

Information Security Governance in Fragmented Regulatory Environments Using RCA and RAITM Frameworks

Maksim Iavich^{*}, Vladimer Svanadze^{**}, Ketevan Grdzeldze^{**}

^{*} Academy Member, National Academy of Sciences of Georgia, Caucasus University, Tbilisi, Georgia

^{**} School of Technology, Caucasus University, Tbilisi, Georgia

Abstract. The fragmentation of internet governance, driven by diverging data protection laws, sovereignty claims, and conflicting regulatory requirements, has created a critical challenge for multinational organizations. Traditional information security frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework provide robust foundations for managing security controls, but they were not designed to navigate contradictions between jurisdictions or adapt to rapidly evolving legal environments. This paper addresses the gap between macro-level analyses of internet fragmentation and the organizational need for actionable governance. We introduce the Resilience-Compliance-Adaptability (RCA) strategic model, which reframes information security governance as a continuous capability encompassing the ability to withstand geopolitical disruptions, meet legal obligations across jurisdictions, and dynamically adjust to regulatory change. To operationalize this strategy, we propose the Regulatory Intelligence, Alignment, Implementation, Testing, Monitoring (RAITM) framework, a five-phase governance cycle that systematically translates legal requirements into security controls, assesses their effectiveness, and maintains alignment over time. © 2026 Bull. Georg. Natl. Acad. Sci.

Keywords: internet fragmentation, information security governance, mathematical model, RCA model, RAITM framework

Introduction

Over the past decade, the vision of a globally unified internet has become a complex reality. Jurisdictions increasingly assert their sovereignty through legislation that governs data flows, security practices, and technology infrastructure within their borders. For different organizations operating across multiple jurisdictions, the result is not merely a patchwork of rules but sometimes direct contradictions between them (Robbins, 2026).

This fragmentation creates particular difficulties for information security governance, as traditional frameworks like ISO27001/NIST CSF 2.0 were not built to address situations where compliance with one jurisdiction's requirements might put an organization at odds with another's. The frameworks assume a relatively stable regulatory environment, consequently the information security managers are forced to

manually analyze legal texts, from various jurisdictions, translate the compatibility of technical controls, verify the usability of control functions and repeat the process as regulations evolve.

In this paper, we offer the Resilience-Compliance-Adaptability (RCA) model as a governance basis as it that provides a strategic foundation, framing information security not only as technical protection but as organizational capacity needed to withstand legal and geopolitical disruption. Using Regulatory Intelligence, alignment, implementation, testing, monitoring (RAITM) offered framework translates this strategy into operational phases. Therefore, the papers offers a structured way to navigate fragmentation using all of these. In addition, we provide a modular description of a software architecture that automates key tasks. The architecture is designed to be used by both technical specialists who need to identify gaps and can be used by executives who require strategic visibility.

The RCA strategic governance model. The internet fragmentation creates novel challenges for organizations, and the existing information security frameworks offer incomplete solutions for them. Organizations face not just a large package of rules but genuine contradictions between jurisdictions and the need to adapt as regulations evolve (Iavich, et al., 2026). The Resilience-Compliance-Adaptability (RCA) model provides this strategic foundation. It does not only prescribe specific technical measures, but RCA articulates three interconnected governance capabilities that organizations must cultivate to operate effectively in fragmented regulatory environments (Baltra, et.al, 2026). These capabilities function as lenses using which organizations can assess their current posture, identify gaps, and guide investment decisions. The model does not replace existing standards such as ISO 27001 or NIST CSF 2.0 but it additionally orients them toward the particular demands of multi-jurisdictional operation.

Resilience. Resilience, in the context of the RCA model, is not only a traditional information security concern related to maintaining confidentiality, integrity, and availability during disruptive events. It includes the organization's capacity to withstand regulatory and geopolitical disruptions that originate outside its boundaries and over which it has little control. This conception of resilience is received from the literature on fragmentation as process and not as fixed state (Perarnaud, 2026). If fragmentation deepens, shifts, and evolves over time, organizations cannot rely on static arrangements. They must build systems and structures that absorb shocks and not shatter under them. Technical resilience means the design of infrastructure that can operate when connectivity to certain jurisdictions is compromised. Operational resilience means maintaining functions even during the legal interpretations change. Governance resilience means sustaining accountability and oversight when regulatory changes. For multinational organizations, resilience also requires the ability to sustain operations across jurisdictions that usually can have contradictory expectations. For this it is usually obligatory to segregate data flows, establish local entities, or adopt technical architectures that permit differential treatment of users based on location. The common thread is not avoidance but it is accommodation without abandonment of core principles.

