Journal of Research, Innovation and Technologies https://doi.org/10.57017/jorit.v3.2(6).01

Exploring the Preventive Contribution of Data Localisation Against Information Technology Outages: The CrowdStrike Case

Yassin Abdalla ABDELKARIM ✉
Luxor Elementary Court, Luxor Governorate, Egypt
Leeds Beckett University, UK
https://orcid.org/0000-0001-7388-1337

Abstract

The severe impacts of the CrowdStrike outage on the world economy and national critical services, e.g., banking, healthcare, and airports, invoked the urgent need to decrease governmental dependence on foreign tech companies to store and manage national data. An effective alternative to this approach is data localisation. The latter includes the physical placement of data infrastructure within the state's territory or imposing ultimate national control over data stored in a server located abroad, along with relevant managing software. The research points out the prominence of data localisation to protect national data, and the functionality of services depending on this data, against technical failures that cause outages. In this endeavour, the research reviews the concepts of territoriality and localisation of cyberspace, along with shedding light on the CrowdStrike outage and explaining its reasons and consequences. Then, it introduces a justification for the validity of data localisation for preventing outages' negative impacts and protecting national data.

Keywords: data localisation, territoriality, sovereignty, cyberspace, CrowdStrike outage, Internet giants.

JEL Classification: K10, K22, K24, K29, K33; O14.

Introduction

The dominance of cyberspace-based information exchange systems qualified data routing and managing systems to be crucial to states' national informational systems. They have dominated the critical services a state presents, e.g., air transport, banking and finance, and healthcare, to its citizenry and foreign residents. It is witnessed these days that several states depend ultimately on tech companies to administer and store national data systems through the powerful infrastructural capabilities of these entities. States are motivated in their approach by the global technological enthusiasm for borderless cyberspace with free-flow data systems. Consequently, national data become located within a foreign territory preventing the actual control of a state over national data. This status ties the functionality of national services, operated by these data, with the integrity and operationality of the infrastructure controlled by foreign companies.

The noted state-of-the-art poses a severe challenge to states concerning maintaining the functionality of their critical services because failures or outages of the storing devices or software inflict direct impacts on the state that owns the data stored therein. The CrowdStrike global outage, which occurred on 19 July 2024, introduced a complete manifestation of the mentioned consequence as a single failure of a software update has inflicted notable damage on global critical national services which fundamentally depend on this software for protection. On this day, the world witnessed grave negative impacts that motivated governments to reconsider their ultimate dependence on tech companies in addition to the criticality of the affected data by the outage. Indeed, the CrowdStrike global outage of cyberspace services alarmed the bell to reconsider the topography of cyberspace regarding the question of data localisation. The nationalist motivation for the latter compels states to initiate strategies to place cyberspace infrastructure within their territory or impose ultimate control over data stored in a server located abroad. Thus, data localisation has become of utmost importance to national security and states have focused on this aspect because of the indispensability of data protection policies.

Accordingly, the research highlights the importance of national data localisation strategies as a preventive measure from the severe impacts of technical cyberspace outages, caused by foreign technical failures. To achieve its objective, the research reviews the concept of territoriality in cyberspace and its nexus to data localisation, then it offers a brief on the CrowdStrike outage and its grave impacts on the global economy and critical services. Afterward, the study figures out the preventive contribution of data localisation to protecting the integrity of national data and, therefore, maintaining the functionality of national critical services.

1. Territorialization and Localisation: A Tight Correlation

Determining the boundaries of a state's territory is the starting line for a government to enforce its policies and regulations. The demarcation of geographic states' territories in the real world is direct by utilizing consensual borders 'drawing mechanisms as affirmed in International Law. Nevertheless, in the digital realm, where physical borders and geographic landmarks disappear, determining a national territory of a state proves problematic and it is illogical to impose policies, such as localisation, without determining their territorial scope of application. Therefore, the study explores the applicability of the territorial perspectives in cyberspace to scavenge their nexus to domestic data localisation strategies.

Territoriality in Cyberspace

The territorialization of cyberspace refers to the process of applying traditional territorial concepts to the digital realm. This process involves states and other actors asserting control and sovereignty over specific parts of cyberspace similar to their physical territories. It is driven by the assumption that online activities that occur within a country, due to the presence of users, servers, or data, should be considered part of that country's cyberspace territory.

