

From Ransomware and Leaks to Intelligence: Persistent Intelligence Exposure in the Russo-Ukrainian War

Csaba KRASZNAY¹

Introduction

Ransomware has evolved beyond its conventional characterization as a threat primarily affecting system availability and organizational finances. The widespread adoption of data exfiltration and double-extortion techniques has introduced an additional dimension of risk: information obtained during an intrusion may retain operational or intelligence value long after the immediate technical consequences of the incident have been mitigated. Compromised information can subsequently facilitate target identification, credential-based attacks, social engineering, organizational profiling, or broader strategic analysis. Accordingly, the consequences of ransomware incidents should not be assessed exclusively in terms of service disruption, financial loss, or the immediate confidentiality impact of unauthorized data disclosure.

Current cybersecurity guidance implicitly acknowledges this problem. The Cybersecurity and Infrastructure Security Agency (CISA), for example, recommends monitoring for compromised credentials exposed on criminal platforms, preventing the reuse of known compromised passwords, and rotating credentials following an incident.² Such measures recognize that exfiltrated information can enable subsequent malicious activity. Nevertheless, conventional incident-response frameworks remain predominantly oriented toward restoring the technical integrity of affected systems. Remediation typically focuses on activities such as credential rotation, patching, removal of malicious artefacts, restoration of compromised systems, and monitoring for indications of continued adversary presence. Although these measures are indispensable, they cannot invalidate information that has already been acquired by an adversary or subsequently disclosed to third parties. Once information concerning an organization's personnel, internal structures, technical environment, business relationships, or strategic priorities has been exposed, conventional remediation cannot fully reverse the resulting informational asymmetry.

The Russo-Ukrainian War provides a particularly relevant empirical context in which to examine this phenomenon. Since the beginning of the full-scale invasion in February 2022, cyber operations have constituted a persistent component of the broader conflict. More recently, campaigns attributed to actors associated with Russian military intelligence have targeted Western logistics and technology organizations involved in supporting Ukraine. Such operations have included credential guessing, spear-phishing, exploitation of organizational access mechanisms, and attempts to obtain information concerning logistical and technological support networks.³

¹ DEPARTMENT OF NETWORKED SYSTEMS AND SERVICES, FACULTY OF ELECTRICAL ENGINEERING AND INFORMATICS, BUDAPEST UNIVERSITY OF TECHNOLOGY AND ECONOMICS, BUDAPEST, HUNGARY, ORCID ID: [0000-0003-3216-2592](https://orcid.org/0000-0003-3216-2592), E-MAIL: KRASZNAY.CSABA@VIK.BME.HU

² CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY 2024

³ ENISA 2025

At the same time, the conflict has generated an unusually large volume of publicly accessible or publicly documented data originating from cyber intrusions. Russian governmental, regulatory, media, and commercial organizations have been affected by ransomware, hack-and-leak operations, and politically motivated intrusions. Collections associated with organizations such as Roskomnadzor, VGTRK, and Russian government ministries have subsequently appeared in public or semi-public repositories. In some cases, these collections comprise hundreds of thousands of files and substantial volumes of organizational data.⁴ The simultaneous presence of intensive intelligence requirements and extensive data exposure makes the Russo-Ukrainian War a particularly suitable environment for examining the potential transformation of cyber leaks into intelligence resources.

The analytical significance of these disclosures extends beyond the content of individual leaked documents. Intelligence value may emerge through the aggregation and contextualization of otherwise fragmented information. Personnel directories may reveal organizational responsibilities; procurement documents may indicate technological dependencies; correspondence may expose decision-making processes; technical documentation may identify infrastructure characteristics; and contractual information may reveal relationships among organizations, suppliers, and governmental institutions. When correlated with other publicly available information, such fragments can contribute to a more comprehensive understanding of an organization's capabilities, dependencies, vulnerabilities, and intentions.

This observation motivates the central research question of this study:

RQ: How can ransomware-related and other publicly documented cyber leaks associated with the Russo-Ukrainian War generate persistent intelligence exposure after the immediate technical consequences of the original incident have been mitigated?

The study advances the following hypothesis:

H1: Ransomware-related and other publicly documented cyber leaks associated with the Russo-Ukrainian War expose informational fragments that, when correlated with additional sources through mosaic-based intelligence analysis, can retain or acquire plausible intelligence utility beyond the original cybersecurity incident.

The article makes three contributions. First, it introduces the concept of Persistent Intelligence Exposure (PIE) to describe the enduring intelligence implications of information disclosed through cyber incidents. Second, it connects research on ransomware and data breaches with the intelligence literature on information aggregation and the mosaic effect. Third, it proposes an OSINT-based analytical approach through which persistent intelligence exposure can be examined without requiring the systematic acquisition or processing of complete stolen datasets. The latter is particularly important from methodological, legal, and ethical perspectives, as it enables the phenomenon to be studied through publicly documented metadata while minimizing unnecessary processing of compromised or potentially sensitive information.

