FROM CYBER RESILIENCE TO DIGITAL TRUST: SELF-SOVEREIGN IDENTITY AS AN INSTRUMENT OF CYBER DIPLOMACY BETWEEN ROMANIA AND THE REPUBLIC OF MOLDOVA

Andreea DINU, Alexandru GEORGESCU, Paul Cristian VASILE
National Institute for Research and Development in Informatics – ICI Bucharest, Romania
andreea.dinu@ici.ro, alexandru.georgescu@ici.ro, paul.vasile@ici.ro

Abstract: Hybrid threats on NATO's Eastern Flank increasingly target not only digital infrastructure but also trust in identities, institutions and information. This article examines how digital trust can strengthen cybersecurity cooperation and cyber diplomacy between Romania and the Republic of Moldova. While existing bilateral, regional and European mechanisms provide a strong institutional basis for cooperation, an operational gap remains in verifying identities, institutional roles, authorisations and digital communications across borders. Building on the RoDID project, the article proposes a Digital Trust Corridor based on Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), trusted issuer registries and secure peer-to-peer communication. It further introduces Verifiable Confidence-Building Measures (VCBMs) as technical mechanisms for translating politically established trust into verifiable digital interactions. The article argues that Self-Sovereign Identity (SSI) cannot solve geopolitical attribution, but can reduce uncertainty regarding legitimate actors, institutional authority and communication provenance, thereby complementing existing cyber-diplomacy instruments
Keywords: Self-Sovereign Identity (SSI); digital trust; cyber diplomacy; cyber resilience; Decentralized Identifiers (DIDs); Verifiable Credentials (VCs); hybrid threats; Romania; Republic of Moldova.

INTRODUCTION

The security environment on NATO's Eastern Flank has undergone a profound transformation in recent years. The distinction between conventional military threats and non-military forms of coercion has become increasingly blurred, as hostile actors combine cyber operations, information manipulation, AI-generated content, sabotage and pressure against critical infrastructure. The European Union identifies cyber-attacks, Foreign Information Manipulation and Interference (FIMI), sabotage and attacks on undersea infrastructure as interconnected elements of the contemporary hybrid threat landscape, while NATO similarly warns that hostile actors exploit the openness and digitalisation of Allied societies to undermine institutions, democratic processes and societal resilience.

These developments are particularly visible on NATO's Eastern Flank. A 2025 NATO Review analysis of the Romanian presidential election crisis described algorithm-driven social-media manipulation and cyber-enabled disinformation as manifestations of an evolving form of hybrid warfare capable of destabilising democratic processes without conventional military intervention. ENISA has likewise highlighted the growing convergence between cybersecurity and information manipulation, including the increasing relevance of AI-enabled disinformation and deepfakes.

The central proposition of this article is that contemporary hybrid warfare targets not only networks and infrastructure, but trust itself: trust in institutions, information, identities and communication channels. AI-generated content, synthetic identities, deepfakes and compromised accounts reduce the cost of making malicious content appear legitimate and illegitimate actors appear trustworthy. Consequently, an attacker does not necessarily need to compromise an entire government network if it can successfully impersonate an official, fabricate an apparently authentic document or undermine confidence in genuine institutional communications.

Trust therefore becomes both a strategic target and a cybersecurity asset. Conventional security mechanisms remain indispensable, but protecting systems alone is insufficient when participants cannot reliably establish who produced a message, whether the sender possesses the claimed authority, or whether information has been altered. Contemporary hybrid resilience increasingly requires mechanisms for establishing the authenticity, provenance and integrity of digital interactions.

This challenge also affects cooperation among Allies and partner states. Collective resilience depends on exchanging sensitive information rapidly across organisational and national boundaries while maintaining confidence in the identities, roles and authorisations of participating actors. The EU's evolving digital identity architecture reflects this broader shift toward trustworthy and interoperable cross-border identification. Similarly, initiatives such as the European Blockchain Services Infrastructure (EBSI) demonstrate how Verifiable Credentials, digital wallets and distributed trust mechanisms can make selected information independently verifiable.

From this perspective, cyber diplomacy can also be understood as a process through which states construct cross-border infrastructures of digital trust. Diplomatic agreements establish the political and legal basis for cooperation, while interoperable digital identities and verifiable credentials can make selected institutional claims cryptographically verifiable without requiring all participants to depend on a single central database. Cyber diplomacy thus acquires an infrastructural dimension: alongside coordinating responses to malicious cyber activity, it can contribute to common standards and governance frameworks defining who and what can be trusted in the digital domain.

Romania and the Republic of Moldova constitute a particularly relevant case for examining this relationship. Beyond their close political and institutional ties, both states are exposed to a similar hybrid threat environment involving cyber operations, disinformation and attempts to undermine institutional resilience. Many of these threats share a common characteristic: they exploit uncertainty regarding identity, authenticity and trust.

Against this background, this article examines how digital trust can become an operational component of cybersecurity cooperation and cyber diplomacy, using Romania and the Republic of Moldova as a case study. It first analyses the evolving hybrid threat environment and the existing bilateral and European frameworks for cyber cooperation, before identifying a persistent gap concerning the verification of identities, institutional roles and digital communications across organisational and national boundaries. Building on the technical concepts developed within the RoDID project, the article then explores how decentralized identifiers, Verifiable Credentials and secure peer-to-peer communication could support a cross-border Digital Trust Corridor between Romania and the Republic of Moldova. On

this basis, it introduces the concept of Verifiable Confidence-Building Measures (VCBMs) and discusses how interoperable digital trust infrastructures could complement traditional instruments of cyber diplomacy. Finally, the article considers the security, governance and interoperability limitations of such an approach and assesses its potential for broader regional cooperation on NATO's Eastern Flank.

Methodologically, the article adopts a qualitative conceptual and policy-analysis approach. It combines a review of institutional and policy documents concerning hybrid threats, cyber diplomacy and Romania–Republic of Moldova cybersecurity cooperation with an analysis of relevant technical literature on Self-Sovereign Identity, Decentralized Identifiers and Verifiable Credentials. The analysis is used to identify an operational trust gap in existing cooperation mechanisms and to assess how technical concepts developed within the RoDID project could address this gap. On this basis, the article develops the Digital Trust Corridor and Verifiable Confidence-Building Measures as conceptual proposals rather than as empirically validated operational systems.

ROMANIA AND MOLDOVA: FROM SHARED CYBER THREATS TO CYBER DIPLOMACY

Recent reports agree that Russian hybrid activity on the Eastern Flank has intensified significantly since 2025. An analysis by the International Institute for Counter-Terrorism and GLOBSEC, cited in the 2026 Munich Security Report, identified more than 150 suspected hybrid incidents across several EU and NATO member states during 2025. Separately, German authorities recorded 321 cases classified as sabotage and vandalism during the same period. The figures are not directly comparable, as they derive from different datasets and apply different definitions and incident-classification criteria.Most of these incidents were carried out through criminal networks recruited by Russian intelligence services in order to avoid direct state attribution, a pattern separately documented by Chatham House researchers examining accountability for Russia's cyber proxies (Eurasia Review, 2026; Chatham House, 2026). GLOBSEC documented more than 570 NATO air-interception missions in 2025, almost three times the number recorded in 2023, alongside the Zapad-2025 exercise, which involved more than 100,000 troops, significantly exceeding the officially announced figures, as part of a deliberate effort to intimidate and increase ambiguity between peace and conflict (GLOBSEC, 2026).