Although scholars and technicians consider cyberspace a common global open space, the *de facto* states' practice over data exchanged within, in addition to the physical architecture of cyberspace, reflects a manifestation of territorial sovereignty (von Heinegg, 2013, p. 126). He claimed that the technical hardship to impose the state's policies in cyberspace does not waive its sovereign exclusive authorities over the national cyber territory. Thus, a state is eligible to implement the required measures to defend its cyber territory. Territorial sovereignty in cyberspace does not necessarily imply that the traditional rules and principles of international law apply to cyberspace in their conventional interpretation. Due to the unique nature of cyberspace and the vulnerability of cyber infrastructure, there is significant uncertainty among governments and legal scholars about whether traditional rules and principles are adequate to address certain pressing concerns (von Heinegg, 2013, p. 127). As a consequence of his view, he asserted the applicability of International Law principles organizing the territorial relations among states, e.g., sovereignty respect and the duty of prevention, to cyberspace (von Heinegg, 2013, pp. 134-138; Zinovieva, 2024, p. 194). Thus, territoriality in cyberspace is not fictitious but it constitutes an outstanding reality. This accords with the UN Expert Group doctrine reviewed in Zinovieva (2024, p. 191). States' practice of authority in cyberspace asserts the applicability of the territorial sovereignty notion in the digital realm. Even states that contradict this doctrine, because of liberal considerations, tend to manage data flows to achieve national security objectives (Zinovieva, 2024, p. 192), which constituted a *de facto* representation of territorial sovereignty in cyberspace, regardless of the *prima facie* allegations of maintaining a liberal Internet environment.

Furthermore, Simmons and Hulvey (2023, p. 625) defend Internet bordering, claiming that states impose boundaries to engineer differences among the international community. Territorialization of human interaction spaces enhances national distinctiveness and evades inter-state cyber conflicts as it determines explicitly the limits of sovereign policies. Furthermore, spaces in cyberspace share the same characteristics as real-world territories (Lambach, 2020, p. 489). They are an analogical extension of the former. Notwithstanding, cyberspace territories are dynamic and non-exclusive; they do not take a fixed topography but are in a status of continuing change according to data routes. States' authority in cyberspace is not absolute; it is composed of regulatory tasks to prevent severe threats in this globally wide-stretching communication network (Lambach, 2020, p. 486). Since

cyberspace consists of users and objects, states' endeavours to regulate and organize them manifest territoriality because states' behaviour accords with their policies concerning real geographic territories (Tsaugourias, 2018, p. 536). Thus, territories are perceived in cyberspace, even if the latter is merely a virtual environment. The universal trend of digital transformation has influenced the conceptualization of territoriality in dynamic cyberspace as it developed a digital version of territoriality linked to the technical operations of information exchange among Internet users (Adonis, 2023, p. 92). A functional territoriality proves efficient to overcome the exceptional technical nature of cyberspace which creates several complex odds against the imposture of national strategies. Accordingly, Zekos (2022, p. 364) argues that territorializing cyberspace should be conducted through advanced geographical digital tracking of data flow on the Internet, in addition to the effect factor, to adapt traditional territoriality to the virtual innovative realm of cyberspace.

Additionally, cyberspace territorialization promotes states' investments in Internet infrastructure since they would utilize it to maintain national sovereignty. States would solely extend national borders imposture mechanisms from the physical dimension to cyberspace (Simmons & Hulvey, 2023, p. 626) under a horizontal imposture scheme (Lambach, 2020, p. 486), which creates a monolith chain of cyber territories. A horizontal linkage between national cyberspace territories enhances the integrity and effectiveness of Internet operations through states' cooperative administration of each territory. This shape of cyberspace mapping introduces more disciplined and organized data flow routes among states, based on the principle of mutual respect of territorial sovereignty, which decreases the potentialities of illegal cyber activities, on the one hand, and provides individuals and entities with a solid structure of cyberspace services, otherwise, anarchism prevails.

Likewise, Japaridze (2023, p. 216) considers states' mutual admittance of national authority over a cyberspace territory an enhancement of global peaceful coexistence. It enables governments to suppress harmful illegal cyber activities, ensuring safer cyberspace environments. Thus, the territorialization of cyberspace proves advantageous for humanity. Territoriality in cyberspace is rooted in the actual practices of states to control data traffic to confront threats (Lambach, 2020, p. 488). It is an ontological *fait accompli* conception needless to repeatedly justified. Nonetheless, an extreme interpretation of territorialization could fragment cyberspace into isolated segments, contradicting the original intent of this global domain. Therefore, territorialization, as a guiding principle, must be balanced carefully (Japaridze, 2023, p. 225) to achieve its original objective of securing data in cyberspace. Furthermore, the coordination of states' approaches to territorialize cyberspace is obligatory to create a universal consensus on a determinant, evading inter-state political confrontations that destabilize cyberspace (Abdelkarim, 2024, p. 390). Thus, the adequate territorialization of cyberspace requires a multilateral scheme. This indication led Fang (2018, pp. 85-86) to link territories in cyberspace to the actual map of a state's Internet devices; they constitute the true boundaries of a national territory in cyberspace.