⁴ SWEET 2024

Data Leaks and Mosaic-Based Intelligence Analysis

Research on ransomware has increasingly moved beyond the analysis of malware characteristics and incident response toward the systematic examination of ransomware ecosystems. One important development has been the treatment of ransomware leak sites as observable sources of empirical data rather than merely as channels of criminal communication and coercion. Müller and Yannikos, for example, analyzed more than 27,000 publicly documented leak-site entries associated with 325 ransomware groups. Their study demonstrates that leak-site publications can be interpreted as behavioural traces from which temporal routines, concentrations of activity, and targeting patterns can be derived.⁵

This methodological development has important implications for intelligence-oriented research. It suggests that the analytical value of cyber leaks does not necessarily depend on direct access to the underlying stolen datasets. Publicly observable metadata, including the identity and sector of the victim, the date of publication, the threat actor involved, descriptions of compromised information, and the organizational context of the incident, may themselves constitute a sufficiently structured empirical basis for identifying patterns of exposure. Consequently, research into the intelligence implications of ransomware can be conducted without reproducing the data-collection practices of the original attackers.

A second relevant strand of research and professional practice concerns the secondary exploitation of compromised information. Cybersecurity guidance already recognizes that information disclosed during one incident may facilitate subsequent malicious activity. Compromised credentials, for example, may be reused for unauthorized access, credential-stuffing attacks, lateral movement, or follow-on intrusions. CISA therefore emphasizes credential monitoring, password rotation, and measures designed to prevent the reuse of known compromised credentials. Similarly, CERT-EU has highlighted the possibility that publicly exposed exfiltrated information may subsequently support targeted phishing and social-engineering operations.⁶

These practices challenge an event-centric interpretation of data breaches. From an incident-response perspective, an intrusion may be considered contained once adversary access has been removed, affected systems have been restored, vulnerabilities have been remediated, and compromised credentials have been replaced. From an informational perspective, however, containment may be impossible. Information that has already been acquired cannot be technically revoked. Moreover, its relevance may persist independently of the technical conditions that enabled the original compromise. A leaked password may rapidly lose value following credential rotation, whereas information concerning organizational hierarchies, supplier relationships, internal processes, technological dependencies, or long-term procurement plans may remain useful for months or years.

This distinction becomes particularly significant when cyber leaks are considered through the conceptual lens of the mosaic effect. Within intelligence studies, the mosaic effect refers broadly to the possibility that individually unclassified, publicly available, or apparently innocuous pieces

⁵ MÜLLER, YANNIKOS 2026

⁶ CERT-EU 2026

of information may, when aggregated, reveal sensitive information or enable conclusions with national-security implications. The concept has long influenced intelligence and information-security practice, including decisions concerning the protection and disclosure of seemingly non-sensitive information.

However, the mosaic metaphor requires qualification. As Heuer argues in *Psychology of Intelligence Analysis*, intelligence analysis does not consist simply of assembling discrete pieces of information until a complete picture mechanically emerges. Analysts interpret information through existing hypotheses, conceptual models, contextual knowledge, and competing explanations. Consequently, the intelligence significance of leaked information is not determined solely by its volume. It depends on whether individual fragments can be contextualized and correlated with other sources in ways that reduce uncertainty concerning a target.⁷

This distinction is central to understanding the intelligence implications of ransomware and hack-and-leak operations. A leaked employee directory may have limited intelligence value in isolation. When combined with professional networking profiles, procurement records, organizational charts, technical documentation, and other open sources, however, it may enable analysts to identify key personnel, infer chains of responsibility, map organizational relationships, or select individuals for further collection or social-engineering activity. Similarly, supplier lists or contractual documents may acquire greater significance when correlated with shipping data, corporate registries, procurement announcements, or information concerning military and governmental programmes.

The Russo-Ukrainian War illustrates the relevance of this analytical mechanism. Western governments have repeatedly reported Russian intelligence interest in organizations involved in logistical, technological, and material support for Ukraine. The NCSC and partner agencies have identified cyber campaigns targeting logistics and technology organizations associated with Western assistance.⁸ Such targeting indicates an intelligence requirement concerning the networks through which support is organized and delivered.

At the same time, the conflict has produced large-scale disclosures affecting Russian governmental, regulatory, media, and commercial entities. Public reporting and repositories maintained by organizations such as Distributed Denial of Secrets have documented extensive collections of leaked information, including hundreds of thousands of files associated with Russian institutions.⁹ The significance of these collections is therefore not confined to their role as evidence of successful cyber operations or as instruments of political embarrassment. They may also constitute fragmented intelligence environments from which organizational structures, relationships, technological dependencies, administrative processes, and strategic priorities can potentially be reconstructed.

The relationship between cyber leaks and intelligence should therefore be understood as a process of information transformation rather than simple disclosure. The original cyber incident produces raw informational exposure. Subsequent aggregation, contextualization, and correlation may

⁷ HEUER 1999

⁸ NATIONAL CYBER SECURITY CENTRE 2025

⁹ FREEMAN 2023

transform that exposure into intelligence. The analytical problem is consequently not whether every leaked document possesses intelligence value, but under what conditions compromised information can contribute to intelligence production after the immediate cybersecurity incident has ended.