A pattern particularly relevant to Romania, as a Black Sea littoral state, can be observed in the Baltic Sea, where at least six suspected acts of sabotage and eleven confirmed cases of damage to submarine telecommunications and energy cables have been recorded since 2022. Most have been attributed to vessels belonging to the so-called Russian and Chinese "shadow fleets," prompting NATO to launch Operation Baltic Sentry to monitor critical underwater infrastructure (RealClearDefense, 2025; Bulletin of the Atomic Scientists, 2026). Although the Black Sea has so far not experienced similarly documented incidents of underwater sabotage—and has fewer potential targets—the exposure of regional cables and pipelines to comparable risks remains an issue that Romanian and Moldovan institutions should address proactively rather than merely reactively.

NATO responded institutionally to this intensification by establishing, in 2025, the position of Special Coordinator for Hybrid Threats, held by the Assistant Secretary General for Cyber and

Digital Transformation, serving as a single focal point for ensuring coherence in the Alliance's response (NATO, 2026). At the European Union level, the Council adopted new conclusions in March 2026 expanding the EU's capacity to counter hybrid threats and strengthening the hybrid toolbox originally established in 2022 (Council of the European Union, 2026).

The cyber dimension of hybrid warfare on the Eastern Flank has already moved beyond the traditional pattern of isolated attacks against government networks. Table 1 summarises the main categories of cyber threats currently documented in the region that are directly relevant to Romania–Republic of Moldova relations, followed by a discussion of the directions in which these threats are expected to evolve over the medium term.

Table 1. Current Cyber Threats on the Eastern Flank

Threat category	Vector / actor	Documented example	Relevance to Romania–Republic of Moldova
DDoS attacks against public institutions	Pro-Russian hacktivist groups such as Killnet	Attacks against approximately 80 Moldovan state IT systems, May–October 2022 (Cobaltstrike.net, 2022; CSIS, 2024)	Shared vulnerability of government institutions in both states
Hack-and-leak operations	Intelligence services and proxy networks	Publication of private conversations involving Moldovan officials through "Moldova Leaks," November 2022 (CSIS, 2024)	Erosion of public trust, subsequently amplified through disinformation campaigns
AI-generated synthetic content (deepfakes)	Disinformation actors affiliated with or close to Russian intelligence services	Deepfake video of President Maia Sandu, December 2023 (Balkan Insight, 2023)	Recurring risk to electoral processes and the credibility of public institutions
AI-assisted phishing and malware generated using language models	Criminal actors and state-sponsored groups	More than 80% of phishing campaigns identified at European level used some degree of AI assistance by early 2025 (ENISA, 2025)	Growing vector for compromising public officials in both Romania and the Republic of Moldova

A first medium-term risk vector concerns the convergence of artificial intelligence and quantum computing in cryptanalysis. The U.S. National Institute of Standards and Technology published the first post-quantum cryptography standards in August 2024, designed to withstand attacks by quantum computers capable of breaking encryption algorithms currently used for key exchange and digital signatures, such as RSA and ECDH (NIST, 2024). Although a functional quantum computer at the required scale is not yet commercially available, Western intelligence services have warned about a "harvest now, decrypt later" strategy, whereby encrypted data intercepted today is stored for future decryption once sufficient quantum-computing capabilities become available. For public institutions and critical-infrastructure operators in Romania and the Republic of Moldova, migration towards quantum-resistant algorithms, supported by research already funded through national cyber-range projects, represents a medium- and long-term priority.

A second vector concerns the growing dependence of public services on artificial intelligence systems used to coordinate utility networks, ranging from electricity distribution to the management of water and sewage systems. Recent cybersecurity industry analyses estimate that, by 2026, more than one-third of global energy and other utility infrastructure will have been exposed to reconnaissance and covert-access activities conducted by AI-assisted human

actors or by AI itself, increasing the risk of coordinated disruptions occurring simultaneously across multiple sectors (SC Media, 2026). A distinct risk, still at an early stage but relevant to the next decade, concerns road-traffic management systems that will coordinate increasing numbers of autonomous or semi-autonomous vehicles through vehicle-to-infrastructure communications. Compromising such systems, by falsifying signals transmitted to vehicles or manipulating traffic-coordination algorithms, could produce direct physical consequences, ranging from artificially induced congestion to deliberately caused accidents, a scenario increasingly discussed in automotive-security literature (Help Net Security, 2025).

Sustained Cyber Pressure on the Republic of Moldova

The Republic of Moldova has faced sustained hybrid pressure since the first year of the war in Ukraine. In May 2022, the pro-Russian hacktivist group Killnet launched DDoS attacks against Moldovan government websites, only days after a similar wave of attacks against Romanian institutions. In October of the same year, additional attacks targeted approximately 80 state information systems (Cobaltstrike.net, 2022; CSIS, 2024). In November 2022, a newly registered website known as "Moldova Leaks" published private Telegram conversations attributed to Moldovan officials. Although the Presidency described the material as fabricated, the episode illustrates the convergence between cyber intrusion and operations designed to undermine public trust (CSIS, 2024).

In December 2023, an AI-generated video circulated on Telegram and other platforms depicting President Maia Sandu making statements she had never made. The Presidency placed the incident within the context of the hybrid war being waged against the country. It formed part of a broader pattern of synthetic and manipulated content targeting Sandu that was separately documented by the Atlantic Council's Digital Forensic Research Lab (Balkan Insight, 2023; DFRLab, 2024).

On 20 October 2024, the Republic of Moldova simultaneously held its presidential election and a referendum on incorporating the objective of European Union membership into the Constitution. The referendum passed by a very narrow margin, with approximately 50.4% of the vote, effectively decided by votes from the Moldovan diaspora after preliminary domestic results had initially indicated that the proposal would be rejected (RFE/RL, 2024a).

In the run-up to the vote, Moldovan police documented the transfer of approximately USD 39 million into the bank accounts of tens of thousands of citizens through the sanctioned Russian bank Promsvyazbank and a network coordinated by associates of convicted oligarch Ilan Șor, who is currently in Russia (RFE/RL, 2024b; OCCRP, 2024). The European Commission and High Representative Josep Borrell publicly characterised these actions as unprecedented Russian interference intended to undermine the country's democratic institutions (EEAS, 2024). President Maia Sandu was re-elected in the second round on 3 November 2024 with approximately 55% of the vote.

The parliamentary elections of 28 September 2025 took place amid an even more intense campaign of foreign information manipulation. This time, however, the Republic of Moldova managed to limit the effects of interference through a combination of institutional measures. The Centre for Strategic Communication and Countering Disinformation, established by law in 2023 at President Sandu's initiative, actively employed both debunking and prebunking

approaches against Russian narratives. At the same time, the European Union activated its own cyber-diplomacy instruments, including rapid-response teams and the Hybrid Fusion Cell, to provide remote support for election security (Georgetown Journal of International Affairs, 2026).

The Centre was reorganised in June 2025 under the direct authority of the Presidency, an institutional change that generated debate regarding the balance between effectiveness and transparency safeguards (REST, 2025). The ability of Moldovan institutions to rapidly and publicly document these interference attempts—from financial schemes to AI-generated synthetic content—constitutes an exercise in institutional transparency from which regional partners can draw useful lessons.