Compliance. Compliance traditionally entails meeting legal obligations as they exist at a given point in time. The RCA model retains compliance as a core capability but reorients it toward the fragmented context. Therefore, for compliance we need to meet all legal obligations across every jurisdiction of operation, it demonstrates accountability to regulators and stakeholders, and provides traceability sufficient for audits and investigations. The fragmentation literature reveals why this is complicated. Jurisdictions adopt data localization requirements (Fidler, 2026), impose security standards on foreign providers (Ortiz Freuler, 2023), they restrict cross-border transfers that may conflict with obligations elsewhere (Perarnaud, 2022). Compliance in this environment is not only the process of checking boxes; it requires mapping obligations

across jurisdictions, identifying conflicts, and to make defensible decisions about how to proceed when full compliance with all requirements is impossible. The RCA model treats this interpretive work as central to the compliance capability.

Adaptability. Adaptability is the capability that responds most directly to the dynamic nature of fragmentation. Organizations must adjust their controls and practices, because regulations evolve, new jurisdictions assert sovereignty over digital spaces, and technical standards shift. Adaptability means dynamic configuration of across jurisdictions, the ability to respond to regulatory change before it becomes violation, and continuous recalibration of governance as circumstances demand. The process-oriented view of fragmentation (Perarnaud, 2026) implies that adaptability cannot be an afterthought or a periodic exercise; rather it must be built into the fabric of information security governance. This requires mechanisms needed to detect regulatory change, analyze its implications for the organization, and implement adjustments without disrupting operations. It also requires organizational culture and structures that treat change as normal rather than exceptional. Adaptability also encompasses the capacity to configure controls differently across jurisdictions, this differential configuration must itself be governed.

Integration of the three capabilities. The RCA model does not treat resilience, compliance, and adaptability as separate silos. They function as an integrated whole; each support and constrains the others. Resilience without compliance risks continued operation through means that violate legal obligations, invites enforcement actions that ultimately undermine resilience. Compliance without adaptability locks the organization into practices that may become obsolete as regulations change. Adaptability without resilience produces constant churn, lacking the stability needed for effective governance. The triangle is not a hierarchy; no single capability dominates the others. Instead, organizations must cultivate all three in balance, recognizing that weakness in any dimension undermines the others. This structure also functions as a loop, with each capability feeding into the others in continuous rotation. Resilience provides stability that enables thoughtful adaptation. Adaptation produces new configurations that must be validated through compliance processes. Compliance documentation reveals areas where resilience may be insufficient. This cyclical dynamic moves the organization away from static compliance toward dynamic governance.

RCA as foundation for RAITM. The RCA model operates at the strategic level, articulating the capabilities required for effective governance without prescribing how to achieve them. This strategic orientation makes it compatible with multiple operational frameworks, including - but not limited to - the RAITM framework introduced in the following section. The relationship between RCA and RAITM mirrors the relationship between strategy and operations more broadly. RCA asks what must be achieved and RAITM asks how to achieve it. The operational framework translates strategic capabilities into phases of activity, each with specific objectives and outputs. This layered approach prevents the framework from becoming too abstract to guide action and too prescriptive to accommodate diverse organizational contexts.

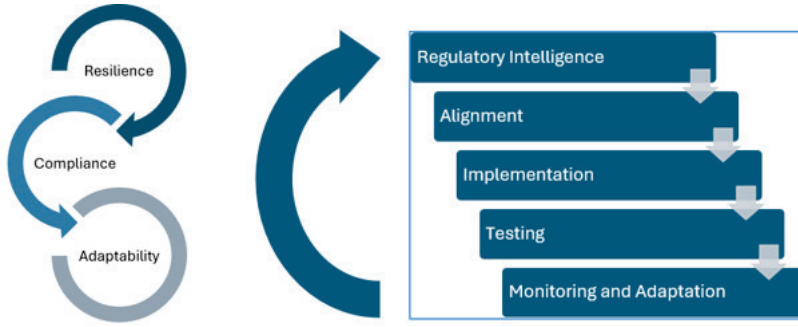


Fig. The RCA model as a loop for RAIM framework – a continuous governance loop for managing fragmentation across jurisdictions.

