Digital State Erasure: Data as Both a Target and a Vector of Political and Military Influence

Mari Ristolainen and Veikko Siukonen
Finnish Defence Research Agency, Riihimäki, Finland

mari.ristolainen@mil.fi
veikko.siukonen@mil.fi

Abstract: Modern states increasingly rely on digital infrastructures and critical data for continuity, governance, and societal resilience. As national functions become more and more digitalized, the accumulation of sensitive data increases data-related risks, including hostile interference and exploitation. This paper introduces the concept of digital state erasure as an analytical framework, defined as the deliberate destruction, manipulation, or strategic exploitation of a nation's critical data in ways that undermine its ability to govern, provide services, authenticate its population, or defend itself. Unlike conventional cyberattacks, digital state erasure targets datasets whose compromise can dissolve a state's operational capacity and institutional coherence. Drawing on critical data studies, this paper conceptualizes critical national data as three interlinked categories and demonstrates how disruptions in either the target or vector dimension can cascade across national systems. This paper further argues that control over critical data constitutes the foundation of state authority and continuity in cyberspace. Losing that control risks digitally erasing a state, even in the absence of conventional military conflict.

Keywords: Digital state erasure, Critical national data, Sovereignty in cyberspace, Resilience, National security

1. Introduction

Digital technologies have fundamentally reshaped how modern states function. Governance, public administration, welfare provision, infrastructure management, and national defence as examples of vital functions of the state are all increasingly dependent on digital platforms, automated decision-making systems, and large-scale data repositories. Population registries, taxation systems, electoral processes, healthcare services, and crisis response mechanisms are now inseparable from data-driven infrastructures.

This transformation has significantly altered the foundations of state power and vulnerability. Where state continuity was once anchored primarily in physical territory, institutions, and personnel, it now depends increasingly on the state's capacity to exercise effective control over its critical national data, in addition to ensuring its confidentiality, integrity and availability (the CIA triad). In this context, considerations of data veracity – relating to the reliability and accuracy of data used for analysis and decision-making – can be understood as closely linked to the integrity dimension (cf. Ardagna et al. 2021). As a result, disruptions to data confidentiality, integrity and availability can have consequences that extend well beyond technical inconvenience, affecting political legitimacy, social trust, and the state's ability to act. Critical national data should be defined and regarded as a strategic resource, since loss of control over such data would undermine state authority and continuity. Without reliable control over critical data, a state's ability to govern, provide services, and maintain institutional continuity may be fundamentally undermined, making data protection a core national security concern (Rossbach 2024). This paper examines whether a state's operational capacity and institutional coherence can be comprehensively undermined – or effectively erased – through an attack directed solely at its critical national data.

The growing strategic significance of data has been more and more recognized in both academic and policy discussions. Research on cyber power and data-driven security highlights how control over data infrastructures and datasets has become an important dimension of contemporary power and influence (e.g., Shandler & Gomez 2023). At the policy level, defence organizations have likewise emphasized the transition toward data-centric architectures in which data is treated as a strategic resource that enables decision-making, operational effectiveness, and institutional resilience (cf. U.S. Department of Defense 2020; Finnish Defence Forces 2025). These developments reflect the broader recognition that modern governmental and military systems are deeply dependent on the confidentiality, integrity and availability of digital data. However, much of this literature focuses primarily on data as an operational or technical resource supporting governance and military effectiveness. Less attention has been paid to how the systematic loss of control over critical national data could undermine the state's ability to function as a governing entity.

From a national security perspective, data must therefore be understood not merely as an operational resource but as a strategic asset. Data occupies a dual role. On the one hand, data constitutes a target: its confidentiality, integrity and availability can be compromised by destroying, corrupting, encrypting, or rendering inaccessible in

order to both undermine and disrupt core state functions. On the other hand, data functions as a vector of influence: through its manipulation, selective disclosure, or strategic withholding, adversaries can shape decision-making, undermine confidence, and create dependency without direct confrontation.

This paper examines how operations on critical national data can challenge state authority and continuity even in the absence of large-scale kinetic force. It introduces the concept of digital state erasure to describe a condition in which the compromise of essential datasets erodes a state's practical ability to govern, authenticate its population, provide services, or recover from crises. In this paper, state authority and continuity refer to the state's ability to exercise legitimate governance, maintain essential functions, and independently recover during crises. The central argument is that, under conditions of deep digital dependency, the loss of control over critical data can be strategically equivalent to the loss or occupation of physical territory.