Regional Cooperation Mechanisms

Table 2 summarises the main regional cooperation mechanisms relevant to the hybrid and cyber dimensions of the relationship between Romania and the Republic of Moldova, ranging from the bilateral level to the NATO level.

Table 2. Regional Cooperation Mechanisms between Romania and the Republic of Moldova

Mechanism	Level / Date	Scope
DNSC–STISC Cooperation Agreement	Bilateral, 23 November 2022	Exchange of information on cyber incidents, best practices and joint projects; the foundation of subsequent bilateral cooperation
Cybercor–TUM–DNSC Protocol	Bilateral, November 2025	Training, certification and joint activities in cybersecurity
Cyber Alliance for Regional Resilience	Trilateral (Romania–Republic of Moldova–Ukraine), February 2026	Threat intelligence sharing, AI-based defensive tools, training and critical infrastructure protection
Odesa Triangle (Foreign Ministers' Format)	Trilateral, since 2022, with successive meetings through 2026	Political coordination, energy, connectivity, countering disinformation and hybrid threats
Bucharest Nine (B9) and Nordic Countries	Regional, since 2015; expanded summit in Bucharest, May 2026	Coordination on defence and deterrence on the Eastern Flank; commitment to deepening relations with the Republic of Moldova
Euro-Atlantic Resilience Centre (E-ARC)	Bucharest, since 2021	Romanian centre of excellence providing resilience expertise, including to Black Sea states that are not members of the EU or NATO, such as the Republic of Moldova
EU–Republic of Moldova Security and Defence Partnership	EU–Republic of Moldova, 2023	The first partnership of its kind concluded by the EU; support for resilience
EU Partnership Mission in the Republic of Moldova (EUPM)	EU–Republic of Moldova, since 2023	Strengthening resilience against hybrid threats, including cybersecurity and FIMI
EU Hybrid Toolbox	EU, June 2022, expanded March 2026	Preventive, cooperative, stability, restrictive and support measures; integrates the FIMI Toolbox and the Cyber Diplomacy Toolbox
NATO Special Coordinator for Hybrid Threats	NATO, position established in 2025	High-level focal point for ensuring coherence in NATO's response to hybrid threats
European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)	Helsinki, since 2017; Romania a member since 2018	Strengthening civil-military resilience capabilities; the Republic of Moldova is not yet a participant

Direct cooperation between the two states in the cyber domain predates the trilateral framework presented in Table 2. An initial cooperation agreement between Romania's National Cyber

Security Directorate (DNSC) and the Republic of Moldova's Information Technology and Cyber Security Service (STISC) was signed on 23 November 2022, just over eight months after the beginning of the war in Ukraine. The agreement established a framework for exchanging information on cyber incidents, sharing best practices and developing joint projects (STISC, 2022).

As responsibilities in this field in the Republic of Moldova were transferred to the newly established Cybersecurity Agency, cooperation was reaffirmed through a DNSC–Cybersecurity Agency memorandum of understanding, signed in June 2024. (DNSC, 2024).

Three months later, in February 2026, this bilateral framework was expanded into a trilateral structure through the signing in Kyiv of the memorandum establishing the Cyber Alliance for Regional Resilience, together with Ukraine. The initiative covers cyber threat intelligence sharing, the joint development of AI-based defensive tools, and the protection of critical infrastructure, while remaining open to other states sharing the same democratic commitment (National Security and Defence Council of Ukraine, 2026; Radio România, 2026).

The Trilateral "Odesa Triangle" Format

Launched at ministerial level in 2022, the Romania–Republic of Moldova–Ukraine trilateral format, known as the "Odesa Triangle," has hosted successive meetings of the three countries' foreign ministers: in Bucharest in 2023, Chișinău in 2024, Chernivtsi in 2025, and Munich in February 2026. Through these successive meetings, the format has gradually consolidated into a coordination mechanism addressing security, energy and regional connectivity.

The foreign ministers have repeatedly emphasised the need for joint action to counter hybrid threats and disinformation, alongside continued support for the European integration paths of the Republic of Moldova and Ukraine (Ministry of Foreign Affairs of the Republic of Moldova, 2026).

European Union Instruments

At the European Union level, the Republic of Moldova benefits from the EU–Moldova Security and Defence Partnership, the first such partnership concluded by the EU with a third country, as well as from the European Union Partnership Mission in Moldova (EUPM). EUPM is a civilian mission headquartered in Chișinău with a distinctive mandate covering a broad spectrum of hybrid threats, including cybersecurity and the fight against Foreign Information Manipulation and Interference (FIMI). Its role is to strengthen Moldova's crisis-management structures and the resilience of its security sector by providing strategic advice, capacity-building support, and assistance in developing policies for the detection, attribution, and response to hybrid threats (EEAS, 2024).

At the horizontal level, the EU Hybrid Toolbox, adopted in 2022 and subsequently reinforced, brings together preventive, cooperative, stability-oriented, restrictive, and support measures. It operates alongside specialised instruments addressing Foreign Information Manipulation and Interference (FIMI) and the Cyber Diplomacy Toolbox, thereby enabling the EU to combine diplomatic, cyber, information, and restrictive measures when responding to hybrid campaigns. These mechanisms are complemented by instruments designed to strengthen preparedness and coordinated responses to hybrid incidents. Together, they provide a framework through

which the EU can support partners such as the Republic of Moldova while responding to cyberattacks, disinformation, interference with democratic processes, and other forms of hybrid activity (Council of the European Union, 2026).

Taken together, these mechanisms demonstrate that Romania and the Republic of Moldova do not lack institutional frameworks for cyber cooperation. The emerging challenge is how trust within these frameworks can be operationalised technically across organisational and national boundaries.

THE MISSING LAYER: DIGITAL IDENTITY AND INSTITUTIONAL TRUST

The previous section has shown that Romania and the Republic of Moldova already possess a substantial institutional framework for cybersecurity cooperation. Bilateral agreements, European Union instruments and emerging regional formats provide mechanisms for information exchange, capacity building, incident response and resilience. The remaining problem is therefore not simply the absence of cooperation mechanisms. It is the ability of actors operating through those mechanisms to establish, rapidly and reliably, that the identities, institutional roles, authorisations and communications on which cooperation depends are authentic.

This problem becomes particularly important in a hybrid-threat environment in which cyber operations are increasingly combined with information manipulation. Hack-and-leak operations, compromised accounts, impersonation, phishing and AI-generated content can all undermine confidence in the source of information without necessarily compromising the technical infrastructure through which that information is transmitted (CSIS, 2024; ENISA, 2025). A communication channel may remain available and encrypted while the identity or authority of one of its participants has been falsified. Conversely, authentic institutional communications may lose their operational value if recipients cannot distinguish them from convincing fabrications.

These incidents suggest that hybrid cyber operations increasingly target not only the availability or confidentiality of information systems, but also the credibility of identities, communications and institutional sources.

This creates two related but distinct attribution problems. The first is malicious attribution: identifying who conducted an attack. The second is positive attribution: reliably establishing whether an actor, institution or communication is legitimate. Distinction is important because the two problems require different instruments. Malicious attribution is fundamentally an intelligence, forensic, political and diplomatic problem. Technical indicators may contribute to attribution, but infrastructure can be routed through third countries, compromised systems may be used as proxies, criminal groups may act on behalf of state interests, and several actors may deliberately employ overlapping tools and tactics (Chatham House, 2026; CEPA, 2025). Digital identity technologies cannot eliminate this ambiguity.