Persistent Intelligence Exposure

To capture this phenomenon, this article proposes the concept of Persistent Intelligence Exposure (PIE). PIE is defined here as a condition in which information exfiltrated during a cyber incident and subsequently disclosed or publicly documented retains—or acquires through combination with other sources—intelligence value after the immediate technical consequences of the original compromise have been mitigated.

The concept is intended to distinguish persistent intelligence consequences from conventional notions of data exposure and breach impact. Data exposure is generally addressed within cybersecurity, privacy, and incident-response frameworks and focuses primarily on unauthorized access to or disclosure of information. Breach-impact assessments similarly tend to emphasize direct consequences such as confidentiality loss, regulatory exposure, financial damage, operational disruption, or reputational harm. PIE instead focuses on the durability and secondary analytical utility of knowledge obtained through the breach.

This distinction is particularly important because different categories of compromised information exhibit different temporal characteristics. Credentials may have substantial immediate operational value but can often be invalidated through password resets, certificate revocation, or account rotation. Technical information may lose relevance following architectural changes, patching, or infrastructure replacement. By contrast, organizational relationships, supply-chain dependencies, institutional responsibilities, or strategic priorities may remain stable for considerably longer periods. The persistence of exposure should therefore be treated as a function of the information itself rather than of the duration of the technical compromise.

For analytical purposes, PIE can be operationalized across five dimensions: Human, Organisational, Relational, Technical, and Strategic. The Human dimension encompasses information concerning identifiable individuals, organizational roles, contact structures, professional responsibilities, and communication patterns. Such information may support target identification, social engineering, or organizational mapping.

The Organisational dimension concerns internal structures and processes, including organizational units, approval mechanisms, workflows, chains of command, and divisions of responsibility. These data can provide insight into how an organization functions and where decision-making authority is concentrated. Because organizational structures often change relatively slowly, this category may exhibit substantial persistence.

The Relational dimension captures information concerning external dependencies and interorganizational relationships, including suppliers, subcontractors, logistics providers, technology partners, and institutional counterparts. This dimension is particularly relevant in the context of defence and national security, where understanding supply chains and support networks may reveal dependencies that are not visible from the analysis of individual organizations alone.

The Technical dimension encompasses system descriptions, infrastructure components, configurations, access-control structures, software environments, and architectural information. Although some technical information may rapidly become obsolete following remediation, other elements – particularly those describing architectural dependencies or technology choices – may remain relevant over longer periods.

Finally, the Strategic dimension includes information concerning procurement, capability development, organizational priorities, planned investments, long-term projects, and future technological or operational developments. Such information may possess particularly durable intelligence value because it provides insight not only into an organization's current state but also into its intended future direction.

These dimensions provide a basis for an empirical coding framework. Rather than systematically downloading and analysing complete stolen datasets, a pilot study could rely on publicly accessible metadata and documented descriptions of incidents. For each case, the analysis could record the date of the incident, victim type, relationship to the Russo-Ukrainian conflict, publicly documented categories of compromised information, presence of the five PIE dimensions, and the estimated persistence of the exposed information.

An additional variable should capture what may be termed mosaic potential: the extent to which exposed information can plausibly be correlated with independent open sources to generate additional analytical value. This variable is conceptually distinct from the sensitivity of the leaked information itself. A seemingly low-sensitivity dataset may possess high mosaic potential if it provides identifiers, relationships, temporal information, or organizational references that can readily be integrated with other sources.

Such an approach has several methodological advantages. First, it permits the study of persistent intelligence exposure without requiring researchers to acquire large quantities of stolen information. This reduces legal and ethical risks associated with the processing of personal, proprietary, classified, or otherwise sensitive material. Second, metadata-based coding offers greater reproducibility than extensive qualitative interpretation of heterogeneous leaked datasets. Third, it enables systematic comparison across incidents and victim categories.

The approach also has important limitations. Public metadata provide only an indirect indication of the information contained in a leak, and descriptions published by threat actors may be incomplete, misleading, or strategically exaggerated. More importantly, the existence of intelligence potential does not demonstrate actual intelligence exploitation. In most cases, publicly available evidence will not permit researchers to determine whether a particular state intelligence service acquired, processed, or operationally employed information originating from a specific leak. The framework should therefore be understood as a means of assessing potential intelligence utility and persistence, rather than as a method for attributing actual intelligence use.

Despite this limitation, PIE has implications for post-breach risk assessment. Conventional remediation asks which systems were compromised, how access was obtained, what vulnerabilities must be addressed, and whether the adversary retains access. An intelligence-aware approach requires an additional question: what does the adversary potentially know as a consequence of the breach, and how can that knowledge be combined with information available elsewhere?

This question is particularly consequential in defence logistics, critical infrastructure, technology supply chains, and defence procurement. In these environments, organizational and relational information may itself constitute strategically relevant knowledge. Patching vulnerable systems and rotating credentials remain necessary components of incident response, but they cannot eliminate knowledge concerning organizational dependencies, key personnel, supplier relationships, internal processes, or long-term priorities once that information has been disclosed.

Persistent Intelligence Exposure therefore reframes the temporal boundaries of cyber incidents. From a technical perspective, an incident may end when adversary access has been eradicated and affected systems restored. From an intelligence perspective, however, the consequences may persist for as long as the information obtained during the incident remains relevant and can be integrated with other sources. Cybersecurity incidents involving data exfiltration should consequently be understood not only as temporary compromises of information systems, but also as potential sources of enduring informational advantage for actors capable of exploiting the resulting fragments.