2. Digital State Erasure as a Concept and a Strategic Dimension

Digital state erasure refers to a strategic process in which a state's operational capacity and institutional coherence are undermined through the deliberate targeting or exploitation of its critical data. The concept does not imply the formal disappearance of the state, but rather the erosion of its effective governmental agency: the state may continue to exist legally, yet lose the ability to function in practice.

This form of erosion differs from conventional cyber operations in both intent and effect. Traditional cyberattacks are typically motivated by extortion, espionage or sub-threshold coercion. Digital state erasure differs from these phenomena in that it focuses specifically on the strategic compromise of critical datasets, rather than infrastructure disruption alone. Digital state erasure, by contrast, targets foundational datasets that underpin governance, legitimacy, recovery and continuity. The objective is not temporary inconvenience but systemic destabilization. Thus, digital state erasure should be distinguished from conventional cyber operations, hybrid pressure, or isolated critical infrastructure disruptions. Not all cyber operations against government systems constitute digital state erasure, even when their immediate effects are severe. The concept applies specifically to operations and dependencies that directly undermine state authority, continuity, and recoverability through data.

Strategically, digital state erasure aligns with operations conducted below the conventional threshold of armed conflict and can be employed across the spectrum of peacetime competition, crisis, and the transition to conflict and war. Shaping activities may be undertaken during periods of peacetime competition and heightened crisis, while execution can support coercive escalation or pre-conflict activities short of open hostilities. It enables adversaries to impose significant costs, constrain policy choices, and undermine societal resilience without necessarily triggering immediate military escalation. As such, it integrates seamlessly into broader strategies of hybrid activities, where technical, legal, economic, informational, and political instruments are employed in a coordinated manner.

In this paper, digital state erasure is not conceptualized as a discrete event or a formally observable outcome, but as an analytical construct that captures the cumulative strategic effects of control over critical national data under conditions of deep digital dependency. It serves as an analytical instrument rather than a predictive model, highlighting how incremental disruptions, dependencies, and external control can undermine effective state governance over time. Although this paper develops a conceptual framework, real-world incidents such as large-scale ransomware attacks on government registries or the destruction of national data infrastructure during armed conflict illustrate the potential relevance of the problem.

3. What is Critical National Data?

Drawing on critical data studies, which conceptualize data as a socio-technical construct embedded in relations of power, governance, and control (Dalton et al. 2016; Iliadis & Russo 2016; Kitchin 2014), critical national data in this paper refers to datasets whose confidentiality, integrity and availability, and, most importantly, controllability are essential to the state's authority and societal functioning. This includes data that enables the identification of individuals, the operation of essential services, the exercise of jurisdiction, and the recovery of systems following disruption. Furthermore, in this paper, data is distinguished from information (cf. e.g., Zins 2007). Data refers to the underlying digital records, registries, and system-level inputs that enable state authority, governance, and operational control, whereas information denotes data that has been processed or interpreted to convey meaning. Crucially, while information primarily shapes perception, data structures the condition under which governance, influence, and coercion become possible.

Despite its importance, critical data is rarely treated as a coherent analytical category within national security research. While prior research has examined data governance, data sovereignty, and data-centric security architectures (e.g., Shandler & Gomez 2023; Rossbach 2024), these approaches typically focus on data protection, cyber resilience, or technological infrastructures. They rarely conceptualize critical national data specifically in terms of its role in maintaining state authority, continuity, and recoverability. Existing approaches tend to favour the protection of physical critical infrastructure sectors (e.g., energy, transport, ICT) and view cybersecurity primarily through a technical lens focused on networks and systems rather than on data as a strategic asset and source of vulnerability (cf. Weber et al. 2023; Mussington 2021). As a result, data is treated as a by-product of technical systems rather than as a strategic asset in its own right.

This conceptual gap has practical consequences. Without a clear understanding of which datasets are critical under all conditions, states struggle to prioritize protection, allocate responsibility, and assess risk. In practice, identifying such datasets requires mapping dependencies between administrative systems, legal authorities, and digital infrastructures. Data that is essential for sovereignty may be outsourced, replicated across jurisdictions, or placed under contractual arrangements that limit state control. The problem is compounded by the tendency to view data governance as an administrative or economic issue rather than a security concern. Decisions driven by efficiency, cost savings, or innovation can gradually shift control over critical data away from the state, creating dependencies that are difficult to reverse. In a crisis, these dependencies may translate into strategic vulnerability.