The RAIM operational framework. The RCA strategic model establishes what capabilities organizations need to navigate fragmented regulatory environments. The RAIM framework translates these strategic requirements into operational phases, providing a structured approach to implementation. The framework comprises five phases: Regulatory Intelligence, Alignment, Implementation, Testing, and Monitoring. Each phase produces specific outputs that feed into subsequent phases, creating a continuous governance cycle that can be represented mathematically to enable quantitative management.

Regulatory Intelligence (R). The Regulatory Intelligence phase addresses the detection component of adaptability identified in the RCA model. Organizations cannot comply with requirements they are unaware of, nor can they adapt to changes they fail to detect. This phase involves the systematic identification and analysis of applicable regulations across all operational jurisdictions.

For each jurisdiction j , the organization must identify the set of applicable regulations. We can define a regulatory applicability function as follows:

$$A_{ij} = f(\text{sector}_j, \text{data}_j, \text{presence}_j, \text{infrastructure}_j),$$

where $A_{ij} \in \{0,1\}$ indicates whether regulation i applies in jurisdiction j , based on factors including:

- sector_j : the industry sectors in which the organization operates in jurisdiction j
- data_j : the categories of data processed in jurisdiction j
- presence_j : the nature of the organization's legal presence in jurisdiction j
- infrastructure_j : the technical architecture deployed in jurisdiction j

The complete set of applicable regulations for jurisdiction j is:

$$\mathcal{R}_j = \{i \mid A_{ij} = 1\}.$$

Fragmentation risk emerges when regulations across jurisdictions impose conflicting requirements. We can define a conflict matrix:

$$\text{Conflict}_{j,k} = \{(i, l) \mid i \in \mathcal{R}_j, l \in \mathcal{R}_k, \text{incompatible}(i, l) = 1\},$$

where $\text{incompatible}(i, l)$ is a function that returns 1 if compliance with regulation i in jurisdiction j would prevent compliance with regulation l in jurisdiction k .

The overall fragmentation exposure for the organization can then be expressed as:

$$F_{\text{total}} = \sum_{j=1}^n \sum_{k=j+1}^n |\text{Conflict}_{j,k}|.$$

This provides a quantitative baseline against which we can measure progress. As the organization implements the RAIM framework, it should aim to reduce F_{total} . For this we must resolve conflicts through architectural segregation, legal entity restructuring, or other means.

The Regulatory Intelligence phase produces a Regulatory Knowledge Base that stores all applicable regulations, their requirements, and identified conflicts. This knowledge base serves as the foundation for subsequent phases.

Alignment (A). The Alignment phase converts legal obligations into governance requirements, security controls, and operational practices. This phase directly supports the compliance capability of the RCA model, for this it creates a structured mapping between what the law requires and what the organization does.

For each regulation i in jurisdiction j , we can identify a set of obligations:

$$\mathcal{O}_{ij} = \{o_1, o_2, \dots, o_m\}.$$

Each obligation o must be mapped to one or more security controls. We define a control set as:

$$\mathcal{C} = \{c_1, c_2, \dots, c_p\},$$

where controls may be drawn from existing frameworks such as ISO 27001 or NIST CSF 2.0, or may be organization-specific.

The mapping function M associates obligations with controls:

$$M: \mathcal{O}_{ij} \rightarrow \mathcal{P}(\mathcal{C}),$$

where $\mathcal{P}(\mathcal{C})$ denotes the power set of $\mathcal{C}$, representing that multiple controls may be required to satisfy a single obligation, and a single control may contribute to satisfying multiple obligations.

A significant challenge in fragmented environments is duplication of effort when similar obligations appear across multiple jurisdictions. We can define an obligation similarity metric:

$$\text{sim}(o_a, o_b) = \frac{|\text{features}(o_a) \cap \text{features}(o_b)|}{|\text{features}(o_a) \cup \text{features}(o_b)|},$$

where $\text{features}(o)$ represents the set of distinctive characteristics of an obligation (data types affected, security objectives, technical requirements, etc.). When $\text{sim}(o_a, o_b)$ exceeds a threshold τ , the organization can treat the obligations as functionally equivalent and implement a single control set that satisfies both.

This enables deduplication, which we can quantify as:

$$\text{Deduplication} = 1 - \frac{|\text{unique_obligations}|}{|\text{total_obligations}|},$$

where $\text{unique_obligations}$ are obligations that cannot be grouped with others, and total_obligations is the raw count across all jurisdictions. Higher deduplication indicates greater efficiency in the compliance program. The output of the Alignment phase is a comprehensive obligation-to-control mapping that shows exactly how each legal requirement will be satisfied. This mapping becomes the specification for implementation.