Research Methodology

This study adopts a qualitative-comparative, OSINT-based research design to examine how publicly documented cyber leaks may generate Persistent Intelligence Exposure after the immediate technical phase of an incident has ended. The design preserves the article's central research question and hypothesis: RQ: How can ransomware-related and other publicly documented cyber leaks associated with the Russo-Ukrainian War generate persistent intelligence exposure after the immediate technical consequences of the original incident have been mitigated? H1: Ransomware-related and other publicly documented cyber leaks associated with the Russo-Ukrainian War expose informational fragments that, when correlated with additional sources through mosaic-based intelligence analysis, can retain or acquire plausible intelligence utility beyond the original cybersecurity incident. The Russo-Ukrainian War is an appropriate empirical frame because publicly available reporting shows both intensified Russian cyber operations against Ukraine and its allies and sustained intelligence interest in logistics, technology, transport, and defence-related support networks.

The temporal sampling frame runs from 1 January 2022 to 30 June 2026, thereby capturing the immediate pre-invasion escalation period as well as the full-scale Russo-Ukrainian War. The inclusion of the pre-invasion period is justified by cyber operations directly associated with Russian military preparations and troop movements preceding 24 February 2022. Within that period, cases are selected through purposive sampling rather than random sampling, because the objective is concept formation and mechanism identification rather than population inference. Incidents are eligible if they satisfy at least one of four relevance criteria: they affect Russian organisations; they affect Ukrainian organisations; they affect defence-related entities in countries that are involved in the conflict, including defence industry, procurement, logistics, and strategic technology; or they affect the broader Russian war-support or Ukraine-support ecosystems, including transport, ports, airports, IT services, supply-chain intermediaries, and public-sector organisations involved in assistance or coordination. This sampling logic is supported by public advisories documenting Russian interest in organisations connected to military aid delivery and by scholarship showing concentration and directionality in Russia-affiliated ransomware activity.

The project is intentionally staged. A pilot sample of 12 incidents is coded first in order to test whether the PIE framework can be applied consistently using only public documentation. The pilot stage is therefore not merely exploratory; it is a formal feasibility test for the operationalization of persistence, mosaic potential, and evidence reliability.

Inclusion requires that an incident be publicly documented through at least one of the following: an official advisory, a victim statement, a government or CERT report, a reputable threat-intelligence report, or a public release page describing the compromised dataset. Exclusion applies where the case is wholly undocumented beyond an uncorroborated leak-site boast; where no meaningful description of leaked material exists; where the case falls outside the time frame; or where there is no plausible relation to Russia, Ukraine, defence, or the support ecosystem defined above. The design expressly permits ransomware incidents, hack-and-leak operations, and other public cyber leaks to coexist in the corpus, because the article examines post-breach intelligence utility rather than malware taxonomy alone. That broader framing is analytically consistent with current official guidance, which increasingly treats data extortion, leak publication, and secondary exploitation as overlapping operational realities.

Each case was coded for the following variables: date, victim, country, sector, threat actor, leak type, conflict relevance, documented leak contents, PIE dimensions, estimated persistence, mosaic potential, evidence reliability, and sources (see Table A). The five PIE dimensions remain unchanged: Human, Organisational, Relational, Technical, and Strategic. Evidence reliability was coded on a three-level scale: verified when confirmed by an official advisory, victim statement, court filing, or equivalent primary source; documented when described in a credible secondary report with concrete supporting detail such as screenshots, file descriptions, or cross-source corroboration; and claimed when supported only by a threat-actor statement or leak-site assertion. This distinction is especially important because official and research reporting repeatedly note that public leak claims can be incomplete, selective, or strategically exaggerated.

The study is designed to minimise legal, ethical, and operational risk. It does not require downloading stolen archives, entering criminal marketplaces, purchasing leaked materials, or reproducing sensitive personal or defence-related content. Instead, it relies on public-domain descriptions, screenshots already circulating in the public sphere, official warnings, and reputable analyses. This is not only ethically preferable; it is methodologically defensible, since recent research demonstrates that leak-site posts and related public traces can support structured empirical analysis without direct possession of the underlying datasets.

Important limitations nevertheless remain. Public descriptions do not reveal the full contents of a leak, and the existence of intelligence potential does not prove actual intelligence exploitation. The framework therefore measures plausible intelligence utility, not confirmed use by a specific service. In addition, a case rich in screenshots may appear analytically denser than a case documented only through a short advisory. The method should therefore be read as a conservative, evidence-bounded approach to identifying persistent exposure rather than as a forensic reconstruction of every breach.