4. Data as a Target and a Vector of Influence

The confidentiality, integrity and availability of critical national data can be targeted through various technical means, ranging from various malware and denial-of-service operations to the manipulation of backups, access controls, and authentication systems (cf. e.g., ENISA 2025). However, non-technical mechanisms are equally important. These include legal jurisdiction, infrastructure dependency, contractual constraints, and geopolitical pressure exerted to service providers, all of which can imperceptibly affect the controllability of data.

As a vector of influence, data can be manipulated to distort situational awareness, undermine trust, and shape political outcomes. Data-driven political communication, micro-targeting and misinformation have demonstrated the capacity to influence electoral behaviour and public perception of democratic legitimacy (Bradshaw & Howard 2019; Dad & Khan 2023; Jungherr 2023; Mont'Alverne et al. 2024). Furthermore, reliance on external digital infrastructure – such as cloud-hosted electoral systems or outsourced data management – can create strategic dependencies that can be exploited indirectly without direct cyberattacks (Farell & Newman 2019; Kwet 2019).

In a recent case, a democratic state planned to migrate its core electoral data – including voter registries, candidate databases, and vote-counting systems – to a foreign-owned cloud service with data centres located outside national territory. This decision was justified primarily on cost-efficiency grounds, but it entailed a significant transfer of control over critical democratic infrastructure (Hakahuhta 2025). Nevertheless, hosting electoral systems in foreign cloud environments introduces structural risks. Access control is no longer exclusively national; data recovery during crises depends on external actors; and the data becomes subject to foreign legal regimes and extraterritorial legislation. Electoral data is foundational to democratic legitimacy, and its integrity and availability must be demonstrable beyond doubt. Importantly, undermining elections does not require vote manipulation. Creating uncertainty about the reliability of voter registries or result calculation may be sufficient to erode public trust. Foreign-hosted electoral infrastructure thus constitutes a strategic vulnerability: electoral data functions simultaneously as a target of disruption and as a vector of influence through which legitimacy, trust, and political stability can be challenged.

In another case, a state indicated the migration of highly sensitive health, welfare, and social security data to cloud services operated by multinational providers, with data potentially stored outside the state's legal jurisdiction. The precise location of the data was not publicly disclosed, and recovery capabilities depended on external infrastructure and contractual arrangements (Koponen 2025). This configuration creates vulnerabilities without requiring technical intrusion. Interface may occur through the compromise of data integrity, restricting availability, or exerting control through legal, regulatory, or geopolitical pressure on service providers. Even limited inconsistencies in medical or welfare records can produce systemic effects, rapidly undermining trust in public services. Disruption to data availability – whether intentional or incidental – translates directly into delayed healthcare, interrupted benefits, and weakened crisis response. If control over who can access critical national data and when systems can be restored shifts to external actors, the state's ability to effectively manage

its own welfare and health systems is significantly reduced. In such conditions, a state's capacity to exercise authority can be constrained without overt or attributable influence.

Consequently, the dual role of data as both target and vector mean that vulnerabilities are not confined to cybersecurity failures. What a state does not fully control can be transformed into leverage against it. In the following, the aim is to demonstrate how critical national data could be systematically categorized from a national security point of view and how each category functions both as an object of attack or larger set of operations and as a mechanism through which political and strategic influence could be exercised.

5. Three Categories of Critical National Data

Data classification is widely recognised as a systematic process for categorising data based on sensitivity, value, and potential impact in the event of compromise. For example, NIST (2023) defines data classification as the process of assigning labels to data sets in order to ensure confidentiality, integrity, and availability requirements. Common classification schemes organise data into public, internal, confidential, and higher sensitivity categories, enabling prioritised protection and governance of critical data assets. Such frameworks are foundational in both organisational and information security contexts, providing a basis for risk management and compliance (cf. e.g., ITU 2025).

This paper conceptualizes critical national data as three interlinked categories: 1) Identity and Authentication Data; 2) Operational and Functional Data; 3) Authority, Control, and Recovery Data. These categories are analytically distinct but mutually reinforcing, and disruption in one category can cascade across the others (cf. Shivayogi 2025; Nguyen, H–N. & Cuong 2025; Ofili et al. 2024). While analytically distinct, these three categories are not equal in strategic significance. Authority, control, and recovery data constitute the uppermost layer, as loss of control at this level constrains the state's ability to restore, validate, or govern the other two categories.