Positive attribution concerns a narrower but operationally significant question. Before an institution shares a sensitive threat report, accepts an incident-response request or grants access to a collaborative platform, it must establish that the requesting actor is who they claim to be, belongs to the institution they claim to represent, possesses the appropriate role and

is currently authorised to perform the requested action. A practical example illustrates this operational gap. Assume that, during a cross-border cyber incident, a Romanian cybersecurity institution receives an urgent request for technical information from an individual claiming to represent a Moldovan incident-response authority. Existing bilateral agreements may establish that cooperation between the two institutions is legitimate, while encrypted communication may protect the transmission channel. However, the receiving institution must still determine whether the individual currently belongs to the claimed organisation, whether that person occupies the stated operational role, whether they are authorised to request the specific information, and whether that authorisation remains valid at the moment of the exchange. These verification steps may currently depend on separate accounts, manual confirmation, organisational directories or bilateral contacts. The operational gap addressed in this article therefore lies between institutional trust established through cooperation agreements and the ability to verify that trust rapidly and technically during a specific digital interaction.

SSI (Self-Sovereign Identity) cannot solve the first problem. It may, however, contribute significantly to the second. Traditional cybersecurity architectures assume that identity can be established reliably through institutional databases, accounts, certificates or centralized identity providers. SSI proposes an alternative model in which an entity can control its own identifiers and present cryptographically verifiable claims without depending on a single identity provider (Allen, 2016; Der, Jahnichen & Sürmeli, 2017). Compromised accounts, impersonation, phishing, hack-and-leak operations and AI-generated content create an environment in which establishing whether an actor, communication or credential is legitimate becomes a security problem.

This section therefore introduces the concept of verifiable institutional identity as a component of cyber resilience. Verifiable institutional identity extends the identity problem beyond the simple authentication of a natural person. In cross-border cybersecurity cooperation, what matters is frequently a combination of claims: that a person controls a particular digital identity; that the person is affiliated with a particular institution; that the institution is recognised by the participating trust framework; that the person currently occupies a specific operational role and that this role provides access to a defined category of information or permits a specific action. A decentralised identity architecture changes the logic of this process. Instead of asking every participating organisation to maintain a complete database of every trusted foreign participant, an institution can determine which organisations are authorised to issue particular credentials and then verify cryptographically the credentials presented by an actor. This model follows the broader SSI logic in which identity control, credential issuance and verification are separated among holders, issuers and verifiers (Der, Jahnichen& Sürmeli, 2017; Stokkink&Pouwelse, 2018).

Trust is therefore not removed from the system. It is made explicit, distributed and technically verifiable. The distinction is especially relevant to the Romania–Republic of Moldova relationship. Existing cooperation creates political and institutional trust. A digital identity layer could translate selected elements of that trust into machine-verifiable claims that can be evaluated during operational exchanges. The result would not be an anonymous or permissionless environment, but a federated trust architecture in which institutions retain their authority while relying on interoperable technical mechanisms for verifying identities and permissions.

In this sense, identity becomes cybersecurity control. Authentication answers the question of who controls a digital identity; credentials can establish what institutional attributes that identity possesses; authorisation policies determine what the authenticated actor is permitted to do; and cryptographic signatures establish the provenance and integrity of communications associated with that identity (W3C, 2021).

The transition from institutional trust to verifiable institutional trust provides the conceptual bridge between the cyber-diplomacy mechanisms discussed above and the technological architecture developed within the RoDID project.

FROM RODID TO A CROSS-BORDER DIGITAL TRUST ARCHITECTURE

The technological concepts developed within RoDID project (Resilient and Interoperable Communication Systems Based on Distributed Technologies and Self-Sovereign Digital Identity) provide a possible architecture for addressing this problem. The project was conceived around an interoperable ecosystem combining distributed technologies, self-sovereign identity, a secure communication protocol and a registry of issuers of verifiable credentials.

The relevant components are:

- decentralized identifiers (DIDs);
- self-sovereign identity;
- verifiable credentials;
- trusted issuer registries;
- secure peer-to-peer communication;
- distributed mechanisms for integrity and traceability.

The proposed approach should also be positioned in relation to the European Union's evolving digital identity framework. The European Digital Identity framework similarly promotes interoperable and verifiable digital identity mechanisms across organisational and national boundaries. The Digital Trust Corridor proposed here does not seek to replicate or replace that framework. Rather, it explores a specialised cybersecurity and cyber-diplomacy use case in which decentralised identifiers, Verifiable Credentials and trusted institutional issuers could support the verification of professional roles, operational authorisations and institutional provenance in cross-border cyber cooperation.

Instead of creating a common centralized identity database, participating institutions could recognize trusted credential issuers while actors retain control over their own digital credentials. This model separates trust in the credential from centralized control over identity.

The starting point is the Decentralized Identifier (DID). DIDs are identifiers designed to allow an entity to be identified independently of a conventional central identity provider. A DID can resolve to a DID document containing verification methods, public keys and service information required for cryptographic interaction (W3C, 2021).

Within the RoDID architecture, an identity is associated with cryptographic keys and a DID document containing the information required for authentication and secure interaction. The corresponding private key remains under the control of the identity holder or institutional agent, while the public information necessary for verification can be resolved through the appropriate DID method.

Control over an identity can consequently be demonstrated cryptographically rather than exclusively through authentication against a remote account database. This reflects the broader SSI principles of user control, portability and reduced dependence on central identity providers (Allen, 2016; Der, Jahnichen and Sürmeli, 2017).

This mechanism is particularly relevant to cross-border cooperation because authentication can be performed without requiring the Romanian and Moldovan institutions to merge their identity-management systems. Within the RoDID P2P (peer-to-peer) model, an actor demonstrates possession of the relevant private key by signing a cryptographic challenge, while the receiving party validates the signature using the public information associated with the DID.

A DID alone, however, proves control over an identifier; it does not necessarily prove institutional authority. This is where Verifiable Credentials (VCs) become central to architecture.

A trusted institution can issue a digitally signed credential containing claims about an identity. In a cybersecurity-cooperation context, those claims could establish, for example, that the holder is an employee of a national cybersecurity authority, belongs to a Computer Security Incident Response Team, is authorised to participate in a specific exercise, has a particular professional certification, or possesses clearance to access a defined category of operational information.

The receiving institution does not need direct access to the issuer's personnel database to evaluate the credential. It needs to verify the cryptographic proof, determine that the issuer is trusted for that type of credential and evaluate whether the claims satisfy its local access policy. Such separation between holder, issuer and verifier is fundamental to SSI and verifiable-credential architectures (Stokkink&Pouwelse, 2018).

This introduces a second component of architecture: the trusted issuer registry. RoDID explicitly envisages the development of a digital registry of issuers of verifiable credentials in order to automate identity verification and improve interoperability between public institutions

For bilateral or regional trust architecture, a trusted issuer registry could contain the identifiers and trust status of participating public institutions and other authorised organisations. Romania and the Republic of Moldova would not have to centralise the identities of all participating users. They would instead agree on the institutional issuers whose credentials are recognised and on the credential schemas and assurance requirements applicable to specific operational contexts. Architecture consequently separates three functions that are often combined in centralised identity systems: identity control, which remains with the holder; attestation, performed by an authorised credential issuer; and verification/authorisation, performed locally by the institution receiving a credential.