Implementation (I). The Implementation phase deploys the policies, technical controls, and monitoring mechanisms identified during Alignment. This phase operationalizes the compliance capability and begins to build resilience through concrete technical and organizational measures.

For each control c identified in the mapping, the organization must achieve a target implementation state. We can define implementation progress as:

$$I_c(t) = \frac{\text{completed_components}_c(t)}{\text{total_components}_c},$$

where $\text{completed_components}_c(t)$ is the number of components of control c fully implemented by time t , and $\text{total_components}_c$ is the total number of components required for full implementation.

Overall implementation progress across all controls becomes:

$$I_{\text{total}}(t) = \frac{\sum_{c \in \mathcal{C}} w_c I_c(t)}{\sum_{c \in \mathcal{C}} w_c},$$

where w_c represents the importance weight of control c , which may be derived from the number or significance of obligations it satisfies.

The implementation phase also must address potential conflicts identified during Regulatory Intelligence. When obligations conflict, implementation cannot simply proceed as if all requirements were compatible. Instead, the organization must make implementation decisions that reflect a defensible resolution strategy. We can represent this as:

$$I_{\text{decision}}(c, j) = \begin{cases} 1 & \text{if control } c \text{ is implemented in jurisdiction } j \text{ as specified} \\ 0 & \text{if control } c \text{ is not implemented in jurisdiction } j \\ m & \text{if modified implementation is applied, where } m \in (0,1) \text{ represents degree of compliance} \end{cases}.$$

The implementation decisions must be documented along with their rationale, creating an audit trail that demonstrates the organization's good faith effort to comply despite conflicts.

Testing (T). The testing phase assesses the maturity of the information security system, develops internal audit functions, and appraises the effectiveness of implemented controls. This phase directly measures the compliance capability and provides input for adaptability by identifying gaps that require attention.

For each control c , we can define its effectiveness as:

$$E_c = \frac{\text{passed_tests}_c}{\text{total_tests}_c},$$

where passed_tests_c is the number of test cases that the control successfully satisfied, and total_tests_c is the total number of test cases designed to assess that control.

Testing should also assess whether the combination of controls collectively satisfies obligations. We can define obligation satisfaction as:

$$S_o = \begin{cases} 1 & \text{if } \forall c \in M(o), E_c \geq \theta_c, \\ 0 & \text{otherwise} \end{cases},$$

where θ_c is the minimum acceptable effectiveness threshold for control c . An obligation is fully satisfied only if all controls mapped to it meet their thresholds.

The overall compliance maturity can then be expressed as:

$$\text{Maturity} = \frac{\sum_{j=1}^n \sum_{i=1}^{m_j} \omega_{ij} S_{ij}}{\sum_{j=1}^n \sum_{i=1}^{m_j} \omega_{ij}},$$

where ω_{ij} are the same weights used in the RCA compliance calculation, to ensure consistency between operational testing and strategic measurement.

The g phase also evaluates the organization's internal audit capability. We can model audit effectiveness as:

$$\text{Audit_quality} = \text{coverage} * \text{accuracy} * \text{timeliness},$$

where:

- coverage is the proportion of controls and obligations subjected to audit
- accuracy is the rate at which audit findings correctly identify genuine issues
- timeliness reflects how quickly audits are conducted after implementation or significant change.

Monitoring (M). The Monitoring phase ensures continuous regulatory and control alignment over time. This phase directly implements the adaptability capability of the RCA model, it transforms compliance from a periodic assessment into a dynamic process. Monitoring detects changes in the external regulatory environment, tracks drift in control effectiveness, and triggers recalibration when needed.

Regulatory change detection can be modeled as a surveillance function over the Regulatory Knowledge Base. For each regulation i in jurisdiction j , we track changes over time:

$$\Delta \mathcal{R}_{ij}(t) = \mathcal{R}_{ij}(t) - \mathcal{R}_{ij}(t-1),$$

where $\mathcal{R}_{ij}(t)$ represents the regulatory requirements at time t , and the difference operator captures amendments, new interpretations, or entirely new regulations.

When a change is detected, the organization must assess its impact. Impact can be quantified as:

$$\text{Impact}_{ij} = |\{c \in \mathcal{C} \mid M(o_{ij}) \cap c \neq \emptyset\}|.$$

That is, the number of controls affected by the change to regulation i in jurisdiction j . More sophisticated impact assessments might weight controls by their criticality or by the severity of the regulatory change.

