarity of their use, and the fact that criminal interaction is disguised as ordinary, unremarkable everyday activity. Wherever millions of law-abiding citizens exchange messages, make purchases, search for employment, participate in discussions, and maintain personal contacts on a daily basis, criminal structures obtain an unprecedented opportunity to dissolve into the general flow of communication and to use its scale and rhythm as a natural cover.

The psychological familiarity of the digital environment creates a particular advantage for organized crime. Individuals tend to perceive a regularly used means of communication as neutral, safe, and mundane. This reduces vigilance, facilitates the recruitment of new participants, blurs the sense of the boundary between what is permissible and what is unlawful, and contributes to the formation among perpetrators of a false perception of distance from the consequences of their acts. When a criminal instruction is transmitted in the form of a brief message, when coordination is carried out through a familiar interface, and when recruitment takes place in a space associated with ordinary communication, the unlawful act loses, in the perception of some participants, its obvious exceptional character. What emerges is a dangerous effect of normalization, in which crime ceases to be experienced as a transgression of socially acceptable boundaries and begins instead to be perceived as one variety of pragmatic employment, intermediary activity, or an "ordinary" service. Such a psychological transformation is especially destructive in youth environments, where digital interaction skills often precede the full development of legal consciousness and civic responsibility.

No less significant is the fact that digital criminal infrastructure possesses a high capacity for recovery. Traditional enforcement measures, even when successful at the level of individual episodes, accounts, groups, or intermediaries, often prove insufficient to achieve a durable result. The closure of one communication channel, the removal of one criminal group, the detention of one coordinator, or the seizure of one body of information does not automatically lead to the destruction of the entire network. On the contrary, the network-based principle of organization allows criminal structures to reproduce lost elements quickly, transfer communication to adjacent platforms, duplicate channels of coordination, use pre-prepared backup accounts, and restore disrupted links within an extremely short period of time. This capacity for self-reproduction reflects one of the most important characteristics of contemporary organized crime-its structural flexibility, by virtue of which even effective coercive actions often produce only a temporary rather than a final effect.

It is precisely for this reason that law enforcement agencies and other security bodies must transition to a fundamentally new model of activity. Previous approaches, based primarily on investigating already completed episodes, reacting only after harmful consequences have materialized, and operating within isolated bureaucratic silos, no longer correspond to the scale and dynamics of the threat. The modern model of counteraction must be interagency in structure, analytically robust in method, technologically equipped in instrumentation, and coordinated in its goals and procedures. In this context, interagency cooperation should be understood not as a formal distribution of powers, but as a genuinely functioning regime of joint work in which information available to different bodies is not dispersed across closed institutional circuits, but integrated into a unified understanding of the structure

of the threat. Organized crime prevails wherever the state is fragmented into separate departmental zones of responsibility; accordingly, effective counteraction is possible only where information, competencies, and operational capacities are brought together within a single system.

Analytical reinforcement of counteraction presupposes abandoning the narrow understanding of investigation as the mere recording of an already identified event. A transition is needed toward identifying patterns, stable connections, role distribution, methods of concealment, channels of financial support, mechanisms of personnel reproduction, routes for the dissemination of prohibited items and information, and the early detection of signs indicating the formation of new criminal configurations. The focus must rest not only on specific perpetrators, but also on recurring behavioral models that point to the existence of an organizing structure. The issue is one of seeing crime not as an isolated act, but as a manifestation of a larger system possessing its own internal discipline, functional specialization, recruitment channels, and mechanisms of self-protection. Only under such an approach can fragmented suppression be replaced by the systemic weakening of the criminal environment.

