Observatoire ARGA

Independent Analytical Review of Public OSINT Allegations and Attribution Methodology

Concerning Dmitrii Artiukhov

(For the purposes of evidentiary reliability assessment and compliance risk evaluation)

Author:

Sergey Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Unit

Mailing address: 14 rue Jacques Laffitte, Bayonne, 64100

Contacts: info@argaobservatory.org, +33 7 58 49 62 27

Website: www.argaobservatory.org

Paris, 30 January 2026

PART 1. General Framework, Scope of Analysis and Qualification of the Source Material

The present analytical text has been prepared for the purpose of conducting a structured review of a publicly distributed OSINT-type publication associated with the project known as “Payment Shield” (“Платёжный ЩИТ”), which contains a set of allegations concerning the alleged involvement of Dmitrii Artiukhov in activities described by the authors of the publication as criminal in nature, including extortion, participation in shadow financial schemes, interaction with illegal gambling infrastructure, and the use of cryptocurrency instruments for the concealment of financial flows.

The referenced publication is presented by its authors as an investigative product and is accompanied by a substantial volume of technical and quasi-technical data, including cryptocurrency wallet addresses, transaction hashes, IP address references, user-agent strings, email identifiers, online aliases, and references to alleged interactions with cryptocurrency exchange services and digital infrastructure providers. At the same time, the narrative structure of the publication contains elements of personalized accusatory rhetoric, direct address to the alleged subject, and categorical evaluative conclusions that are presented as established fact.

For the purposes of this analysis, it is essential to distinguish between three separate layers of information: publicly available allegations, technical correlation indicators, and institutionally verified factual findings established through procedural or regulatory mechanisms. This distinction is critically important because the reviewed publication systematically conflates these categories and presents technical correlation artifacts as if they were equivalent to verified evidence of personal involvement.

From a methodological standpoint, the publication demonstrates the characteristics of a narrative OSINT construction in which fragmented digital traces, indirect associations, and hypothetical logical connections are assembled into a unified accusatory scenario without the presentation of an evidence chain meeting the standards of forensic analytics, criminal procedure, or regulated financial investigation. The publication does not provide references to primary data sources that have undergone independent verification, does not contain certified expert reports, does not disclose procedural validation of obtained information, and does not demonstrate a documented chain of custody for digital materials allegedly relied upon by the authors.

Particular attention must be drawn to the absence of references to any procedural documents issued by law enforcement authorities, court decisions, formal notifications of charges, international enforcement notices, or regulatory sanction designations. Accordingly, the publication cannot be interpreted as reflecting an established legal status of Dmitrii Artiukhov or as documenting the outcome of an official investigation conducted by competent authorities.

The publication further relies heavily on extended correlation attribution methodology, whereby the alleged connection between digital identifiers and a specific individual is inferred through the accumulation of indirect indicators such as alias similarity, email pattern overlap, IP intersection,

activity timing correlations, and behavioral assumptions. Within professional forensic and investigative practice, such indicators are treated exclusively as risk markers or preliminary intelligence signals that require independent corroboration. They do not constitute identity confirmation.

Based on the above, the publication should be treated strictly as a collection of unverified public allegations capable of generating reputational and compliance exposure but lacking evidentiary characteristics required for legal, regulatory, or enforcement decision-making.

It is further necessary to recognize that within modern cross-border compliance environments, the mere existence of publicly distributed OSINT allegations can create secondary institutional risk, namely the risk of financial institutions adopting restrictive measures based on unverified narrative sources. In this context, the present analysis is not intended to evaluate Dmitrii Artiukhov as an individual but rather to evaluate the evidentiary reliability and methodological robustness of the source material itself, and to determine the extent to which such material can be considered suitable for compliance or regulatory reliance.

PART 2. Assessment of the Claimed "De-Anonymisation" Process and Methodological Limitations of Digital Identity Attribution

A substantial portion of the reviewed publication is dedicated to describing what is presented as a process of identifying individuals allegedly associated with the "Payment Shield" project through the analysis of digital traces, including online aliases, recruitment advertisements, forum activity, telephone numbers, and social media data. Based on the combination of these elements, the authors of the publication assert the establishment of identity attribution and subsequently infer functional roles within the alleged project structure.