Data Localisation as a National Strategy

Localisation is a national state practice to control data flows from foreign sources to the inner society and *vice versa,* ensuring that data generated within a specific jurisdiction remains within its geographical boundaries. Han (2024, p. 265) defines data localisation as "a policy implemented by a state that requires entities to store data within its sovereign territory". Therefore, it constitutes a logical consequence of cyberspace territorialization that includes the state's exercise of authority over cyberspace infrastructural hardware to control data transfers (Lambach 2020, p. 485). Data localisation includes the placement of physical cyberspace infrastructure within the national territory or imposing direct control over servers where national data is stored even if located abroad.

Cyberspace includes a physical layer made up of computers, integrated circuits, cables, communication infrastructure, and similar components (Tsaugourias, 2018, p. 539). Thus, the localisation of cyberspace physical infrastructure is a multi-dimensional process that includes states' efforts to own the physical equipment operating cyberspace, whether located on their national soil or abroad. States' ownership of cyberspace infrastructural hardware manifests a logical conclusion of admitting private ownership in cyberspace (Lambach, 2020, p. 488). As

Han (2024, p. 265) indicates, the sovereign responsibility of a state to safeguard national data is the chief motivation for localizing data. Since cyberspace data is majorly stored in servers owned by US entities, severe breaches of national security occur in practice due to the contribution of Internet Giants to enabling the US official agencies to execute data mining operations[1]. Remarkably, he limited the execution of localisation strategies to the state's ability to harness and benefit from the positive network effect, which is a chief strength of Internet Giants. This contradiction creates an imbalanced relationship between the state and Internet Giants concerning data storage capabilities (Han 2024, p. 268). Consequently, this imbalance enables states to evaluate whether the network effect generated by platforms aligns with national interests and if they can effectively utilize the resulting benefits.

Data localisation imposes the state's objectives on how cyberspace is used by the citizenry thus it localizes cyberspace infrastructure establishments to enforce the national grip on hovering data within the national cyber territory (Simmons & Hulvey, 2023, pp. 627-628). Moreover, states encourage domestic industry enterprises to prefer nationally generated data in their business rather than data from foreign sources and, as well, submit data traffic in the national territory in cyberspace to political and sovereign considerations such as national security (Lambach, 2020, p. 485). This fact elaborates on the increasing state's demand to localize the physical cyberspace data servers and centers regardless of the government's obvious intent to control and survey data. Localisation has become a global national trend because of the states' endeavours to maintain the functionality of national services, that depend on cyber facilities, and protect sensitive data against either foreign threats, e.g., espionage, or technical glitches (Lambach, 2020, p. 495; Baur-Ahrens, 2017, p. 44). Nevertheless, the European Court of Justice considered this policy a violation of the fundamental human right to privacy (Simmons & Hulvey, 2023, p. 629). Therefore, the European General Data Protection Regulation[2] stipulates complete compliance with the protection of data privacy requirement to permit states' acquisition of data transfer infrastructure. According to their analysis of data localisation policies, localisation of cyberspace infrastructure reflects the state's attitude about data surveillance and governance (Simmons & Hulvey, 2023, pp. 630-631). It is a separation mechanism to distinguish domestically sourced data from their foreign counterpart that offers a pure domestic version of data flow schemes.

States adopt several techniques to achieve cyberspace data localisation. They can construct domestic servers to prevent national data from routing via foreign servers (Baur-Ahrens, 2017, p. 44). This implies that data traffic will be completely controlled and surveyed by the state. The US Department of Commerce, through its National Telecommunications and Information Administration (NTIA), has implemented a significant internet routing security measure[3]. This initiative, part of the National Cybersecurity Strategy[4], aims to enhance cybersecurity across the Department. The measure addresses long-standing concerns about internet routing incidents, which can disrupt services. The NTIA has developed Route Origin Authorizations (ROAs) to authenticate its network addresses, ensuring that internet traffic reaches its intended destinations. In addition, China recognized the strategic importance of Internet control early, structuring its architecture as an intranet with strict border controls (Salamatian et al., 2021, p. 2).