Control drift detection monitors whether implemented controls continue to function as intended. For each control c , we track its effectiveness over time:

$$\Delta E_c(t) = E_c(t) - E_c(t-1).$$

Negative drift indicates deterioration that may require intervention before compliance is compromised.

Sovereignty conflicts arise when new regulations in one jurisdiction directly contradict existing requirements in another. We can extend the earlier conflict function to detect emerging conflicts:

$$\begin{aligned} \text{New_conflicts}(t) &= \{(j, k) \mid \exists i \in \mathcal{R}_j(t), l \in \mathcal{R}_k(t) \text{ such that } \text{incompatible}(i, l) \\ &= 1 \text{ and } \text{incompatible}(i, l) = 0 \text{ at } t-1\}. \end{aligned}$$

Early detection of emerging conflicts gives the organization maximum time to develop resolution strategies.

The Monitoring phase feeds back into Regulatory Intelligence, completing the cycle. When changes are detected, the organization must reassess applicability, realign controls, implement adjustments, and retest effectiveness. This continuous loop is captured by:

$$\text{RAITM_cycle}(t) = R(t) \rightarrow A(t) \rightarrow I(t) \rightarrow T(t) \rightarrow M(t) \rightarrow R(t+1).$$

Integration with RCA metrics. The RAITM framework produces operational data that feeds directly into the RCA strategic metrics defined in Section 3. The relationship can be expressed as:

$$\text{RCA}_{\text{index}}(t) = f(\text{RAITM_outputs}(t)).$$

Conclusion

This paper addresses a growing challenge for multinational organizations, such as governing information security in an environment of regulatory fragmentation. As various jurisdictions increasingly claim about their digital sovereignty by divergent and sometimes conflicting regulations, traditional frameworks like ISO 27001 and NIST CSF 2.0 provide necessary but insufficient guidance. They help organizations build mature security programs but do not equip them to navigate contradictions between jurisdictions or adapt as regulations evolve.

The RCA model offers a strategic foundation for meeting this challenge. By articulating three interconnected capabilities, the model provides that must cultivate, thus a lens through which organizations can assess their current posture and guide investments. Resilience enables organizations to withstand regulatory and geopolitical disruptions. Compliance ensures they meet legal obligations across all jurisdictions. Adaptability enables them to adjust as the regulatory landscape shifts.

The regulatory intelligence, alignment, implementation, testing, monitoring (RAITM) framework translates this strategy into operational phases. Each phase produces specific outputs that feed into subsequent phases, they create a continuous governance cycle. Regulatory intelligence identifies applicable requirements and conflicts. Alignment maps obligations to controls. Implementation deploys the controls. Testing verifies effectiveness, and finally, monitoring detects changes and triggers recalibration.

To make this approach practical, the paper proposed a six-module software architecture that automates key framework tasks. The regulatory knowledge base stores structured regulatory information. The regulatory mapping engine determines applicability. The framework mapper translates obligations into controls. The gap assessment engine evaluates current state. The monitoring engine tracks changes over time. The governance dashboard communicates results to decision-makers.

A hypothetical use case illustrated how the framework and software can function in practice, it demonstrates benefits that include improved regulatory coverage, reduced duplication which is achieved with deduplication, early detection of changes, and enhanced visibility for leadership.

The paper contributes to research as it connects macro-level fragmentation analysis with organizational response, it provides mathematical formulations that enable quantitative assessment, and identifies directions for future empirical work. It contributes to practice as it offers a structured methodology for a problem that is often handled ad hoc, and it specifies software requirements that could guide tool development. It contributes to policy as it illustrates the compliance burden that fragmentation imposes and by suggesting avenues for regulatory cooperation.

The fragmentation of the internet does not show signs of reversing. Current developments suggest that digital sovereignty and regulatory divergence will continue to intensify. Organizations that learn to navigate this environment will be better positioned to operate globally, serve customers across borders, and withstand the disruptions that fragmentation inevitably brings. The RAITM framework offers one path toward that capability, it grounds the response to fragmentation in structured governance rather than reactive coping.

Acknowledgements

This research is funded by the Internet Corporation for Assigned Names and Numbers (ICANN) through the ICANN Grant Program. The views and opinions expressed in this research are those of the authors and do not reflect the official policy or position of ICANN.