From the standpoint of established digital forensic and investigative standards, such an approach cannot be considered sufficient to confirm identity attribution. The publication relies on a linear correlation model in which the existence of connections between aliases, online accounts, telephone identifiers, and platform registrations is interpreted as evidence of a single controlling user. In contemporary digital environments, particularly within semi-anonymous communication ecosystems, such overlaps may arise for a wide variety of reasons, including shared credential use, delegated account access, proxy infrastructure usage, registration using third-party contact data, or deliberate identity obfuscation.

Particular emphasis is placed in the publication on the use of a telephone number as a primary identity anchor. The narrative suggests that the presence of a telephone number across multiple digital services establishes control of those services by a specific individual. However, this interpretation does not account for the widespread use of virtual numbers, SIM cards registered to third parties, corporate communications infrastructure, VoIP routing solutions, and multi-user access environments. Without documented confirmation from telecommunications providers identifying the actual user of the number during specific time intervals, and without independent corroborating evidence, such data cannot be considered reliable personal identifiers.

The publication further references the existence of video footage allegedly showing an individual working on a laptop with a browser window open to a domain referenced elsewhere in the

publication. However, the publication does not provide any information regarding the authentication of the video material, the identification process of the individual depicted, the exclusion of staged or coincidental capture, or the integrity and storage continuity of the original digital file. The absence of metadata disclosure, acquisition context, and storage verification procedures precludes treating such material as reliable evidence even within internal investigative frameworks, let alone within judicial or regulatory contexts.

Notably, the publication proceeds from these indirect digital correlations to categorical conclusions that a specific individual functioned as an administrator of the referenced channel. No evidence is presented regarding platform operator confirmations, administrative log access records, verified login traces from controlled devices, or infrastructure ownership verification. In the absence of such elements, conclusions regarding operational control of digital infrastructure remain speculative.

Within international cybercrime and financial investigation practice, identity attribution requires a multi-layer evidentiary structure typically including telecommunications records, service provider records, event logs, and documented preservation of digital evidence integrity. The reviewed publication does not demonstrate the presence of such a structure, and therefore the described “de-anonymisation” process cannot be considered to meet minimum evidentiary reliability standards.

It is therefore appropriate to characterize the identity attribution narrative presented in the publication as an analytical reconstruction based on probabilistic correlation rather than verified identity confirmation. The use of such probabilistic reconstruction as the basis for allegations of criminal involvement is inconsistent with established forensic, investigative, and evidentiary principles.

Furthermore, the publication fails to distinguish between the existence of technical access to a digital asset and the active operational use of that asset during a defined timeframe. In modern distributed digital environments characterized by shared infrastructure and delegated access models, such distinctions are critical. The absence of such differentiation significantly weakens the reliability of the conclusions presented and materially increases the risk of misattribution.

Taken together, the section of the publication dedicated to the alleged “de-anonymisation” of participants must be treated as a hypothesis-level analytical construct rather than as a verified investigative finding supported by institutionally validated evidence.

PART 3. Claims of Insider Cooperation, Alleged Access to Internal Communications and Documents, and Source Reliability Concerns

Following the alleged identification of one of the supposed administrators of the project, the publication transitions to what is presented as a decisive evidentiary escalation: the claim that the identified individual allegedly agreed to “cooperate” and provide internal information from management-level internal communication channels. The publication further asserts that such cooperation resulted in access to internal communication systems, internal documentation, and a so-called “White List” allegedly containing records of entities purportedly subjected to extortion practices.

From an investigative methodology perspective, this transition represents one of the most structurally vulnerable elements of the publication. The authors effectively request that the reader accept, without independent verification, both the existence of the insider source and the authenticity of the allegedly obtained materials. The publication does not disclose the identity or verifiable status of the source, does not provide context regarding how access was obtained, does not disclose the scope or completeness of the allegedly obtained data, and does not provide original unredacted source files or verifiable extraction metadata. No evidence is provided regarding hash verification, extraction environment documentation, or technical proof of data integrity preservation.

Within established investigative practice, including corporate investigations and digital forensic examinations, information obtained from insider sources is subject to at least two independent validation layers. First, it must be verified that the source actually possessed the claimed level of access during the relevant time period. Second, the chain of custody of the extracted materials must be documented in order to exclude modification, selective extraction, or fabrication. The publication provides no indication that either validation step was performed. As a result, the reader is asked to rely on unsupported claims regarding both the existence and authenticity of the alleged internal data.

The publication simultaneously asserts that the alleged insider was connected to potentially unlawful activities while treating information allegedly provided by that same individual as reliable evidence against third parties. This creates an inherent conflict-of-interest problem and undermines the neutrality of the source. Individuals facing potential liability frequently possess strong incentives to shift responsibility, provide selective information, or construct narratives that minimize their own exposure. The publication does not demonstrate any attempt to mitigate this fundamental risk through independent corroboration or documentary confirmation.