Secure communication constitutes the next layer. Peer-to-peer architecture allows direct communication between autonomous nodes while reducing dependence on a single central communication service. The RoDID P2P architecture combines this principle with DID-based authentication and cryptographically protected sessions.

After the participating identities are resolved, the parties can prove possession of their respective private keys, negotiate a common transport mechanism and establish an encrypted communication channel. Mutual authentication can therefore bind the secure session to the decentralised identities participating in it.

RoDID further proposes interoperability with DIDComm for the exchange of encrypted, signed and verifiable messages between decentralised identity agents. Transport-layer security can complement these mechanisms where appropriate; TLS 1.3 remains a standard mechanism for securing transport communications (Rescorla, 2018).

This matters because identity verification and secure communication should not be treated as separate processes. An encrypted channel protects the confidentiality of information, but its strategic value depends on knowing who is present at each end of the channel. Conversely, a verified identity is of limited value if subsequent communications can be intercepted or altered.

Binding authenticated decentralised identities to end-to-end encrypted communication therefore connects identity assurance directly to message confidentiality, integrity and provenance.

RoDID also provides a basis for contextual authorisation. Authentication can be supplemented with VCs containing attributes such as role, institutional affiliation or access rights. The receiving agent can then apply local policies requiring a particular credential, a recognised issuer or periodic re-authentication. A further component is traceability and auditability. Distributed ledgers can provide tamper-evident records and chronological traceability where those properties are necessary, although their suitability depends on the specific application rather than on decentralisation as an end in itself (NIST, 2018).

The RoDID model similarly permits sensitive operations, including identity creation or revocation, connection establishment, credential verification, message exchange and changes to access policies—to be represented in cryptographically protected audit records. This does not require sensitive operational data to be placed on a public blockchain. Sensitive data can remain off-chain and under institutional control. Distributed infrastructure is instead useful for establishing selected trust anchors, verifying integrity, maintaining issuer information or providing evidence that a particular state of information existed at a particular moment.

Finally, architecture is designed for interoperability rather than technological isolation. Compatibility with W3C DID specifications provides a common technical basis for resolution and verification across systems (W3C, 2021). The RoDID implementation extends this logic through support for W3C-compatible DIDs and Verifiable Credentials, DIDComm-based communication, multiple DID methods and interfaces with existing enterprise identity infrastructures. The technical contribution can therefore be summarised as a chain of verifiability:

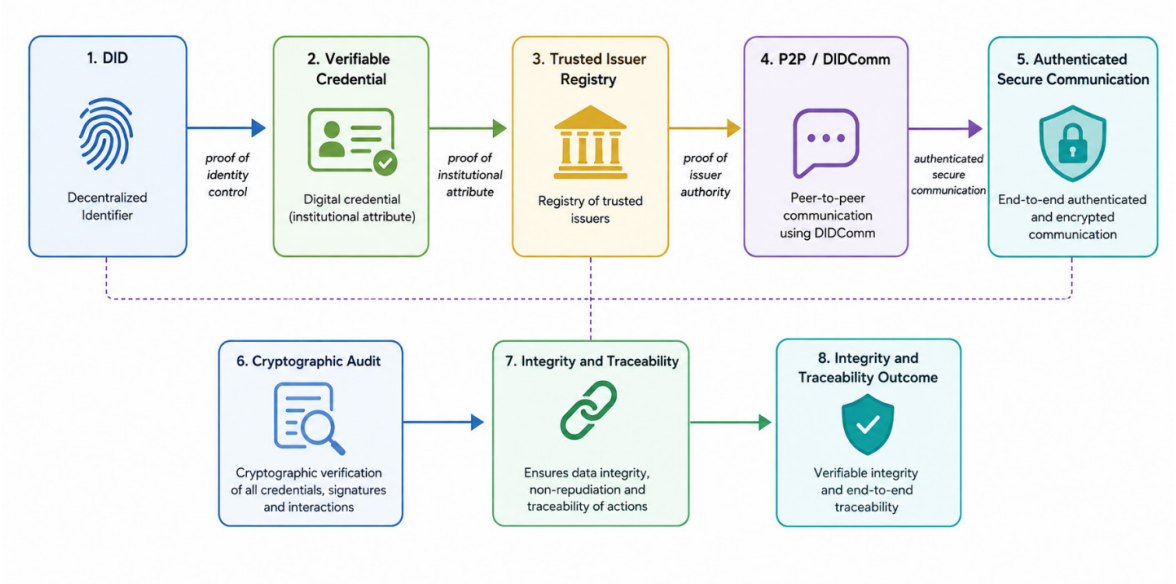


Figure 1. Chain of verifiability [own source]

Taken together, these components transform SSI from an individual identity-management concept into a possible architecture for institutional cooperation.

THE DIGITAL TRUST CORRIDOR

Existing policy analysis has already identified the need for a dedicated threat-information exchange channel between the Romanian and Moldovan cybersecurity authorities. This recommendation builds on an already established pattern of bilateral cybersecurity cooperation and information exchange between Romanian and Moldovan institutions (STISC, 2022).

Such a mechanism, however, immediately raises questions of identity, authorization and trust: who may participate in the exchange, which institution certifies that participant, what information may that actor access, and how can such authorization be revoked?

We describe the architecture addressing these questions as a Digital Trust Corridor. The term does not designate a new physical network or a replacement for existing bilateral cooperation. Rather, it describes a federated digital trust layer through which participating Romanian and Moldovan institutions could mutually recognise selected identities, credentials, institutional roles and authorisations.

At the governance level, participating institutions would define which organisations are authorised credential issuers, which credential types are recognised, what assurance levels are required for different categories of information and how credentials are suspended or revoked. At the technical level, DIDs, VCs, secure P2P communication and cryptographic verification would make those governance decisions operational.

Verified cybersecurity experts: DNSC or the Moldovan Cybersecurity Agency could issue verifiable credentials confirming that an individual belongs to an authorized incident-response team. The credential could contain only the attributes necessary for the operational context.

Data minimisation is consistent with the SSI principle that an identity interaction should reveal only those attributes necessary for the particular transaction (Allen, 2016). The receiving institution could verify both the credential and its issuer before granting access.

Trusted threat-intelligence exchange: Access to sensitive information could depend on cryptographically verifiable institutional credentials rather than conventional user accounts alone. A threat-intelligence platform could require, for example, a valid credential establishing that the holder belongs to an authorised national CERT or other recognised cybersecurity organisation. More sensitive collections could require additional credentials or attributes. The architecture would also allow authorisation to remain dynamic. If a person changes role, leaves an organisation or loses the required authorisation, the credential can expire or be revoked without requiring every partner organisation to manually update an independent user database.

Cross-border incident response: Members of joint response teams could authenticate themselves across institutional boundaries without requiring the creation of a common centralized identity database. The technical feasibility of this type of authentication is supported by the RoDID P2P model, in which identities can be mutually authenticated through DID resolution, cryptographic challenge-response mechanisms and additional Verifiable Credentials describing roles and permissions. The same mechanism could support time-limited emergency credentials. Access could be granted specifically for an incident, automatically expiring after a defined period, and restricted to selected systems or datasets.