China utilizes cyber territorialization to refer to the state's control over its cyber infrastructure and the information that enters or becomes available within its borders (Tsaugourias, 2018, p. 547). Thus, China enforces this sovereign localisation through filtering, which involves using technical, political, legal, or social methods to block access to certain information or activities, or to prevent such information or activities from entering the state's sovereign cyberspace.

In addition, Iran, on contrary to several Middle East states, has successfully developed a national network that balances two seemingly conflicting characteristics. It is both highly resilient, with numerous Autonomous

[1] See https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html accessed on 24 July 2024.
[2] Council Regulation 2016/679, (General Data Protection Regulation), 2016 O.J. (L 119) 1. https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/#gsc-main-content
[3] https://www.ntia.gov/press-release/2024/us-department-commerce-implements-internet-routing-security (21 July 2024)
[4] https://www.whitehouse.gov/oncd/national-cybersecurity-strategy/ accessed 21 July 2024.

Systems (ASes) and a rich internal path ecosystem, and highly controlled, with all outgoing traffic routed through three main government-controlled ASes. This design allows Iran to isolate its network from the global Internet while maintaining robust internal connectivity without causing congestion among the central Ases (Salamatian et al., 2021, p. 12). Consequently, the Iranian territorialization approach created a parallel national cyberspace that can resist global Internet outages because the whole data routes are domestically isolated from the international network. Similarly, according to Russia's Federal Law No. 242-FZ, operators are required to ensure that the recording, systematization, accumulation, storage, adjustment (update, alteration), and retrieval of personal data of Russian citizens are conducted through database servers located within Russia. Significant fines are imposed on organizations and individuals who fail to comply with these data localisation requirements (Wu, 2021, p. 11). On 28 April 2024, Egypt inaugurated its national cloud data center to store the national data. The Egyptian data center constitutes the core of the national digital transformation strategy. It has added new horizons for entrepreneurship in all fields and industries, providing new opportunities to combine several fields in one work environment.[5]

Furthermore, the policy of centralizing data storage facilities enhances the national localisation strategy. By establishing grand national data storage centers, the state can strengthen its grip on the source of exchanged data domestically on the Internet. According to Baur-Ahrens (2017, p. 45), Deutsche Telekom suggested to the German Federal Government and the European Union (EU) to initiate a national routing system within Germany and eventually expand it to a Schengen routing system. This proposal aims to prevent US and British intelligence agencies from accessing data flows within the Schengen area. South Africa introduced the National Data and Cloud Policy, which includes requirements to store and process data considered "critical information infrastructure" within the country's borders and to mirror data generated from South African natural resources[6].

To sum up, contemporary practices of states disclose the prominence of imposing control over national data by localizing them. This process manifested the threshold to organize data flows through a state's cyber territory. Data localisation does not include solely servers and cables; it is an economic process with political perspectives. States stitch both pillars together to serve their preventive objectives in cyberspace.

2. Explaining the Nexus: The Concept of Data Sovereignty

The nexus between cyberspace territorialization and data localisation highlights the ongoing tension between maintaining a global, open internet and the desire of states and corporations to exert control over their digital domains. Since data localisation implies that data about citizens or residents of a certain country should be collected, processed, or stored within that country, before being transferred overseas, it is considered a firm manifestation of the sovereign territorialization of cyberspace. Furthermore, localisation enhances the governments' policies to strengthen their sovereign authorities over the national cyber territory (Duggal, 2019, p. 4). Thus, territorialization implies the physical placement of internet infrastructure, such as servers and data centers, within a country's borders. Thus, this concept is closely linked to infrastructure localisation as Salamatian et al. (2021, p. 17) concluded that localizing Internet infrastructure is a chief pillar of cyberspace territorialization strategies. It protects sensitive national data from being leaked or lost. In this aspect, states handle data as a national resource that requires protection. Moreover, the linkage pointed out by Zekos (2022, p. 346) between a state and cyberspace activities that affect its interests justifies imposing a state's policies, including localizing data flow physical routes.

[5] State opens 1st biggest data, cloud computing centre in MENA (The Egyptian Gazette on 28 April 2024) https://egyptian-gazette.com/egypt/state-opens-1st-biggest-data-cloud-computing-centre-in-mena/ accessed on 25 July 2024.
[6] Draft National Policy on Data and Cloud, Department Of Communications And Digital Technologies, Government Gazette on 1 April 2021. https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

Furthermore, the imposture of national control over data in cyberspace, regardless of the location of their servers, is a chief aspect of data sovereignty. States derive this authority from the natural right of their citizenry to manage their data (Hellmeier et al., 2023, p. 2) under the broad concept of the right to self-determination.