Additional legal and evidentiary concerns arise from the alleged method of obtaining internal communications and documents. If internal communications and system access data belonging to third parties were indeed accessed and transferred, the publication raises serious questions regarding authorization, data protection compliance, confidentiality obligations, and evidentiary admissibility. For the purposes of the present analysis, the critical issue is evidentiary reliability: information of unknown origin, unsupported by verifiable acquisition and preservation documentation, cannot be treated as reliable evidence for institutional or regulatory conclusions.

The alleged existence of a “White List” containing records of entities purportedly subjected to extortion represents an especially serious allegation affecting potentially numerous third parties. However, the publication provides no description of how such a list was created, no verification methodology, no documentation confirming actual payments, and no evidence demonstrating the presence of legally recognizable extortion elements such as coercive demand, threat, or causal linkage between alleged demand and financial transfer. The claim therefore remains declarative rather than evidentiary.

Even if internal communications or internal documentation were hypothetically to exist, their evidentiary value is not automatic. For internal data to be considered reliable evidence, authorship must be verified, context must be confirmed, data integrity must be validated, and

risks of selective extraction or manipulation must be excluded. The publication instead relies on fragmentary references to screenshots and message excerpts without presenting full communication context or independent verification procedures.

The publication also employs a common narrative technique: substituting the appearance of insider knowledge for evidentiary reliability. The use of technical terminology such as “internal management chats,” “bot access,” and “internal documents” creates a perception of evidentiary strength while failing to satisfy fundamental evidentiary verification requirements.

Accordingly, the section of the publication relying on alleged insider cooperation must be considered methodologically weak. It is based on unverified source claims, lacks documented validation procedures, contains clear source bias risks, and does not satisfy minimum evidentiary custody standards. Any conclusions drawn from such alleged internal data must therefore be treated as unverified allegations rather than verified investigative findings.

PART 4. Interpretation of Cryptocurrency Transaction Data, Exchange Interaction Claims, IP and User-Agent References: Substitution of Technical Correlation for Identity and Control Attribution

A significant portion of the publication is dedicated to the description and interpretation of cryptocurrency transactions, alleged interactions with exchange and conversion services, references to IP address activity, user-agent strings, email identifiers, and other technical parameters. These technical elements are presented by the authors as forming a cumulative evidentiary basis supporting the assertion that specific cryptocurrency wallet addresses are controlled by Dmitrii Artiukhov and were allegedly used for the movement and conversion of funds associated with criminal activity.

From the standpoint of professional blockchain forensic methodology, such conclusions require a significantly higher evidentiary threshold than is demonstrated in the publication. While public blockchain ledgers allow for the observation of transactional movement between addresses, the visibility of transaction flows does not, by itself, establish beneficial ownership, operational control, or identity attribution. Professional blockchain investigations typically differentiate between transaction-level linkage, probabilistic clustering of addresses, and identity attribution based on independently verified KYC or regulatory disclosure data. The publication effectively collapses these layers into a single inference step without demonstrating the analytical methodology used to bridge these evidentiary gaps.

The publication repeatedly uses language implying ownership or control of wallet addresses by a specific individual without disclosing the analytical basis for such attribution. There is no indication that probabilistic clustering models were applied, no disclosure of confidence thresholds, no evidence of reliance on recognized forensic analytics providers, and no demonstration of independent expert validation. Without these elements, any assertion of wallet ownership remains speculative.

The publication further relies on references to IP addresses and user-agent strings as supporting evidence of identity attribution. However, such technical indicators are inherently non-unique. IP addresses may represent shared infrastructure, data centers, VPN services, proxy routing

environments, or enterprise network gateways. User-agent strings reflect device and software configuration but can be replicated or modified. In digital forensic practice, such indicators may support investigative direction but cannot serve as primary identity confirmation.

Particular attention must be given to the publication's claims regarding alleged confirmations from cryptocurrency exchange or conversion service operators. The publication references alleged responses from such services linking transaction activity to specific emails, IP addresses, and personal identifiers. However, the publication provides no original correspondence, no verifiable communication headers, no legal basis for data disclosure, no confirmation from the service operators themselves, and no documentation allowing independent verification of authenticity. In the absence of such documentation, it is not possible to determine whether the data was genuinely obtained from the referenced services, whether it was modified, or whether it corresponds to the transactions described.