Table A: Coding table for PIE related incidents

Variable	Definition	Coding rule	Example
----------	------------	-------------	---------

Variable	Definition	Coding rule	Example
Date	Earliest public documentation of incident or leak	ISO date	2025-05-21
Victim	Named affected entity	Standardized official/public name	Roskomnadzor
Country	Jurisdiction of victim	ISO country name	Russia
Sector	Functional sector	One primary sector	Public administration
Threat actor	Attributed or claimed actor	Named group or “unknown”	Inc Ransom
Leak type	Mode of disclosure	Ransomware, hack-and-leak, extortion, mixed	Ransomware leak
Conflict relevance	Why the case fits the Russo-Ukrainian frame	Russia / Ukraine / defence / support ecosystem	Ukraine-support logistics
Documented leak contents	Publicly described data types	Short structured summary	Emails, contracts, screenshots
Human	Presence of person-level data	N / L / M / H	Staff names, mailboxes
Organisational	Structure/process information	N / L / M / H	Workflows, internal folders
Relational	External ties and dependencies	N / L / M / H	Suppliers, contractors
Technical	Systems/configurations/infrastructure	N / L / M / H	Databases, backups, architecture
Strategic	Plans, procurement, capability priorities	N / L / M / H	Defence development report
Estimated persistence	Expected duration of continuing value	Low / Medium / High	High
Mosaic potential	Ease of linking with OSINT or other leaks	1–5 ordinal scale	4-5

Variable	Definition	Coding rule	Example
Evidence reliability	Source confidence	Verified / Documented / Claimed	Documented
Sources	Traceable source base	Full citation set	Advisory + report + repository

Analysis of Publicly Documented Data Leaks

The completed pilot coding demonstrates that Persistent Intelligence Exposure is observable across a heterogeneous set of cyber incidents associated with the Russo-Ukrainian War. The twelve selected cases span public administration, military and defence organisations, telecommunications, energy infrastructure, transport, cybercrime, and strategic technology sectors. Although the sample is purposive and therefore does not support population-level inference, the coding reveals several consistent patterns. Organisational, Relational, and Strategic exposure are particularly prominent: Relational PIE was assessed as high in ten of the twelve cases, while Organisational and Strategic PIE were assessed as high in nine cases each. Technical PIE was also substantial, although its intensity varied more strongly according to the nature of the compromised material. Human PIE showed the greatest variation, ranging from limited exposure in predominantly technical datasets to extensive person-level information in leaks involving military personnel, internal communications, or personal documents.

The case comparison also demonstrates that the five PIE dimensions are analytically distinct but frequently overlap. Human PIE appears where leaked materials expose identifiable individuals, roles, contact structures, or communication patterns that can support profiling and target identification. Organisational PIE emerges from internal repositories, workflows, document structures, and chains of responsibility. Relational PIE is particularly pronounced where correspondence, procurement records, or financial documentation reveal suppliers, contractors, institutional counterparts, or other external dependencies. Technical PIE is strongest where leaked materials contain source code, system references, architecture, databases, credentials, or engineering documentation. Strategic PIE is visible where the compromised information concerns procurement, capability development, long-term projects, operational priorities, or future technological development. The cases therefore indicate that a single cyber leak may simultaneously expose several layers of organisational knowledge whose combined analytical value exceeds that of any individual document or data category.

Mosaic potential is similarly high across the pilot sample. Nine of the twelve incidents received the maximum score of 5, while the remaining three were assessed at 4. This reflects the extent to which leaked identifiers, organisational references, technical artefacts, supplier relationships, programme names, and other fragments can plausibly be correlated with independent open sources. Public procurement databases, corporate registries, sanctions lists, professional profiles, transport and infrastructure information, prior leaks, and other OSINT sources can provide the external context necessary to transform isolated fragments into more structured knowledge. The pilot therefore supports the proposition that intelligence value is generated not simply by the

sensitivity or volume of compromised information, but by its persistence, contextual richness, and capacity for correlation.

The cases further demonstrate that such intelligence potential is independent of the original attacker's motivation. The sample includes politically motivated hacktivists, insiders, unidentified sources, and financially motivated ransomware actors. In several cases, the original intrusion was evidently not conducted for intelligence purposes. Nevertheless, once information entered the public or semi-public information environment, it became potentially accessible to actors unrelated to the initial compromise. This distinction is particularly relevant in the context of the Russo-Ukrainian War, where official reporting has documented sustained intelligence interest in logistics, technology, defence procurement, critical infrastructure, and other support networks. The pilot findings therefore suggest that cyber leaks should be assessed not only as consequences of the original intrusion, but also as potentially persistent information resources whose intelligence utility may develop through subsequent aggregation, correlation, and reinterpretation. The case-level coding results are presented in Table B.