5.1 Identity and Authentication Data: Who the State Recognizes and Protects

The first category of critical national data consists of datasets that identify and authenticate individuals, organizations, and other legal entities. These include population registries, citizenship and residency records, personal identity numbers, tax identifiers, company registries, land ownership records, and other administrative datasets that establish legal personality and status. Together, they define who belongs to the political community, who is entitled to protection and services, and who is subject to obligations and enforcement.

From the perspective of state authority, identity data forms the basis of trust between the state and society. Public administration, welfare provision, law enforcement, and democratic participation all rely on the assumption that identity data is accurate, consistent, and authoritative. Even minor inconsistencies can generate legal uncertainty, while systemic corruption can undermine confidence in the state's ability to govern fairly and predictably.

As a target, identity and authentication data can be corrupted, deleted, or rendered unreliable in ways that erode institutional trust, and during a conflict, when combined with other instruments of influence, these effects can become paralyzing. If records of citizenship, residency, or legal status are compromised, the state may be unable to determine who is eligible for services, who may exercise political rights, or who falls under its jurisdiction. Restoring such data is not merely a technical task but a political one, as decisions about validity and correction inevitably involve questions of legitimacy.

As a vector of influence, identity and authentication data can be manipulated to enable impersonation, administrative paralysis, or selective exclusion. Control over authentication mechanisms can allow external actors to disrupt governance indirectly by creating uncertainty, contestation, or bureaucratic overload. In extreme cases, the inability to reliably authenticate individuals can paralyze core state functions, as every decision becomes potentially disputable.

Because identity and authentication data underpin all other categories of critical data, its compromise tends to cascade across governance systems. Service delivery, taxation, voting, and law enforcement all depend on reliable identification, making this layer particularly sensitive to both deliberate attack and structural dependency.

5.2 Operational Data: How the State Functions

The second category of critical national data consists of operational data that enables the day-to-day functioning of the state. This includes data used in public administration, emergency management, healthcare, energy

systems, transportation, financial oversight, and military logistics. Such data supports planning, coordination, and real-time decision-making across sectors.

Operational data is often distributed across complex digital ecosystems involving public authorities, private providers, and international service platforms. While this distribution can enhance efficiency and resilience under normal conditions, it also increases systemic complexity and interdependence. Decisions made in one domain may have immediate consequences in others, amplifying the effects of disruption.

As a target, operational data can be destroyed, delayed, or distorted to halt essential processes. Disruption does not need to be total to be effective; selective interference with key datasets or decision-support systems can degrade performance sufficiently to overwhelm administrative capacity. During crises, even temporary loss of operational data can have disproportionate effects on public safety and trust, and when coordinated with other tools of influence, the resulting synergistic effect can be greater than the sum of its individual components.

As a vector of influence, operational data can be manipulated to shape outcomes without overt disruption. Altered datasets, biased inputs, or delayed information flows can distort situational awareness and lead decision-makers toward suboptimal or harmful choices. This form of influence is particularly difficult to detect, as decisions may appear procedurally correct while being substantively flawed.

The strategic significance of operational data lies in its role as the unifying factor of governance. When control over this data is weakened, the state may retain formal authority while losing practical capacity, creating a gap between legal responsibility and operational control.

5.3 Authority, Control, and Recovery Data: Who Controls the Digital Backbone

The third category of critical national data concerns authority, jurisdiction, and recovery capability. This category includes system logs, backup repositories, cryptographic keys, root certificates, domain name control, and other data that determine who can validate outcomes, restore systems, and assert ultimate control over digital infrastructures.

Control over this category is essential for sovereignty in cyberspace. Even if operational systems are disrupted, a state that retains authority over recovery mechanisms can re-establish functionality and trust. Conversely, if recovery data or control mechanisms are compromised or placed under external jurisdiction, the state's autonomy is directly challenged.

As a target, attacks on authority and recovery data can prevent restoration, prolong disruption, and magnify the effects of failures in other layers. Destruction or corruption of backups, for example, can transform manageable incidents into existential crises for governance systems.

As a vector of influence, external control over recovery mechanisms can be used to exert pressure, enforce dependency, or constrain political choices. States that rely on foreign-controlled cloud platforms, certification authorities, or system administrators may find that their ability to recover or verify outcomes is contingent on the cooperation of external actors.