კიბერუსაფრთხოება

ინფორმაციული უსაფრთხოების მართვა ფრაგმენტირებულ რეგულაციურ გარემოში RCA და RAITM ჩარჩოების გამოყენებით

მაქსიმ იავიჩი*, ვლადიმერ სვანაძე**, ქეთევან გრძელიძე**

* აკადემიის წევრი, საქართველოს მეცნიერებათა ეროვნული აკადემია, კავკასიის უნივერსიტეტი, თბილისი, საქართველო

** კავკასიის უნივერსიტეტი, ტექნოლოგიების სკოლა, თბილისი, საქართველო

ინტერნეტის მმართველობის ფრაგმენტაციამ, რომელიც გამოწვეულია მონაცემთა დაცვის განსხვავებული კანონებით, სუვერენტიტეტთან დაკავშირებული მოთხოვნებითა და ურთიერთშეთავსებელი რეგულაციური მოთხოვნებით, კრიტიკული გამოწვევა შეუქმნა ტრანსნაციონალურ ორგანიზაციებს. ინფორმაციული უსაფრთხოების ჩარჩოები, როგორცაა ISO/IEC 27001 და NIST-ის კიბერუსაფრთხოების ჩარჩო (CSF), ქმნიან მტკიცე საფუძველს უსაფრთხოების კონტროლის მექანიზმების სამართავად, თუმცა ისინი არ არის შექმნილი იურისდიქციებს შორის არსებული შეუთავსებლობების დაძლევის ან სწრაფად ცვალეზად სამართლებრივ გარემოსთან ადაპტაციის მიზნით. წინამდებარე ნაშრომში განხილულია ინტერნეტის ფრაგმენტაციის მაკრო-დონის ანალიზსა და ორგანიზაციულ დონეზე ქმედითი მმართველობის საჭიროებას შორის არსებული ნაპრალი. ჩვენ წარმოვადგენთ „მდგრადობის, შესაბამისობისა და ადაპტურობის (Resiliencia, Compliance and Adaptability – RCA) სტრატეგიულ მოდელს, რომელიც ინფორმაციული უსაფრთხოების მმართველობას განიხილავს, როგორც უწყვეტ შესაძლებლობას, რაც მოიცავს გეოპოლიტიკური რყევებისადმი მედეგობას, სხვადასხვა იურისდიქციაში სამართლებრივი ვალდებულებების შესრულებასა და მარეგულირებელ ცვლილებებთან დინამიკურ ადაპტაციას. ამ სტრატეგიის პრაქტიკული რეალიზაციისთვის, შემუშავდა RAITM ჩარჩო (რეგულაციური მონიტორინგი, შესაბამისობა, იმპლემენტაცია, ტესტირება და მონიტორინგი). ეს არის მართვის ხუთეტაპიანი ციკლი, რომელიც სისტემურად გარდაქმნის სამართლებრივ მოთხოვნებს უსაფრთხოების კონტროლის მექანიზმებად, აფასებს მათ ეფექტურობას და უზრუნველყოფს მათ მუდმივ შესაბამისობას მიმდინარე რეჟიმში.

REFERENCES

- Baltra, G., Saluja, T., Pradkin, Y., & Heidemann, J. (2026). Understanding partial reachability in the internet core. *1st New Ideas in Networked Systems (NINeS 2026). Open Access Series in Informatics (OASICS)*, 139, 4:1-4:32. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. <https://doi.org/10.4230/OASICS.NINeS.2026.4>
- Fidler, M. (2026). Internet fragmentation's outward turn. <https://dx.doi.org/10.2139/ssrn.6214278>
- Iavich, M., Svanadze, V., & Kovalchuk, O. (2026). A deterministic, rule-based framework for detecting anomalous IP packet fragmentation. *Future Internet*, 18(1), 19. <https://doi.org/10.3390/fi18010019>
- Ortiz Freuler, J. (2023). The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century. *Global Media and China*, 8(1), 6-23. <https://doi.org/10.1177/20594364221139729>
- Perarnaud, C. (2026). From internet to offnets: Exploring the hidden process of off-netisation. *First Monday*, 31(2). <https://doi.org/10.5210/fm.v31i2.13797>
- Perarnaud, C., Rossi, J., Musiani, F., & Castex, L. (2022). 'Splinternets': Addressing the renewed debate on internet fragmentation (Research Report). European parliament, Panel for the Future of Science and Technology (STOA), Available at: https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2025/06/The-Splinternets-Outward-Turn_JUNE-3.pdf
- Robbins, S. (2026). A Trade-off worth making: internet fragmentation and digital sovereignty. *Ethics and Information Technology* 28(1), Article 15. <https://doi.org/10.1007/s10676-026-09890-5>

Received March, 2026