Verified institutional communications: Official cybersecurity alerts, technical reports or requests for assistance could be cryptographically associated with trusted institutional identities. Digital signatures provide assurance regarding message integrity and the cryptographic identity controlling the signing key. They do not, by themselves, establish the substantive truth of the signed information (NIST, 2018). This creates an important distinction between content verification and source verification. SSI cannot determine whether every statement contained in an official report is correct. It can, however, provide evidence about the provenance of that report.

Cyber exercises and regional cooperation: The same trust infrastructure could support Romania–Moldova–Ukraine exercises and eventually other regional cooperation frameworks. The Cyber Alliance for Regional Resilience already establishes a trilateral setting involving Romania, the Republic of Moldova and Ukraine for threat intelligence, defensive technologies, training and critical-infrastructure protection (National Security and Defence Council of Ukraine, 2026; Radio România, 2026).

A trust corridor initially implemented bilaterally could therefore be extended through mutual recognition arrangements rather than redesigned as a completely new system. The Digital Trust Corridor should consequently be understood as a federation of trust decisions rather than a federation of databases. Political agreements determine the participating institutions and governance principles; trusted issuers attest institutional attributes; individuals and agents control their cryptographic identities; receiving organisations verify the credentials and retain sovereignty over access decisions. Such a model also allows gradual deployment. This approach corresponds closely to the RoDID development methodology, which progresses from identity and communication components towards vulnerability testing and ultimately a pilot scenario in the governmental domain. The corridor thus converts an existing policy

recommendation, a dedicated channel for cybersecurity cooperation, into a more specific technical question: how can trust inside that channel be established, verified and revoked across institutional and national boundaries?

SELF-SOVEREIGN IDENTITY AS CYBER DIPLOMACY INFRASTRUCTURE

Existing cyber diplomacy frameworks predominantly operate through political coordination, capacity building, diplomatic signalling, restrictive measures and incident response. At EU level, these functions are reflected in mechanisms such as the Cyber Diplomacy Toolbox and the broader Hybrid Toolbox, which combines diplomatic, cyber, information and restrictive instruments in responses to malicious and hybrid activity (Council of the European Union, 2026).

We propose complementing this policy layer with a technological layer of verifiable trust. This proposition expands the meaning of cyber diplomacy without replacing its established instruments. Diplomatic relations, international law, political commitments and institutional agreements remain the foundations on which states decide whether and how to cooperate. Technology cannot determine which states should trust each other or what political commitments they should undertake. It can, however, help operationalise specific consequences of those commitments.

The Romania–Republic of Moldova case illustrates this distinction. Bilateral agreements and European or regional frameworks establish that cooperation should take place. They identify institutions, define areas of common interest and create political expectations concerning assistance and information exchange. A digital trust infrastructure can make selected answers to the resulting operational questions independently verifiable. Cyber diplomacy therefore acquires an infrastructural dimension. The diplomatic agreement establishes the trust relationship at the political level; an interoperable identity framework can translate selected elements of that relationship into credentials, issuer policies and verification rules that information systems can evaluate automatically.

From Confidence-Building Measures to Verifiable Confidence-Building Measures

Cyber diplomacy is usually understood through norms, confidence-building measures, diplomatic coordination, attribution, sanctions and responses to malicious cyber activity. Traditional confidence-building measures reduce uncertainty between states through transparency, communication, contact points, information exchange, consultation mechanisms and cooperative activities. Their function is fundamentally political: they make behaviour more predictable and reduce the probability that ambiguity or misunderstanding will produce escalation. In increasingly digital forms of cooperation, however, part of that uncertainty is operational. Even where states have agreed to exchange information, the receiving system must determine whether a particular digital actor is authorised to participate in that exchange. This creates the possibility of what may be termed Verifiable Confidence-Building Measures (VCBMs). This logic is consistent with established international approaches to ICT confidence-building. Within the OSCE, cyber/ICT confidence-building measures have focused on transparency, national points of contact, information exchange, consultation and cooperation in order to reduce the risks of misunderstanding and escalation between participating States. Similar principles have been reflected in UN processes addressing responsible State behaviour in cyberspace, including the work of the UN Groups of Governmental Experts and the Open-

ended Working Group. These mechanisms primarily operate at the political and institutional level. The VCBM concept proposed in this article builds on this established logic by examining how selected elements of an agreed trust relationship could additionally be expressed and verified through interoperable digital identity mechanisms.

A VCBM would not replace a diplomatic confidence-building measure. It would provide a technical mechanism through which a politically agreed trust relationship can be verified during digital interaction.

The value of this approach is not that cryptography creates diplomatic trust. The value lies in reducing the gap between diplomatic agreement and operational execution. SSI does not replace diplomatic trust. Nor does it solve the geopolitical attribution problem associated with cyberattacks. Instead, it can reduce uncertainty regarding legitimate actors and communications within trusted international networks. Cyber diplomacy can therefore operate simultaneously at two levels:

- political trust, established through agreements, institutions and diplomatic relationships;
- verifiable digital trust, established through cryptographic credentials and interoperable identity infrastructures.

The combination of the two creates what can be described as programmable trust between institutions. The term "programmable" does not imply that diplomatic relationships can be reduced to software rules. It refers to the ability to express specific consequences of an institutional trust relationship as verifiable technical policies. This model may be particularly useful for relations between EU and NATO members and partner states. They frequently cooperate closely without sharing a single national identity infrastructure, personnel database or administrative system. A decentralised model allows interoperability without requiring institutional merger.

For Romania and the Republic of Moldova, a Digital Trust Corridor could serve as an experimental environment for this expanded conception of cyber diplomacy. A realistic first step would be a limited trust framework involving a small number of cybersecurity institutions, credential types and operational use cases, followed by testing in joint exercises and controlled threat-information exchanges.

LIMITS AND SECURITY RISKS

A digital trust infrastructure should not be confused with a cyber attribution mechanism. This limitation is particularly important in an environment in which state-sponsored operations may employ criminal groups, proxies and shared technical infrastructure, complicating attribution to a specific state actor (Chatham House, 2026; CEPA, 2025).

SSI can verify identity, credential, issuer, authorization and provenance of a signed communication. It cannot automatically demonstrate who executed an attack, who controls a proxy or who is geopolitically responsible for an operation.

Digital identity therefore reduces specific forms of uncertainty rather than eliminating the broader problem of trust. A diplomatic SSI infrastructure would itself create new governance and cybersecurity challenges. These include compromised wallets or cryptographic keys,

malicious or compromised credential issuers, revocation mechanisms, metadata leakage, interoperability problems and the governance of trust registries.

The first and most direct risk concerns private-key compromise. In a DID-based architecture, possession of the private key is central to proving control over an identity. If an attacker acquires that key, the attacker may generate cryptographically valid messages in the victim's name. The RoDID security analysis therefore identifies secure key storage, encrypted backups, hardware security mechanisms and key rotation as central defensive requirements.

A second problem is issuer compromise. Verifiable Credentials transfer part of the trust problem from the holder to the issuer. If a trusted institution's credential-issuing infrastructure is compromised, an attacker could potentially create credentials that are technically valid but institutionally fraudulent.