This category thus represents the deepest point of vulnerability in digital governance. When authority over the digital backbone is lost, the state may continue to exist formally, but its capacity to act independently and recover from disruption is fundamentally weakened.

6. Discussion: What if a state Loses Control Over its Critical Data?

While earlier research has recognized the strategic importance of data in cyber security and defence policy, the concept of digital state erasure highlights the cumulative governance-level consequences that may arise if a state loses control over critical national data. From an analytical perspective, early indicators of digital state erasure may include persistent external dependency over identity, authentication, or recovery mechanisms; legal or contractual constraints limiting sovereign access to critical datasets; uncertainty regarding data integrity that delays decision-making; and the inability to independently restore systems under crisis conditions.

The preceding categorisation demonstrates that digital state erasure should be understood not as an isolated act or a singular catastrophic event, but as a cumulative and potentially gradual process. Because the three categories of critical national data are deeply interlinked, disruptions in one category can propagate across governance systems, producing cascading effects that far exceed the initial point of failure. Identity data, operational data, and authority- and recovery-related data reinforce one another in ways that make modern states simultaneously efficient and structurally fragile.

A central strategic implication is that the loss of control over critical data undermines state continuity even when formal institutions remain intact. A state may continue to possess territory, armed forces, and legal authority, yet struggle to exercise effective governance if it cannot reliably authenticate its population, trust its administrative data, or restore essential systems after disruption. In such conditions, the state's existence becomes increasingly symbolic rather than operational. Authority is asserted in principle, but not consistently enacted in practice.

These dynamic challenges and traditional security assumptions that equate national survival primarily with physical defence and territorial integrity. Digital state erasure, while often conducted below the threshold of armed conflict and without clear attribution, can intensify as tensions escalate, becoming an increasingly significant component of coercive measures. Strategic vulnerability emerges not from a single decisive blow, but from persistent uncertainty regarding data confidentiality, integrity, availability, and, moreover, control. Over time, this uncertainty erodes institutional confidence, public trust, and the credibility of decision-making.

The discussion also highlights the risks associated with efficiency-driven digitalization. Cost savings, scalability, and rapid deployment have motivated states to outsource critical data storage, processing, and system management to transnational cloud providers and complex vendor ecosystems. While these arrangements may improve performance under normal conditions, they frequently introduce dependencies that weaken sovereign control. Jurisdictional ambiguity, contractual limitations, and reliance on external recovery mechanisms can constrain a state's ability to act autonomously in times of crisis.

From a resilience perspective, contested control over data is often more destabilizing than an outright loss. When authorities cannot be certain whether data has been manipulated, selectively altered, or rendered incomplete, decision-making becomes hesitant and reactive. Officials may delay action to avoid errors, while citizens may lose confidence in the fairness and reliability of public institutions. This erosion of trust can itself become a strategic outcome, even if no single system has fully collapsed.

Digital state erasure therefore aligns closely with broader patterns of hybrid operations and grey-zone competition. Rather than seeking immediate collapse, an adversary may aim to degrade governance capacity incrementally, exploiting legal, technical, and institutional seams. The ambiguity surrounding data control complicates attribution and response, reducing the likelihood of decisive countermeasures and enabling sustained pressure over time.

Importantly, the discussion underscores that technical cybersecurity measures alone are crucial but alone insufficient to address these challenges. Encryption, redundancy, and intrusion detection are necessary components of protection, but they do not resolve questions of authority, jurisdiction, and recovery. Strategic resilience requires explicit recognition of which datasets are existential for the state, where they are located, under which legal regimes they operate, and how they can be restored independently under extreme conditions. Without such clarity, states may inadvertently accept structural vulnerabilities that only become visible during crises.

7. Conclusions: Data, Sovereignty, and the Future of State Security

This paper argued that modern state authority and continuity are increasingly inseparable from control over critical national data. As governance, security, and societal resilience become data-dependent, the confidentiality, integrity, availability, and controllability of key datasets emerge as foundational elements of sovereignty. The concept of digital state erasure captures this transformation by showing how the deliberate destruction, manipulation, or strategic exploitation of critical data can undermine a state's ability to function without the use of kinetic force.

By conceptualizing critical national data as three interlinked categories, this paper provided a framework for understanding why certain datasets are strategically irreplaceable. Identity and authentication data define who the state governs and protects; operational data enables the delivery of services and the exercise of authority; and authority- and recovery-related data determines who ultimately controls the state's digital backbone. Vulnerabilities in any one layer can cascade into the others, producing systemic effects that compromise institutional coherence, legitimacy, and continuity.