Even if transaction confirmation from a service were hypothetically verified, such confirmation would not automatically establish the identity of the transaction initiator. Modern financial and cryptocurrency infrastructure frequently involves intermediaries, OTC liquidity brokers, payment processors, and third-party service providers executing transactions on behalf of clients. Without verified KYC documentation demonstrating direct operational control by a specific individual, attribution remains unproven.

The publication also references hosting infrastructure data and alleged account registration data associated with a hosting provider. Even assuming such registration data were authentic, account registration does not establish operational use of the infrastructure for specific transactions, nor does it establish exclusive control. Infrastructure accounts may be accessed by multiple users, delegated administrators, contractors, or unauthorized actors.

A recurring methodological flaw within the publication is the transformation of technical coincidence into categorical attribution. The publication asserts the existence of a "consolidation wallet" allegedly used for criminal financial flows without demonstrating verification of private key control, without demonstrating forensic tracing of fund origin, and without demonstrating transaction purpose analysis. In professional financial crime investigation, such conclusions require multi-layer confirmation, including technical, financial, and behavioral evidence.

Accordingly, the cryptocurrency-focused section of the publication reflects a common OSINT misinterpretation pattern: observable transaction visibility is treated as equivalent to identity verification and operational control attribution. Public blockchain transparency confirms transaction occurrence, but it does not confirm the identity of actors controlling the involved addresses.

In the absence of forensic attribution procedures, independent expert review, and documented regulatory or institutional confirmation, the cryptocurrency analysis presented in the publication must be considered technical observation interpreted through an accusatory narrative framework rather than verified forensic evidence. Reliance on such interpretation for legal or compliance decision-making creates a substantial risk of misattribution and disproportionate institutional response.

PART 5. Behavioral Narrative Construction, Lifestyle-Based Inferences, Alias Pattern Speculation, and Substitution of Evidentiary Analysis with Narrative Framing

The final section of the reviewed publication demonstrates a noticeable shift from technical or pseudo-technical analysis toward narrative-driven characterization of Dmitrii Artiukhov as an individual. At this stage, the publication moves beyond even correlation-based technical claims and instead relies on a mixture of biographical references, behavioral assumptions, lifestyle commentary, and stylistic pattern speculation, which are collectively used to support the publication's overarching accusatory narrative.

The publication attempts to draw conclusions from alleged similarities between online aliases used across different periods and alleged similarities to aliases used by other individuals referenced within the narrative. From a digital forensic perspective, alias pattern comparison can only be treated as a supplementary indicator requiring strong independent corroboration. The use of similar wording, thematic references, or stylistic patterns does not constitute identity confirmation. Such overlaps may arise randomly, through imitation, or through deliberate attempts at impersonation. The publication does not demonstrate the use of linguistic forensic methodology, authorship attribution analysis, or probabilistic linguistic modeling that would be required to treat such comparisons as evidentiary rather than speculative.

The publication further introduces psychological and motivational characterizations, including statements implying personal financial motivation or behavioral predisposition toward high-risk financial activity. Such statements are not supported by verifiable data, are not based on expert psychological analysis, and fall entirely outside the evidentiary scope of any professional investigation. They function purely as narrative reinforcement rather than fact-based analytical conclusions.

The biographical elements presented within the publication are also framed within a predetermined accusatory narrative rather than presented neutrally. References to education, employment history, participation in fintech or cryptocurrency projects, and involvement in international commercial structures are presented as implicitly suspicious. From an evidentiary standpoint, participation in fintech or digital asset sectors cannot be treated as an indicator of unlawful activity, as these sectors represent legitimate segments of the global economy characterized by high cross-border mobility and complex regulatory variation.

The publication additionally attempts to rely on lifestyle-based inference, including references to property ownership, vehicle purchases, international movement of assets, and changes in corporate ownership structures. Such elements are presented rhetorically rather than analytically. The existence of high-value assets or international asset mobility does not establish unlawful fund origin in the absence of financial forensic examination demonstrating income-expenditure mismatch or direct linkage to unlawful proceeds.

Particularly notable is the publication's attempt to infer causality between corporate restructuring decisions and alleged law enforcement or media activity. Corporate ownership changes may occur for a wide range of commercial, tax, investment, or organizational reasons. In the absence of documentary evidence demonstrating a causal relationship between such restructuring and enforcement action, any assertion of such linkage remains speculative.