An accurate conception of data sovereignty requires a universal consensus on the implementation schemes of national policies (Hellmeier et al., 2023, p. 6; Hellmeier & von Scherenberg, 2023, p. 7). As a result, states can assert their sovereign strategies over electronic transactions and interactions that impact their interests. According to this logic, data localisation expresses the state's sovereignty over national data, which manifests the concept of data sovereignty. The latter refers to the subordination of national data in cyberspace to domestic legal frameworks (Hummel et al., 2021, p. 1). This concept transcends geography because a state can exercise its authority over data stored in a server abroad (Hummel et al., 2021, p. 13). From this perspective, the physical localisation of cyberspace infrastructure is not required to impose sovereign data policies provided that a state can manage and control streamed data. The crucial factors, in this case, are the concept of ownership and the state's data control capabilities (Abbas et al., 2024, p. 2) because limiting data sovereignty to the mere authority over the Internet causes inter-state fractions due to their different understandings of this conception and applications of relevant national strategies.

Data sovereignty is a solid concept in the digital realm enhanced by governments' practices, disregarding their variances, to organize and control national data in cyberspace (Hellmeier & von Scherenberg, 2023, p. 3). It offers states an upper authority to determine the course and fate of data on the Internet to achieve national objectives such as protecting sovereign national cyber interests. This patriotic motivation remains the chief momentum to impose national sovereignty over exchanged data in cyberspace. Despite several conclusions, the desire to control data remains the core pillar of data sovereignty (Abbas et al. 2024, p. 3) as a consequence of the rising adoption of cloud computing and extra-territorial data routing schemes.

A report by the Belfer Center for Science and International Affairs at Harvard Kennedy School connected data localisation with sovereignty requirements by indicating that states' attitudes to placing cyberspace infrastructure within its borders are a direct consequence of the growing digital dominance of markets and politics (Wu, 2021, p. 6). It is a state's practice to express its national data sovereignty in cyberspace, which constitutes an obvious manifestation of territorialization. Wu (2021, p. 22) indicates in her report that states, concerning data localisation, are motivated by a patriotic desire to achieve digital independence, regardless of the effective outcome of their policies. It is a shield against the dominance of Internet Giants that belong to imperial Western superpowers.

To conclude, data sovereignty in cyberspace constitutes a rendezvous point of the territorial understanding of the virtual realm with the domestic policies imposed by states to safeguard their sovereign interests. The conception of subordinating cyberspace data to national regulations and policies corresponds with the utter purpose of data localisation by ensuring that the relevant entities, whether individuals, organizations, or governments, have authority over how data is used, stored, and shared within their jurisdiction. Thus, the territorial localisation of cyberspace data is the accurate manifestation of enforcing sovereignty over data in cyberspace. In addition, data sovereignty is the chief justification of the states' desire to enforce localisation policies disregarding the openness of cyberspace and the cross-border data flows enhanced by rapid global technological advancements. Therefore, the integral coherence of data sovereignty and territorial localisation formulates an obvious conclusion, a description qualifies the linkage between these concepts to support data localisation national strategies.

3. CrowdStrike Global Outage

CrowdStrike Holdings, Inc., an American cybersecurity technology company based in Austin, Texas, specializes in cloud workload protection, endpoint security, threat intelligence, and cyberattack response services. It is an $83 billion company with more than 20,000 subscribers around the world including Amazon.com and Microsoft. The company has played a key role in investigating several high-profile cyberattacks, including the 2014 Sony Pictures hack, the 2015–16 cyberattacks on the Democratic National Committee (DNC), and the 2016 DNC email leak. In July 2024, a faulty update to its security software caused global computer outages, disrupting air travel, banking, broadcasting, and other services[7].

The Outage

On 19/07/2024, critical infrastructure globally was affected by a major outage of services caused by a CrowdStrike update of the cybersecurity software Falcon Sensor[8]. A recent CrowdStrike update is causing Windows computers to crash and display the blue screen of death. Reports indicate that companies across various industries worldwide are unable to reboot their systems. A faulty CrowdStrike software update disrupted systems globally, grounding flights, halting broadcasts, and affecting services from banking to healthcare.

As posted on X by CrowdStrike CEO George Kurtz, the company admits accountability for the outage caused by its software update. He denied the occurrence of cyber-attacks or incidents, declaring the company's attempts to isolate and fix this technical flaw[9]. CrowdStrike officially apologized for the outage and reasoned it by a technical defect in the Falcon Sensor product[10].