A key conclusion is that a state cannot be fully sovereign if it lacks control over the data upon which governance, legitimacy, and recovery depend. Control over critical data constitutes the digital foundation of sovereignty in cyberspace. Losing that control risks digitally erasing a state from the map, even in the absence of conventional military conflict. Therefore, sovereignty in cyberspace should not be fragmented into subcategories, like 'data

sovereignty', but rather highlights how control over data is central to exercising sovereignty itself in the contemporary security environment. The growing reliance on foreign-owned infrastructure, cloud platforms, and transnational service providers therefore represents not only a technical or economic choice, but a strategic trade-off with long-term implications for national autonomy.

Preventing digital state erasure requires a shift in how states conceptualize security and resilience. Critical national data must be identified, prioritized, and governed explicitly as a part of national security planning. This includes ensuring sovereign control over the most sensitive datasets, maintaining independent recovery capabilities, and aligning legal, institutional, and technical frameworks to support continuity under crisis conditions. Such measures are not aimed at technological isolation, but at preserving the state's ability to act independently when it matters most.

Ultimately, the strategic value of data lies not only in its content, but in the authority it enables. A state that loses the ability to authenticate its population, conduct legitimate elections, provide essential services, or restore its systems after disruption risks losing more than operational capacity – it risks losing its political existence as a self-governing entity. In this sense, critical data constitutes the digital foundation of state authority and continuity. Its protection is therefore not merely a matter of cybersecurity or administrative efficiency, but a core obligation of sovereign governance in the digital age.

Ethics declaration: Ethical approval was not required for the research described in this paper.

AI declaration: AI tools were used to support language editing; the conceptual framework, analysis, and conclusions are the responsibility of the authors.

References

Ardagna, C.A., Bellandi, V., Damiani, E., Bezzi, M. & Hebert, C. (2021) "Big Data Analytics-As-A-Service: Bridging the Gap Between Security Experts and Data Scientists", *Computers and Electrical Engineering*, Vol 93 [online] https://doi.org/10.1016/j.compeleceng.2021.107215 [Accessed March 10 2026].

Bradshaw, S., & Howard, P. N. (2019) *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Oxford Internet Institute, Oxford University [online] https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf [Accessed March 10 2026].

Dad, N., & Khan, S. (2023) "Reconstructing Elections in a Digital World", *South African Journal of International Affairs*, Vol 30, No 3, pp 473–496 [online] https://doi.org/10.1080/10220461.2023.2265886 [Accessed March 10 2026].

Dalton, C. M., Taylor, L., & Thatcher, J. (2016) "Critical Data Studies: A Dialog on Data and Space", *Big Data & Society*, Vol 3, No 1, [online] https://doi.org/10.1177/2053951716648346 [Accessed January 12 2026].

ENISA (2025) *ENISA Threat Landscape 2025*, ENISA, October 2025, [online] https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf [Accessed January 16 2026].

Farrell, H. & Newman, A.L. (2019) "Weaponized Interdependence: How Global Economic Networks Shape State Coercion", *International Security*, Vol 44, No 1, pp 42–79 [online] https://doi.org/10.1162/isec_a_00351 [Accessed March 10 2026].

Finnish Defence Forces (2025) *Puolustusvoimien data- ja tekoälystrategia [Data and AI Strategy of Finnish Defence Forces]*, Finnish Defence Forces 29.10.2025, [online] https://puolustusvoimat.fi/-/puolustusvoimien-data-ja-tekoalystrategia-on-julkaistu [Accessed March 10 2026].

Hakahuhta, A. (2025) "Suomen vaalidata siirtyy Amazonin pilveen – USA:n vaalivilppiepäilyjä tutkinut asiantuntija varoittaa riskeistä" [Finnish election data to be transferred to Amazon's cloud – expert who investigated US election fraud allegations warns of risks], *Yle* 6.11.2025, [online] https://yle.fi/a/74-20191502 [Accessed November 7 2025].

Iliadis, A., & Russo, F. (2016) "Critical Data Studies: An Introduction", *Big Data & Society*, Vol 3, No 2, [online] https://doi.org/10.1177/2053951716674238 [Accessed January 12 2026].

ITU (2025) "What is Data Classification?", *ITUonline.com* 13.1.2026, [online] https://www.ituonline.com/tech-definitions/what-is-data-classification/ [Accessed January 13 2026].