The technological capacity of the state also requires fundamental rethinking. In circumstances where criminal communities rapidly master new methods of concealment, automate certain processes, use distributed communication schemes, and seek to minimize direct contact among participants, state institutions cannot remain in a perpetually reactive position. At the same time, an important qualification is necessary here: technological strengthening should not be understood exclusively as the accumulation of surveillance tools. Genuine capacity means having personnel capable of correctly interpreting digital traces, unified methodologies for their recording and evaluation, legal grounds for timely intervention, secure channels of interagency interaction, and an organizational culture oriented toward the rapid transformation of disparate information into evidentiary and operationally meaningful results. Technology without methodology and without qualified analysis does not create an advantage; it merely increases the volume of unprocessed material.

Special attention should be paid to the position of state security agencies, since platform-based criminalization affects not only the criminal law sphere in its traditional sense. As digital platforms increasingly become channels for coordinating the illicit trafficking of prohibited substances, arms trading, the recruitment of operatives, the laundering of criminal proceeds, the dissemination of violent practices, the undermining of public order, and covert external influence on domestic processes, the problem extends beyond ordinary criminal statistics. It begins to affect the resilience of the state as a complex political and legal system. When criminal networks gain the ability to rely on transnational digital communications, exploit the economic and social vulnerabilities of the population, influence local communities, finance

destructive activities, and disguise them as ordinary digital practices, the threat ceases to be particular and becomes systemic.

The issue here concerns the protection of public security, institutional resilience, and elements of national sovereignty. Under contemporary conditions, sovereignty manifests itself not only in control over territory, borders, and formal legal regimes, but also in the state's ability to ensure normative order within those communicative spaces through which a significant portion of social life is conducted. If critically important segments of social coordination are mediated by digital platforms lying beyond the state's effective jurisdictional reach; if criminal networks use those platforms for the sustained reproduction of their activities; and if the state is compelled constantly to react ex post facto, without the ability to shape the structural conditions under which such environments operate, then the issue is not merely one of difficulties in investigative practice. It is one of the gradual erosion of the state's capacity to guarantee the rule of law in those forms of social interaction that have become foundational for the modern individual. Hence the need to regard platform-based criminalization as a phenomenon possessing not only criminal-law significance, but also strategic significance.

At the same time, it would be mistaken to assume that this problem can be resolved solely through the efforts of a single state, however developed its legal and institutional mechanisms may be. The transnational character of digital crime objectively makes the international dimension a central condition of effective counteraction. Accounts may be created in one jurisdiction, coordination may be carried out through the infrastructure of another, data may be stored on the technical facilities of a third, and the consequences of criminal activity may be manifested within the territory of a fourth. Such dispersion destroys the traditional linear model of law enforcement, under which a state encountering an offense on its territory possesses a sufficient set of tools for the rapid identification of offenders and suppression of their activities. In the digital environment, this chain is broken by numerous interstate barriers: differences in legal regimes, the length of mutual legal assistance procedures, divergence in requirements governing data retention and disclosure, and the absence of uniform standards of response on the part of digital intermediaries.

It is precisely for this reason that the international community must move from declaratory formulas to genuinely functioning mechanisms of cooperation. For too long, the problem has been discussed primarily in terms of general calls for collaboration, while criminal networks have, in the meantime, developed practical, rapid, and highly effective schemes of transnational coordination. States cannot afford the luxury of slowness where criminal communication is measured in seconds and official requests in weeks and months. What is needed are mechanisms for the expedited exchange of relevant information, coordinated procedures for the preservation of digital traces, generally recognized criteria for

their admissibility, joint operational measures, and unified-or at the very least comparable-approaches to the responsibility of those intermediary structures that in practice provide the environment for mass criminal interaction. Without this, the gap between the speed of criminal adaptation and the speed of state response will only widen.