The Consequences

The overwhelmingness of cyberspace techniques in administering the global economy permitted a single cyber incident to inflict severe wide-scale economic impacts. Airlines schedules suffered delays and cancellations leading to passengers over crowdedness in airports[11]. Also, healthcare providers declared a medical emergency due to a global IT outage caused by CrowdStrike. Two hospitals in northern Germany (Luebeck and Kiel) cancelled elective surgeries, while the University Clinic of Schleswig-Holstein assured emergency services remain unaffected[12]. England's National Health Service (NHS) reported disruptions to appointment bookings and patient records but no impact on emergency services[13].

Financially, according to Allianz, the outage affected insurance as employees were unable to log in to their computers[14]. Commonwealth Bank of Australia noted technical deficiencies faced by customers concerning instant money transfers. Similar issues occurred with German banks according to the Deutsche Kreditwirtschaft[15]. Brazilian lender Bradesco announced the unavailability of its digital platforms because of the outage. Macquarie Capital was unable to provide liquidity for unexpired warrants on Hong Kong Exchange. Moreover, The London Stock Exchange

---

[7] https://www.crowdstrike.com/en-us/ accessed on 21 July 2024.

[8] Bishop, K. & Kharpal. A. CrowdStrike issue causes major outage affecting businesses around the world (CNBC,19 July 2024) https://www.cnbc.com/2024/07/19/crowdstrike-suffers-major-outage-affecting-businesses-around-the-world.html (20 July 2024)

[9] https://x.com/George_Kurtz/status/1814235001745027317 accessed on 20 July 2024.

[10] Our Statement on Today's Outage (CrowdStrike Blog on 19 July 2024) https://www.crowdstrike.com/blog/our-statement-on-todays-outage/ accessed on 20 July 2024.

[11] Berlin airport faces major disruptions amid global tech outage (Reuters on 19 July 2024) https://www.reuters.com/technology/berlin-airport-faces-major-disruptions-amid-global-tech-outage-2024-07-19/ accessed on 20 July 2024.

[12] Two German hospitals cancel elective operations citing global IT outage (Reuters on 19 July 2024) https://www.reuters.com/business/healthcare-pharmaceuticals/two-german-hospitals-cancel-elective-operations-citing-global-it-outage-2024-07-19/ accessed on 20 July 2024.

[13] Update on cyber incident: Clinical impact in south east London (NHS England on 19 July 2024) https://www.england.nhs.uk/london/2024/07/19/update-on-cyber-incident-clinical-impact-in-south-east-london-friday-19-july/ accessed on 20 July 2024.

[14] Traders eye return to business as usual after cyber outage; issues remain (The Business Times on 20 July 2024) https://www.businesstimes.com.sg/companies-markets/traders-eye-return-business-usual-after-cyber-outage-issues-remain accessed on 20 July 2024.

[15] The German Banking Industry Committee, see https://die-dk.de/

Group's (LSEG) Workspace news and data platform experienced an outage that disrupted user access globally, impacting financial markets[16].

Furthermore, the outage, despite its pure technical causes, generated universal cybersecurity concerns. Australia's cyber intelligence agency - the Australian Signals Directorate (ASD), announced on Saturday that "malicious websites and unofficial code" are being circulated online, purportedly offering solutions to recover from Friday's global digital outage, which affected media, retailers, banks, and airlines[17]. Thus, ASD urges Australian Internet users to source their technical information and updates from CrowdStrike solely to prevent unwanted cyber incidents.

Localisation of Cyberspace Data to Prevent Outages

Establishing national data centers is effective in localizing data under laws that mandate that data pertaining to a country's citizens must be processed and/or stored within that country. These laws can apply to all personal data or be limited to specific types, such as health or financial information. They affect not only online services but also traditional sectors of the economy, including banking. In this section, the research reviews the Internet Giants' stance on data localisation, highlighting their share in controlling cyberspace data, and then it sheds light on the privileges of domestic data localisation versus several cyber threats.