Jungherr, A. (2023) "Artificial Intelligence and Democracy: A Conceptual Framework", *Social Media + Society*, Vol 9, No 3 [online] https://doi.org/10.1177/20563051231186353 [Accessed March 10 2026].

Kwet, M. (2019) "Digital Colonialism: US Empire and the New Imperialism in The Global South", *Race & Class*, Vol 60, No 4, pp 3–26 [online] https://doi.org/10.1177/0306396818823172 [Accessed March 10 2026].

Kitchin, R. (2014) *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. SAGE Publications Ltd, [online] https://doi.org/10.4135/9781473909472 [Accessed January 12 2026].

Koponen, J. (2025) "Kelan muutos vie suomalaisten arkaluontoiset terveystiedot ulkomaisiin konesaleihin" [Kela's (Social Insurance Institution of Finland) change will transfer Finns' sensitive health data to foreign data centres], *Yle* 13.11.2025, [online] https://yle.fi/a/74-20193175 [Accessed November 13 2025].

Mont'Alverne, C., Arguedas, A. R., Banerjee, S., Toff, B., Fletcher, R., & Nielsen, R. K. (2024) "The Electoral Misinformation Nexus: How News Consumption, Platform Use, and Trust in News Influence Belief in Electoral Misinformation", *Public*

Opinion Quarterly, 88(SI), pp 681–707 [online] https://ora.ox.ac.uk/objects/uuid:459f042c-f526-45ff-aa98-1ba27edb4c20 [Accessed March 10 2026].

Mussington, D. (2021) "Securing the Critical National Infrastructure", in Paul Cornish (ed.), *The Oxford Handbook of Cyber Security*, Oxford Handbooks, 8.12.2021, [online] https://doi.org/10.1093/oxfordhb/9780198800682.013.26 [Accessed January 12 2026].

Nguyen, H–N. & Cuong, L. (2025) "Overview of Data Classification and Applications in Data Security", *International Journal of Environmental Sciences*, [online] https://doi.org/10.64252/ac0b3685 [Accessed January 12 2026].

NIST (2023) "Data Classification Concepts and Considerations for Improving Data Protection", *NIST IR 8496 ipd*, November 2023, [online] https://doi.org/10.6028/NIST.IR.8496.ipd [Accessed January 13 2026].

Ofili, B. T., Ezeadi, S. C., & Jegede, T. B. (2024) "Securing US National Interests with Cloud Innovation: Data Sovereignty, Threat Intelligence and Digital Warfare Preparedness", *International Journal of Science and Research Archive*, Vol 12, No 1, pp 3160–3179, [online] https://doi.org/10.30574/ijsra.2024.12.1.1158 [Accessed January 13 2026].

Rossbach, N. H. (2024) *Intelligence and Data Resilience: A Small State Perspective on Digitalisation and National Defence Towards the 2030s*. Försvarshögskolan (FHS), [online] https://www.diva-portal.org/smash/get/diva2:1919672/FULLTEXT01.pdf [Accessed January 13 2026].

Shandler, R. & Gomez, M.A. (2023) "The hidden threat of cyber-attacks – undermining public confidence in government", *Journal of Information Technology & Politics*, Vol 20, No 4, pp 359–374, [online] https://doi.org/10.1080/19331681.2022.2112796 [Accessed March 10 2026].

Shivayogi, S. K. (2025) "Data Classification Methodologies and Implementation", *Journal of Computer Science and Technology Studies*, Vol 7, No 5, pp 202–210, [online] https://doi.org/10.32996/jcsts.2025.7.5.26 [Accessed January 13 2026].

U.S. Department of Defense (2020) *Executive Summary: DoD Data Strategy*, U.S. Department of Defense, 30.9.2020, [online] https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF [Accessed March 10 2026].

Weber, V., Pericàs Riera, M. & Laumann, E. (2023) "Mapping the World's Critical Infrastructure Sectors", *DGAP Policy Brief 35 (November 2023)*, German Council on Foreign Relations, [online] https://doi.org/10.60823/DGAP-23-39548-en [Accessed January 13 2026].

Zins, C. (2007) "Conceptual Approaches for Defining Data, Information, and Knowledge", *Journal of the American Society for Information Science and Technology*, Vol 58, pp 479–493, [online] https://doi.org/10.1002/asi.20508 [Accessed January 13 2026].