The publication further relies on rhetorical questioning designed to create a presumption of guilt through narrative framing. Such rhetorical techniques are characteristic of opinion-based or advocacy publications and are not used within professional investigative or forensic reporting, where conclusions must be derived from verifiable and reproducible evidence.

Taken collectively, the final section of the publication demonstrates a transition from evidentiary analysis to narrative construction. Technical references, biographical elements, behavioral speculation, and lifestyle commentary are merged into a unified accusatory storyline without adherence to evidentiary verification standards. This narrative transition materially reduces the reliability of the conclusions and prevents the publication from being treated as a source suitable for legal, regulatory, or compliance reliance.

Accordingly, the publication's ultimate conclusions regarding alleged "obvious involvement" must be treated as opinion-based interpretations rather than findings supported by verified evidence meeting forensic, procedural, or regulatory standards.

PART 6. Overall Evidentiary Reliability Assessment and Applicability for Legal and Compliance Decision-Making

The cumulative review of the content, structure, source base, and analytical methodology of the publication demonstrates that the material represents a narrative construction primarily based on the interpretation of open digital traces, indirect correlation patterns, and unverified assertions regarding the origin of certain data sets, including information allegedly obtained from anonymous or non-verifiable sources. The publication does not demonstrate adherence to minimum evidentiary standards recognized within international criminal investigation practice, digital forensic examination, corporate investigation frameworks, or financial compliance analytics.

The publication does not reference verified procedural documentation, does not reference court rulings, does not reference formal law enforcement notifications, does not reference regulatory enforcement actions, and does not reference internationally recognized sanction or restriction designations. Accordingly, the publication cannot be interpreted as reflecting an established legal status of Dmitrii Artiukhov, nor can it be treated as documentation of the outcome of any officially conducted investigation by competent authorities.

The analytical methodology employed within the publication demonstrates systematic conflation of fundamentally distinct categories of information, including public allegations, technical correlation indicators, and institutionally verified factual findings. Technical indicators such as digital identifier overlap, IP address intersections, blockchain transaction flows, and behavioral pattern assumptions are repeatedly interpreted as evidence of personal involvement. Such methodology is inconsistent with established evidentiary evaluation standards, particularly within modern digital environments where such indicators are probabilistic rather than identity-confirming.

The publication further demonstrates the absence of documented data acquisition provenance and evidentiary preservation procedures. The lack of disclosure regarding acquisition methodology, transfer conditions, original source documentation, data integrity verification

measures, and custody continuity prevents the material from being treated as evidentiary-grade data. Within regulatory or judicial contexts, data lacking such verification would typically not be considered reliable without independent forensic validation and procedural legalization.

The publication also demonstrates the presence of narrative pressure elements, including personalized rhetorical framing, emotionally charged language, and the use of rhetorical questioning techniques. The presence of such narrative devices is inconsistent with neutral investigative reporting and further reduces the material's reliability as a potential source of objective factual information.

Within international financial compliance practice, the existence of public accusatory publications may create secondary institutional exposure risk, specifically the risk that financial institutions may adopt restrictive measures based on unverified narrative sources. In this context, the publication may be considered relevant solely as a reputational risk signal requiring further verification, but not as a source of verified factual findings.

Based on the above, the publication cannot be considered a source sufficient to support conclusions regarding alleged involvement of Dmitrii Artiukhov in unlawful activity, nor can it serve as an independent basis for legal or compliance decision-making, including but not limited to financial restrictions, termination of business relationships, asset freezes, or formation of enforcement or investigative positions.

Overall Conclusion

The conducted review demonstrates that the publication represents a collection of unverified public allegations interpreted by its authors within an accusatory narrative framework without adherence to internationally recognized evidentiary verification standards.

The material relies on correlation-based interpretation of digital traces, unsupported claims regarding data origin, and subjective interpretation of behavioral and biographical elements. The publication does not contain evidence subjected to independent forensic validation, does not demonstrate procedural legalization of data, and does not confirm the existence of an established legal enforcement status in relation to Dmitrii Artiukhov.

Accordingly, the publication may be treated exclusively as an open-source informational narrative capable of generating reputational exposure but lacking the evidentiary characteristics required for use within legal, regulatory, or compliance decision-making processes.

Reliance on such publications as the basis for restrictive or enforcement-oriented institutional action creates material risk of misattribution, risk of failure to meet good-faith information assessment standards, and risk of disproportionate measures being applied to an individual whose factual connection to the alleged activities has not been established through recognized procedural or forensic mechanisms.