Internet Giants' Opposition

In cyberspace, Internet Giants, e.g., Meta and X, hold the upper authority to supervise and control exchanged data on several social networking platforms. Internet giants, as private entities, possess certain rights over their users. They extend these inherent proprietorship rights and acquire additional ones through contracts and service agreements. These contracts impose rules and regulations on users, enabling these companies to exercise legislative and administrative authority like that of a government (Kim & Telman 2015, p. 745). Their powerful technological dominance over data motivated governments to involve them in official cybersecurity operations, such as data mining (Kim & Telman 2015, p. 728). This governmental approach granted Internet Giants a de facto superiority in cyberspace leading them to compete with national governments in data control, elevating them to be quasi-governmental actors in cyberspace. Likewise, Hendry clarified that the opposition of Internet Giants to governmental data localisation strategies is caused by the misconception of the correlation between cybersecurity risks and the location of cyberspace physical infrastructure[18]. They consider data localisation as an obstacle against free cross-border data flows. In the same context, Meta CEO Mark Zuckerberg expressed his opposition to data localisation. He argued that while certain countries might have legitimate reasons for such policies, authoritarian regimes could exploit data localisation to access and control their citizens' data, thereby curbing dissent. Zuckerberg emphasized the importance of considering the motives behind data localisation demands and warned that setting a precedent could make it easier for authoritarian governments to justify similar measures[19]. Tech giants operate on a global scale and their platforms connect people across borders, transcending physical boundaries that might be disrupted by cyberspace fragmentation caused by national policies of data localisation; an approach that goes against the interconnectivity required to push forward modern human civilization.

[16] What disruptions have been reported after the global tech outage? (Reuters on 20 July 2024) https://www.reuters.com/markets/commodities/what-disruptions-have-been-reported-after-global-tech-outage-2024-07-19/ accessed on 20 July 2024.
[17] Australia warns of malicious websites after cyber outage (Reuters on 20 July 2024) https://www.reuters.com/technology/cybersecurity/australia-warns-malicious-websites-after-cyber-outage-2024-07-20/ accessed on 20 July 2024.
[18] Hendry, J., Tech giants rally against data localisation in Australia (InnovationAus.com on 7 September 2022) https://www.innovationaus.com/tech-giants-rally-against-data-localisation-in-australia/ accessed on 27 July 2024.
[19] Mark Zuckerberg opens up on data localisation and why he's not in favour (Indian Express: Tech Desk on 19 April 2019) https://indianexpress.com/article/technology/tech-news-technology/mark-zuckerberg-opens-up-on-data-localisation-and-why-he-not-in-favour-5700109/ accessed on 22 July 2024.

Furthermore, it has been proven that states' strategies to localize data might frustrate certain plans of Internet Giants. On 26 July 2024, an investigation published in Politico disclosed intentional data mining operations conducted by X social network exploiting users' data to enhance the abilities of AI applications[20]. Users' data on these platforms are fertile soil strengthening the capabilities of machine learning models inter alia other AI applications (Injadat et al., 2016, p. 8) by deploying mining techniques that collect and analyse this data to extract certain patterns or build algorithms. This technical method violates the essentials of Internet users' privacy and justifies governmental interventions to safeguard data.

Economically, data localisation increases the cost of domestic data hosting by 60% because the Internet enables centralized data storage and processing, taking advantage of economies of scale in cloud computing and a seamless, global Internet[21]. When governments break apart these efficiencies, they exponentially raise relevant costs. This consequence manifests an economic drawback of data localisation. Over the past decade, an array of scholarly investigations has meticulously dissected the adverse effects of data localisation. These effects reverberate across the economic landscape, impacting critical dimensions such as overall output, international trade, and productivity (CIPL 2023, p. 4). In the contemporary rapidly digitalizing global economy, data localisation emerges as a double-edged sword; businesses find themselves caught in a replication conundrum. To comply with data localisation requirements, they must duplicate personnel, datasets, data center infrastructure, and technological resources across various localizing jurisdictions. Moreover, companies must adapt when countries enforce data localisation rules by investing time, energy, and management attention to understand local regulations. Adaptability requirement increases compliance costs because of the differences among jurisdictions concerning localisation requirements (Han 2024, p. 264). This is the case for governments as well; data localisation imposes expenses on states to meet data mirroring requirements, particularly when data is stored abroad (Medine, 2024, p. 7). The Policy Research Institute, Japan Ministry of Finance, concluded that data localisation measures violate the fundamentals of the global free flow of trade required to sustain the world economy (Yoshinori, 2021, p. 18) and states should refrain from exploiting the general exceptions of the free trade principle, affirmed by World Trade Organization (WTO) and the General Agreement on Trade in Services (GATS)[22]. Thus, data localisation does not constitute a mere technical manoeuvre; it is an economic ballet. As businesses pirouette between compliance and expansion, the costs ripple through the interconnected fabric of this digital world. Moreover, data localisation frustrates Internet Giants' access to the best-talented employees because it disrupts the global flow of relevant human resources data (CIPL, 2023, p. 7), which deteriorates the efficiency of the global workforce.