This makes revocation a central governance requirement. Institutional roles change frequently. Personnel leave organisations, responsibilities change, temporary incident teams are dissolved and devices or credentials may be compromised. A cross-border trust framework must therefore verify not only whether a credential was valid when issued but whether it remains valid when presented.

A further risk concerns metadata leakage. Encryption of message contents does not necessarily conceal communication patterns such as frequency, packet size or timing. The RoDID security analysis explicitly identifies correlation of metadata as a potential privacy risk in decentralised communication systems.

The architecture must also account for Sybil attacks. In distributed environments an attacker may create multiple identities in an attempt to manipulate trust, reputation or network behaviour. The RoDID security model identifies verifiable credentials issued by recognised authorities as one mechanism for assigning greater trust to institutionally validated identities than to anonymous or newly created identifiers.

Man-in-the-Middle and replay attacks remain relevant as well. Mutual authentication, digital signatures, nonces and timestamps are established mechanisms for limiting these attacks, while encryption standards such as TLS provide additional protection for communication channels (Rescorla, 2018).

Interoperability introduces another category of risk. Supporting multiple DID methods, credential schemas, cryptographic suites and legacy identity infrastructures increases flexibility but also increases complexity. Consequently, semantic and governance interoperability are as important as protocol interoperability.

The governance of the trusted issuer registry presents a particularly significant diplomatic question. Who decides which institutions may issue credentials? Can one state unilaterally revoke recognition of another issuer? How are disputes handled? What happens when an issuer is compromised during an ongoing incident? These questions demonstrate why decentralisation does not eliminate governance. It changes its object.

Blockchain should therefore not be treated as a universal solution. NIST similarly emphasises that blockchain architectures involve specific trade-offs and should be selected according to the requirements of the use case rather than treated as a universal replacement for conventional databases (NIST, 2018).

The critical innovation proposed here is therefore not the blockchain itself, but the trust architecture combining decentralized identifiers, verifiable credentials, secure communications and governance rules. The architecture must also remain compatible with the legal and regulatory frameworks applicable to participating institutions. The ability to technically verify or record information does not automatically establish a legal basis for processing or sharing it. Privacy, data protection, retention rules, institutional mandates and security-classification requirements must therefore form part of the trust framework.

Finally, the Digital Trust Corridor proposed in this article remains an architectural concept rather than an operationally validated bilateral infrastructure. RoDID demonstrates and documents technological components on which such a system could be constructed. A prudent implementation path would consequently begin with a limited pilot involving non-classified information, a restricted number of participating institutions and narrowly defined credential types. Cyber-range exercises could then test compromised credentials, malicious issuers, revocation failures, replay attacks, unavailable registries and interoperability failures before the architecture is considered for operational incident response.

These limitations do not weaken the relevance of SSI to cyber diplomacy. They define more precisely what it can contribute. SSI is not a mechanism for establishing geopolitical truth. It is a mechanism for making selected claims about legitimate actors, institutional authority and digital communications independently verifiable.

CONCLUSIONS

Contemporary hybrid threats increasingly exploit uncertainty regarding identities, information and institutional communications, making trust an operational component of cyber resilience. The Romania–Republic of Moldova case demonstrates that existing cooperation mechanisms provide a substantial political and institutional foundation, but that a technical layer is still needed to make selected identities, roles and authorisations verifiable across borders.

Building on RoDID, this article proposed a Digital Trust Corridor combining DIDs, Verifiable Credentials, trusted issuer registries and secure P2P communication. Rather than creating a common identity database, this architecture would enable participating institutions to recognise trusted issuers while retaining sovereignty over identities, data and access decisions.

The article also introduced Verifiable Confidence-Building Measures (VCBMs) as a bridge between cyber diplomacy and digital trust. Diplomatic agreements establish political trust, while interoperable identity infrastructures can make selected consequences of that trust technically verifiable. SSI therefore does not replace diplomacy or solve geopolitical attribution; it reduces uncertainty regarding legitimate actors, institutional authority and communication provenance.

The proposed Digital Trust Corridor remains an architectural concept and should initially be tested through limited bilateral pilots and cyber-range exercises. Ultimately, in a hybrid environment increasingly shaped by impersonation, synthetic content and contested authenticity, the ability to verify trust across institutional and national boundaries may become as important as the ability to protect digital infrastructure.

Acknowledgments

This work was supported by the RoDID project, "Resilient and Interoperable Communication Systems Based on Distributed Technologies and Self-Sovereign Digital Identity" (Project Code PN 23 38 01 01), under Contract No. 13N/2023, within the National Core Programme FUTURE TECH, carried out by the National Institute for Research and Development in Informatics – ICI Bucharest.

REFERENCE LIST

Allen, C. (2016) 'The path to self-sovereign identity'. Life With Alacrity. Available at: https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/ (Accessed: 17 August 2026).

Balkan Insight (2023) 'Moldova dismisses deepfake video targeting President Sandu'. Available at: https://balkaninsight.com/2023/12/29/moldova-dismisses-deepfake-video-targeting-president-sandu/ (Accessed: 17 August 2026).

Bulletin of the Atomic Scientists (2026) Seabed zero: Baltic sabotage and the global risks to undersea infrastructure. Available at: https://thebulletin.org/2026/02/seabed-zero-baltic-sabotage-and-the-global-risks-to-undersea-infrastructure/ (Accessed: 17 August 2026).

Center for European Policy Analysis (CEPA) (2025) 'The hybrid threat imperative: Deterring Russia before it is too late'. Available at: https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/ (Accessed: 17 August 2026).

Center for Strategic and International Studies (CSIS) (2024) 'Moldova's Sisyphean security struggle'. Available at: https://www.csis.org/analysis/moldovas-sisyphean-security-struggle (Accessed: 17 August 2026).

Chatham House (2026) Holding state-sponsored hackers and other cyber proxies to account. Available at: https://www.chathamhouse.org/2026/03/holding-state-sponsored-hackers-and-other-cyber-proxies-account (Accessed: 17 August 2026).

Cobaltstrike.net (2022) 'Moldova has accused the hacker group Killnet of attacking the government'. Available at: https://cobaltstrike.net/2022/05/03/moldova-has-accused-the-hacker-group-killnet-of-attacking-the-government/ (Accessed: 17 August 2026).

Council of the European Union (2026) 'Hybrid threats'. Available at: https://www.consilium.europa.eu/en/policies/hybrid-threats/ (Accessed: 17 August 2026).

Der, U., Jähnichen, S. and Sürmeli, J. (2017) 'Self-sovereign identity – Opportunities and challenges for the digital revolution'. *CoRR*, abs/1712.01767. Available at: https://arxiv.org/abs/1712.01767 (Accessed: 17 August 2026).

Digital Forensic Research Lab (DFRLab) (2024) 'US celebrities unwittingly recruited to undermine Moldova's president'. Available at: https://dfrlab.org/2024/02/15/us-celebrities-unwittingly-recruited-to-undermine-moldovas-president/ (Accessed: 17 August 2026).

European External Action Service (EEAS) (2024) 'Joint statement by the European Commission and High Representative Josep Borrell on the second round of presidential elections in Moldova'. Available at: https://www.eeas.europa.eu/delegations/moldova/joint-statement-european-commission-and-high-representative-josep-borrell-second-round-presidential_en (Accessed: 17 August 2026).