Table B: Pilot coding of 12 cybersecurity incidents

incident_id	incident_name	date	victim_name	country	sector	conflict_relevance	threat_actor_leak_type	source_links	documented_leak_contents	evidence_level
P01	Belarusian Railways disruption	2022-01-24	Belarusian Railways	Belarus	transport/rail	Russia-support ecosystem	Belarusian Cyber Partisans, ransomware	Reuters ¹⁰ ;	encrypted servers, DBs, workstations	documented
P02	Roskom-nadzor leak	2022-03-10	Roskom-nadzor – Republic of Bashkortostan office	Russia	Public administration / media and communications regulation	Russia – direct	Anonymous, Hack-and-leak	DDoSecrets Roskom-nadzor; ¹¹	360k+ files, emails, censorship data	documented
P03	Conti internal leaks	2022-02-28	Conti ransomware group	Russia	cybercrime, Ransomware-as-a-Service	Russia – direct	Pro-Ukraine Conti insider / member, insider, hack-and-leak	The Record; ¹²	internal chat logs, code, manuals	verified
P04	Russian soldier leak	2022-03-01	Russian military personnel dataset	Russia	military/defence	Russia – direct	Unknown / potentially pro-Ukrainian hacktivist or intelligence source, data leak, doxxing	Ukrainska Pravda; ¹³	names, DoB, addresses, unit, passport	documented
P05	Donetsk People's Republic emails	2023-05-15	Occupation administrations in Donetsk region	Ukraine (Russian occupied territory)	occupation administration	Ukraine – occupied territory / direct	KibOrg, hack-and-leak	DDoSecrets ¹⁴	1M+ emails and documents	documented
P06	GUOV i	2022-	GUOV i	Russia	defence	Russia –	Depaix	Security	15,600 emails	documented

¹⁰ BALMFORTH 2022

¹¹ DISTRIBUTED DENIAL OF SECRETS 2024A

¹² CIMPANU 2022

¹³ UKRAINSKA PRAVDA 2022

¹⁴ DISTRIBUTED DENIAL OF SECRETS 2024B

incident_id	incident_name	date	victim_name	country	sector	conflict_relevance	threat_actor_leak_type	source_links	documented_leak_contents	evidence_level
	GS leak	04-19	GS		construction	direct	Porteur, Anonymous, hack-and-leak	Affairs ¹⁵	about defence projects	
P07	Elvees leak	2024-01-17	Elvees	Russia	Microelectronics / semiconductors / defense and security technology	Russia – direct	Unknown / apparently pro-Ukrainian source, Hack-and-leak	DDoSecrets Elvees; ¹⁶	70,000 files, product and development docs	documented
P08	Gazregion leak	2022-04-18	LLC Specialized Construction Company Gazregion (SSK Gazregion)	Russia	gas pipeline construction	Russia – direct	Depaix Porteur; Network Battalion 65 (NB65); unidentified Anonymous-affiliated source, hack-and-leak	The Intercept ¹⁷	emails, files, decryption keys	documented
P09	Convex surveillance leak	2023-01-31	Convex	Russia	ISP/telecom	Russia – direct	CAXXII, hack-and-leak	Kyiv Post ¹⁸	120 GB, Green Atom monitoring program	documented
P10	Tetraedr leak	2022-02-26	Tetraedr	Belarus	defence manufacturer	Russia-support ecosystem	Anonymous Liberland & Pwn-Bär Hack Team, hack-and-leak	CyberNews ¹⁹	200+ GB of email weapon and radar profiles	documented
P11	Hungarian Defence Procurement Agency incident	2024-11-06	VBŰ / Defence Procurement Agency	Hungary	defence procurement	Ukraine-support ecosystem – indirect	INC Ransom, ransomware	Cyber Threat Report ²⁰	screenshots, procurement materials, later auction statement	documented
P12	Conpet / Qilin incident	2026-02-03	Conpet	Romania	energy pipeline operator	Ukraine-support ecosystem – indirect	Qilin, ransomware	The Record ²¹	sample documents, financial documents, passport scan statement	documented

incident_id	PIE_Human	PIE_Organisational	PIE_Relational	PIE_Technical	PIE_Strategic	mosaic_potential_score	persistence_estimate	notes
P01	L	M	M	H	M	4	M	Political ransomware-like hacktivism
P02	M	H	H	H	H	5	H	GRFC/Russian CensorFiles is a strong mosaic source
P03	H	H	H	H	H	5	H	occurred immediately after the declaration of war

¹⁵ PAGANINI 2022

¹⁶ DISTRIBUTED DENIAL OF SECRETS 2024C

¹⁷ LEE 2022

¹⁸ SMART 2023

¹⁹ BLACK 2022

²⁰ FRÉSZ, BÉRES 2024

²¹ ANTONIUK 2026

incident_id	PIE_Human	PIE_Organisational	PIE_Relational	PIE_Technical	PIE_Strategic	mosaic_potential_score	persistence_estimate	notes
P04	H	H	H	N	M	5	H	personal identification and unit connection can be permanently reused
P05	H	H	H	M	H	5	H	operational metadata of occupation administrations is strong
P06	M	H	H	M	H	5	H	defense investment and supply chain can be inferred
P07	L	M	H	H	H	5	H	high technical and capability value
P08	M	H	H	H	H	5	H	decryption keys are especially valuable
P09	H	H	H	H	H	5	H	state surveillance architecture can be reconstructed
P10	M	H	H	H	H	5	H	Belarusian defense manufacturer, Russian warfare ecosystem
P11	M	H	H	M	H	4	H	conflict-relationship partly inferential
P12	H	M	M	M	M	4	M	conflict-relationship partly inferential; exfil partly sample-doc.-supported

Legend for PIE and Persistence estimate:

N – No documented evidence: the public record does not substantiate the presence of this dimension.

L – Limited: isolated or incidental information relevant to the dimension.

M – Moderate: multiple documented elements permitting partial reconstruction or inference.