The question of the responsibility of digital intermediaries also requires special consideration. Contemporary public discourse often oscillates between two extremes: either intermediaries are assigned almost all blame for what occurs in the digital environment, or, conversely, they are regarded as entirely neutral carriers of others' activity, neither capable of nor obliged to influence what takes place. Both positions appear methodologically untenable. A digital intermediary is indeed not identical to the criminal community using its infrastructure, but neither can its role be reduced to mere technical presence. The larger the platform, the more deeply it is integrated into everyday life, and the more actively it shapes rules of access, regimes for the dissemination of information, data retention arrangements, user identification mechanisms, and procedures for responding to requests from public authorities, the more evident its influence on the overall configuration of criminogenic risks becomes. Accordingly, the issue should be framed not in terms of abstract accusation, but in terms of clearly formulated, legally defined, and internationally coordinated obligations to assist in the suppression of organized crime, while strictly observing legality and human rights.

Ultimately, the principal conclusion of the study is that the fight against organized crime in the digital environment cannot be confined to responding to individual messages, individual accounts, individual episodes of prohibited content dissemination, or individual criminal acts. Such an approach is strategically inadequate by definition, because it operates at the periphery of the phenomenon without affecting its reproductive core. Contemporary organized crime exists as an integrated infrastructure: it possesses communication channels, recruitment systems, an internal division of labor, financial routes, rules of concealment, disciplinary mechanisms, logistics, procedures for replacing lost participants, and methods of integration into the everyday digital environment. As long as the state combats only the visible fragments of this system, the system itself continues to exist, reconfigure itself, and return in a new guise.

It follows that the true object of counteraction must be the infrastructure of criminal interaction itself-in the entirety of its organizational, communicative, financial, legal, and social dimensions. It is necessary to identify centers of coordination, disrupt stable channels of communication, block mechanisms of personnel reproduction, suppress sources of material support, eliminate the conditions that allow impunity through disguise as ordinary digital activity, and create such a legal and institutional environment in which the existence of a

criminal network becomes unprofitable, difficult, and dangerous. Only an infrastructural approach makes it possible to shift the fight against crime from the mode of endless reactive pursuit to the mode of systematically weakening its viability.

At the same time, it is critically important to understand that durable results are possible only through the integration of coercive, legal, analytical, and societal dimensions of counteraction. Coercive action is necessary where a concrete threat must be neutralized and criminal resources removed from circulation. Legal action is necessary to establish clear rules of liability, procedures for access to relevant information, and limits on permissible intervention. Analytical action is necessary to understand the hidden structure of the criminal network and to forecast its further evolution. Finally, the societal dimension is indispensable because any criminal infrastructure feeds not only on technical possibilities, but also on social weaknesses: legal illiteracy, economic vulnerability, distorted value orientations, tolerance for shadow practices, and the habit of perceiving the digital environment as a space of irresponsibility. Wherever society fails to develop an internal immunity to criminal normalization, the state will inevitably face the continual reproduction of new perpetrators and new intermediaries.

Thus, contemporary organized crime relying on digital communication platforms represents not a temporary anomaly and not a merely particular technological challenge, but one of the most serious tests for the rule of law in the twenty-first century. Its strength lies in its speed, flexibility, transnational reach, and ability to use the everyday digital environment as the basic resource of its own existence. Accordingly, the response of the state and the international community must be no less systemic, no less rapid, and, above all, no less integrated. Historical experience clearly demonstrates that crime prevails where law lags behind reality, where agencies act in disunity, where international cooperation drowns in formalities, and where society fails to recognize the scale of the threat. Yet the same experience demonstrates something else as well: where political will is joined with scientific clarity, institutional discipline, and strategic foresight, even the most complex forms of criminal organization can be systematically deprived of their resilience.

For this reason, the concluding thesis must be stated with maximum clarity: in the digital age, the protection of legal order requires combating not the superficial manifestations of crime, but the very architecture of its networked existence. Only such an approach corresponds to the true scale of the challenge. Only it is capable of ensuring not a short-term, but a long-term result. And only it makes it possible to preserve what constitutes the foundation of statehood and social peace: human security, institutional stability, the effectiveness of law, and the sovereign right of the state to protect its own legal space from those forces that seek to turn everyday communication into an instrument of organized criminal domination.