European Union Agency for Cybersecurity (ENISA) (2025) *ENISA Threat Landscape 2025*. Available at:https://www.enisa.europa.eu/sites/default/files/202601/ENISA%20Threat%20Landscape%202025_v1.2.pdf (Accessed: 17 August 2026).

Eurasia Review (2026) Hybrid Warfare 2026: Russian propaganda destroying Europe from within. Available at: https://www.eurasiareview.com/12032026-hybrid-warfare-2026-russian-propaganda-destroying-europe-from-within-analysis/ (Accessed: 17 August 2026).

Georgetown Journal of International Affairs (2026) 'How the EU rewrote its cyber diplomacy playbook in Moldova's 2025 elections'. Available at: https://gjia.georgetown.edu/science-technology/how-the-eu-rewrote-its-cyber-diplomacy-playbook-in-moldovas-2025-elections/ (Accessed: 17 August 2026).

GLOBSEC (2026) How Russia's hybrid warfare will escalate in 2026 and what Europe must do. Available at: https://www.globsec.org/what-we-do/commentaries/how-russias-hybrid-warfare-will-escalate-2026-and-what-europe-must-do (Accessed: 17 August 2026).

Help Net Security (2025) 'Connected cars drive into a cybersecurity crisis'. Available at: https://www.helpnetsecurity.com/2025/04/04/cybersecurity-risks-cars/ (Accessed: 17 August 2026).

Information Technology and Cyber Security Service (STISC) (2022) 'The Republic of Moldova and Romania strengthen their cooperation in the field of cybersecurity'. Available at: https://stisc.gov.md/ro/comunicate-de-presa/republica-moldova-si-romania-isi-consolideaza-cooperarea-domeniul-securitatii (Accessed: 17 August 2026).

NATO (2026) 'Countering hybrid threats'. Available at: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (Accessed: 17 August 2026).

National Cyber Security Directorate (DNSC) (2024) 'The National Cyber Security Directorate (DNSC) and the Cyber Security Agency (ASC) of the Republic of Moldova signed a Memorandum of Understanding'. Available at: https://www.dnsc.ro/citeste/directoratul-national-de-securitate-cibernetica-dnsc-si-agentia-de-securitate-cibernetic-asc-a-republicii-moldova-au-semnat-un-memorandum-de-intelegere (Accessed: 17 August 2026).

National Institute of Standards and Technology (NIST) (2024) 'NIST releases first 3 finalized post-quantum encryption standards'. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (Accessed: 17 August 2026).

National Security and Defense Council of Ukraine (2026) 'Ukraine strengthens its leadership in cybersecurity: NCCK forms regional cyber alliance with Romania and Moldova'. Available at: https://www.rnbo.gov.ua/en/Diialnist/7250.html (Accessed: 17 August 2026).

National Institute of Standards and Technology (NIST) (2018) *Blockchain Technology Overview*. NISTIR 8202. Available at: https://doi.org/10.6028/NIST.IR.8202 (Accessed: 17 August 2026).

Organized Crime and Corruption Reporting Project (OCCRP) (2024) 'A Russian non-profit interferes in Moldova's EU referendum and builds an anti-Western influence machine'. Available at: https://www.occrp.org/en/feature/a-russian-non-profit-interferes-in-moldovas-eu-referendum-and-builds-an-anti-western-influence-machine (Accessed: 17 August 2026).

Radio Free Europe/Radio Liberty (RFE/RL) (2024a) 'Results show Moldovans determined to continue on way to Europe, Sandu says'. Available at: https://www.rferl.org/a/moldova-vote-sandu-russia-meddling-european-union-passes/33165749.html (Accessed: 17 August 2026).

Radio Free Europe/Radio Liberty (RFE/RL) (2024b) 'Moldovan police accuse pro-Russian oligarch of $39M vote-buying scheme'. Available at: https://www.rferl.org/a/moldova-police-accuse-shor-russia-oligarch-39m-vote-buying/33172951.html (Accessed: 17 August 2026).

Radio Romania (2026) 'Romania, Ukraine and the Republic of Moldova launch the Cyber Alliance for Regional Resilience'. Available at: https://www.radioromania.ro/Actualitate/romania-ucraina-si-republica-moldova-lanseaza-alianta-cibernetica-pentru-rezilienta-regionala-id153620.html (Accessed: 17 August 2026).

RealClearDefense (2025) NATO's subsea cable strategy turns into a Catch-22. Available at: https://www.realcleardefense.com/articles/2025/10/24/natos_subsea_cable_strategy_turns_into_a_catch-22_1142966.html (Accessed: 17 August 2026).

Rescorla, E. (2018) *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. Internet Engineering Task Force (IETF). Available at: https://datatracker.ietf.org/doc/html/rfc8446 (Accessed: 17 August 2026).

REST (2025) 'Transparency or censorship? Moldova's battle against disinformation'. Available at: https://restmedia.st/transparency-or-censorship-moldovas-battle-against-disinformation/ (Accessed: 17 August 2026).

SC Media (2026) 'Critical infrastructure facing cyber surge in OT and supply chains in 2026'. Available at: https://www.scworld.com/feature/critical-infrastructure-facing-cyber-surge-in-ot-and-supply-chains-in-2026 (Accessed: 17 August 2026).

Stokkink, Q. and Pouwelse, J. (2018) 'Deployment of a blockchain-based self-sovereign identity', in *2018 IEEE International Conference on Blockchain*. 1st edn. IEEE, pp. 1336–1342. doi: 10.1109/Cybermatics_2018.2018.00230.

World Wide Web Consortium (W3C) (2021) *Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations*. Available at: https://www.w3.org/TR/did-core/ (Accessed: 17 August 2026).



Andreea DINU is a Researcher and Head of the Cybersecurity Unit at the National Institute for Research and Development in Informatics – ICI Bucharest. Her work focuses on cybersecurity, cyber diplomacy, critical infrastructure protection, cyber resilience, digital identity and emerging technologies. She is involved in European and international research and innovation projects addressing cyber ranges, cybersecurity training and exercises, trustworthy AI and the protection of critical infrastructures. Her activities also include international cooperation, capacity building and the development of scenario-based cybersecurity exercises, with particular interest in strengthening institutional resilience and cooperation between technical, policy and diplomatic stakeholders in the cyber domain.



Alexandru GEORGESCU is a Senior Researcher at the National Institute for Research and Development in Informatics – ICI Bucharest, with expertise in cybersecurity, critical infrastructure protection and resilience, and the security implications of emerging technologies. His research addresses complex risks affecting critical infrastructures and essential services, including cyber and hybrid threats, systemic resilience, and the interaction between technological developments, security policies and international cooperation. His work is particularly relevant to cyber diplomacy through its focus on strategic resilience, cross-border security challenges and the development of cooperative approaches to emerging cyber risks.



Paul Cristian VASILE is a Researcher at the National Institute for Research and Development in Informatics – ICI Bucharest, with professional and research interests in cybersecurity, cyber diplomacy, emerging technologies and international cooperation. His work contributes to research and innovation activities addressing the strategic and policy dimensions of cybersecurity, with particular attention to resilience, cooperation among relevant stakeholders and the evolving international cyber threat landscape. His interests include the role of technological innovation in security and the development of collaborative approaches to addressing cross-border cyber challenges.



This is an open access article distributed under the terms and conditions of the
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.