H – High: substantial documented information permitting systematic reconstruction, profiling, or analysis.

Legend for Mosaic Potential Score:

1 – Very low: little plausible correlation with independent OSINT

3 – Moderate: several identifiable correlation opportunities

5 – Very high: multiple identifiers, relationships or technical/organisational references readily linkable to independent sources

2 and 4 are intermediate values.

Dates refer to the earliest reliably identifiable public documentation of the incident or leak and do not necessarily represent the date of initial compromise.

The Hungarian Defence Procurement Agency Case

The alleged attack against the Hungarian Defence Procurement Agency (Védelmi Beszerzési Ügynökség – VBÜ) is well suited for use as a focused case study because the public reporting is unusually specific while still remaining bounded by ethical constraints. According to the publicly

available Cyber Threat Report by Ferenc Frész and Katalin Béres, the Inc Ransom group listed the victim on 6 November 2024 and published 46 screenshots as proof of access. Based on those screenshots, the authors identify at least four categories of potentially affected material: user “home” folders, databases and backups from the Andoc document-management system, sensitive financial documents and correspondence, and military documents, including a report linked to the Hungarian Defence Force Development Program 2022. The same report stresses that these are screenshots rather than original files and that authenticity therefore cannot be conclusively verified, even if the material appears consistent with a Hungarian-language internal IT environment.²²

Methodologically, this case is valuable precisely because it sits in the documented rather than verified category. It is also analytically important that the same report characterises Inc Ransom as a financially motivated actor and finds no evidence of state backing. That feature strengthens, rather than weakens, the PIE argument: if a financially motivated ransomware operation can place defence-relevant information fragments into public circulation, intelligence value may arise independently of the original attacker’s intent, as described in Table C.

Table C: PIE analysis of the VBÜ breach

Publicly documented artifact category	Indicative content	PIE dimension(s)	Mosaic potential	Qualitative relevance	intelligence
User home folders	Personal work files, naming conventions, role-linked folders	Human, Organisational	High	Supports mapping and inference	personnel and role
Andoc databases and backups	Document-management traces, archival structure, records logic	Organisational, Technical	High	Reveals workflow and information governance	internal and
Financial documents and mail	Budgets, invoices, correspondence, counterparties	Relational, Strategic, Human	High	Enables supplier and decision-chain reconstruction	and
Military-related documents	Programme status, planning or reporting references	Strategic, Organisational	Very high	Potential insight into capability development priorities	into development
File lists and folder structures shown in screenshots	Repository layout, naming practices, possible access paths	Organisational, Technical	Medium to High	Useful for institutional and system mapping	

On the five-dimension model, the case displays unusually broad coverage. The Human dimension is implicated by personal folders and correspondence. The Organisational dimension appears through internal repositories, document handling, and evidence of back-office workflow. The

²² FRÉSZ, BÉRES 2024

Relational dimension is potentially present in financial records and communications that may reveal contractors, suppliers, or institutional interlocutors. The Technical dimension is suggested by visible databases, backups, and system-specific references. The Strategic dimension is the most consequential, because the public description explicitly mentions military documentation and a defence development report.

The case does not permit a claim that a foreign intelligence service actually exploited the exposed material. What it does permit is a disciplined assessment of plausibility. A procurement agency sits at the intersection of organisational priorities, supplier relationships, budgeting, logistics, and capability development. Public procurement notices also identify the agency as a central purchasing body in the defence sector, which reinforces the inference that any exposure involving its internal correspondence, financial documents, or programme materials may have significance beyond ordinary reputational harm.

From a PIE perspective, the most important conclusion is temporal. Password resets, host isolation, or system restoration would not erase knowledge that may already have been derivable about programme names, counterparties, institutional dependencies, document flows, or responsible personnel. The case therefore illustrates why a post-breach assessment in national-security settings cannot stop at the question of whether systems were restored. It must also ask what durable picture of the organisation could now be assembled by correlating exposed fragments with public procurement data, company information, professional profiles, and other open sources. In that sense, the VBÜ incident provides a compact demonstration of the article's main claim: cyber leaks can create persistent intelligence exposure even when the original incident remains only partially observable and even when the initial attacker appears financially motivated rather than intelligence-driven.

Conclusions

This study has argued that the consequences of cyber incidents involving data exfiltration may extend considerably beyond the restoration of affected systems. The concept of Persistent Intelligence Exposure (PIE) captures this enduring dimension by focusing on information that retains, or acquires through correlation with other sources, intelligence value after the immediate technical consequences of an incident have been mitigated. The examined cases suggest that Human, Organisational, Relational, Technical, and Strategic information can persist beyond conventional incident-response timelines and, through mosaic-based analysis, contribute to a more comprehensive understanding of organisations, dependencies, capabilities, and priorities. Across the pilot sample, Organisational, Relational, and Strategic exposure emerged particularly consistently, while nine of the twelve cases exhibited very high mosaic potential.

The findings therefore support the central proposition of the study: the intelligence significance of a cyber leak cannot be assessed solely through the sensitivity of individual documents or the original motivation of the attacker. Information fragments released through ransomware, hack-and-leak operations, or other cyber incidents may acquire secondary value when combined with publicly available information. The Hungarian Defence Procurement Agency case illustrates this mechanism particularly clearly, demonstrating how even partially documented exposure may reveal organisational structures, supplier relationships, technical environments, and strategic priorities whose relevance may survive technical remediation.

Persistent Intelligence Exposure consequently suggests a broader temporal and analytical understanding of cyber incidents. In defence, critical infrastructure, and other national-security-sensitive environments, post-incident assessment should address not only whether adversary access has been removed, but also what durable knowledge may have entered the wider information environment. Future research should further validate the PIE framework across larger datasets and different geopolitical contexts, and examine how persistence and mosaic potential can be incorporated into systematic post-breach risk assessment.

Funding

This paper was supported by the Bolyai János Research Scholarship of the Hungarian Academy of Sciences.

References

- ANTONIUK, Daryna (2026): Romania's oil pipeline operator confirms cyberattack as hackers claim data theft. *The Record*, 6 February, 2026. Online: <https://therecord.media/romania-conpet-oil-pipeline-ransomware-attack>.
- BALMFORTH, Tom (2022): Belarusian group claims hack on railway system after Russian troop moves. *Reuters*, 24 January, 2022. Online: <https://www.reuters.com/legal/litigation/belarusian-group-claims-hack-railway-system-after-russian-troop-moves-2022-01-24/>
- BLACK, Damien (2022): Hero hackers claim to have breached Belarusian weapons firm. *Cybernews*, 26 February, 2022. Online: <https://cybernews.com/news/hero-hackers-claim-to-have-breached-belarusian-weapons-firm/>.
- CERT-EU (2026): European Commission cloud breach: a supply-chain compromise. 2 April, 2026. Online: <https://cert.europa.eu/blog/european-commission-cloud-breach-trivy-supply-chain>.
- CIMPANU, Catalin (2022): Conti ransomware gang chats leaked by pro-Ukraine member. *The Record*, 28 February, 2022. Online: <https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member>.
- CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (2024): #StopRansomware Guide | CISA. *#StopRansomware*, 2024. Online: <https://www.cisa.gov/stopransomware/ransomware-guide>.
- DISTRIBUTED DENIAL OF SECRETS (2024a): Roskomnadzor - Distributed Denial of Secrets. 23 January, 2024. Online: <https://ddosecrets.org/article/roskomnadzor>.
- DISTRIBUTED DENIAL OF SECRETS (2024b): Donetsk People's Republic emails - Distributed Denial of Secrets. 16 January, 2024. Online: <https://ddosecrets.org/article/donetsk-people-s-republic-emails>.
- DISTRIBUTED DENIAL OF SECRETS (2024c): Elvees - Distributed Denial of Secrets. 17 January, 2024. Online: <https://ddosecrets.org/article/elvees>.

ENISA (2025): *ENISA Threat Landscape 2025*. ENISA.

FREEMAN, Lindsay (2023): Seeing Through the Fog: The Impact of Information Operations on War Crimes Investigations in Ukraine., In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, IEEE, , pp. 365–379.

FRÉSZ, Ferenc – Katalin BÉRES (2024): Ransomware támadás érhet a Védelmi Beszerzési Ügynökséget. *CyberThreat Report*, 14 November, 2024. Online: <https://www.cyberthreat.report/p/ransomware-tamadas-erhet-a-vedelmi-beszerzesi-ugynokseget>.

HEUER, Richards J. (1999): *Psychology of intelligence analysis*. Center for the Study of Intelligence, Central Intelligence Agency.

LEE, Micah (2022): Russia Is Losing a War Against Hackers Stealing Huge Amounts of Data. *The Intercept*, 22 April, 2022. Online: <https://theintercept.com/2022/04/22/russia-hackers-leaked-data-ukraine-war/>.

MÜLLER, Lea – York YANNIKOS (2026): Analyzing Concentration, Temporal Routines and Targeting in Public Ransomware Leak Site Data. *arXiv preprint*. Online: <https://doi.org/10.48550/ARXIV.2605.24559>.

NATIONAL CYBER SECURITY CENTRE (2025): UK and allies expose Russian intelligence campaign targeting western logistics and technology organisations | National Cyber Security Centre. 21 May, 2025. Online: <https://www.ncsc.gov.uk/news/uk-partners-expose-russian-intelligence-campaign>.

PAGANINI, Pierluigi (2022): The Anonymous collective hacked other Russian organizations. *Security Affairs*, 20 April, 2022. Online: <https://securityaffairs.com/130409/hacktivism/anonymous-hacked-other-russian-organizations.html>.

SMART, Jason Jay (2023): Hacking Group Claims to Have Uncovered Massive Russian Domestic Spying Program. *Kyiv Post*. 31 January, 2023. Online: <https://www.kyivpost.com/post/11706>.

SWEET, Julia (2024): *Russian hackers and the war in Ukraine: digital threats and real-world consequences*. Lexington Books.

UKRAINSKA PRAVDA (2022): Personal data of 120,000 Russian servicemen fighting in Ukraine. *Ukrainska Pravda*, 1 March, 2022. Online: <https://www.pravda.com.ua/eng/news/2022/03/01/7327081/>.