Data localisation by the physical placement of servers and other infrastructure within the state's territory invokes a danger to national security in the context of armed conflicts. The military targeting of national cyberspace infrastructure might damage the state's data establishments. It should be noted that in the context of geopolitical tensions and the imminent threat of Russia's invasion in February 2022, the Ukrainian government proactively addressed data security vulnerabilities. Before the invasion, Ukrainian legislation mandated data localisation - requiring certain government and private sector data to be stored within the country's borders. Recognizing the risks posed by physical attacks on localized servers, the Ukrainian parliament swiftly enacted new legislation (CIPL 2023, p. 9). This legislative action allowed critical data to be moved to cloud-based infrastructure.

[20] Goujard, C., Elon Musk's X under fire over harvesting users' data to train AI chatbot (Politico on 26 July 2024) https://www.politico.eu/article/elon-musks-x-under-fire-over-harvesting-users-data-to-train-ai-chatbot/ accessed on 31 July 2024.
[21] The Costs of Data Localization (TechWonk Blog on 17 August 2016) https://www.itic.org/news-events/techwonk-blog/the-costs-of-data-localization accessed on 27 July 2024.
[22] https://trade.ec.europa.eu/access-to-markets/en/content/general-agreement-trade-services-gats accessed on 27 July 2024.

The Ukrainian government securely transferred essential information related to government operations, taxation, banking, education, and property by collaborating with private cloud service providers. Rather than relying solely on in-country servers, this strategic move ensured that critical data was distributed across global cloud networks, mitigating the risk of disruption or destruction. Therefore, the physical localisation of data does not suffice to protect the integrity of national data but, on the contrary, utilizing a globally distributed network of cyberspace infrastructure provides data with a more effective protection against intentional and nonintentional cyber threats.

The Indispensability of Data Localisation

Despite the several deficiencies of data localisation, highlighted by Internet Giants, the contemporary status of cybersecurity proves the indispensability of adopting localisation policies to secure national data and the performance of critical services utilizing cyberspace.

The primary advantage of national cyberspace data routing is that data remains within the country's borders, avoiding foreign wires and servers (Baur-Ahrens, 2017, p. 45), and hindering foreign authorities' attempts to intercept, read, or manipulate the data. Thus, states employ data localisation to defend the citizenry's privacy against various cyber threats. Nevertheless, a frequently cited disadvantage is the potential decrease in data traffic quality, as nationally routed traffic is more prone to overloads and congestion. Additionally, this approach may prevent access to alternative routes that could enhance failure safety and reliability (Baur-Ahrens, 2017, p. 45). Nonetheless, those technical deficiencies do not undermine the functionality of Internet infrastructure domestic localisation in preventing the negative impacts of outages caused by foreign technical failures. The restricted access to sensitive data decreases the potentiality of misusing them either by national or foreign entities, solidifying therefore the protection of national data.

Furthermore, data localisation protects states against foreign data mining operations. It is known that storing national sensitive data in servers placed on foreign soil facilitates accessing this data by the host government. As declassified by Snowden,[23] the US National Security Agency (NSA) collaborated with Internet Giants to execute data mining plans that target Internet users' data stored in servers within the US territory. This incident invoked national security concerns as motivation to adopt data localisation policies. There is an argument that the unrestricted flow of data to hostile or authoritarian regimes threatens the national security of their geopolitical adversaries (Sheppard et al., 2021, p. 5). For example, the US and India resist Chinese endeavours to access their databases. Also, in the Middle East, Arab states and Israel do not welcome mutual access to national data in cyberspace. Therefore, data localisation is a mere evolution of the theory of national security. Additionally, data localisation measures can discriminate between domestic and foreign platforms, giving domestic platforms certain advantages or protection (Han, 2024, p. 266). Regarding global geopolitical rivalries, data has become a fierce weapon affecting the states' capabilities and determining their actual power (Han, 2024, p. 270). This fact elevates data localisation to be the appropriate instrument to maintain the inter-state balance concerning technological superiority and its impacts on national security and manage the cosmopolitan scheme of international relations with respect to political economy and technology. Furthermore, data localisation can boost the competitiveness of domestic platforms by helping them become familiar with data regulations in other states, allowing them to adapt more easily (Han 2024, p. 266). Adaptability is crucial to national security since it enables foreign entities to comply with domestic regulations which enhances their contribution to domestic society.

[23] Edward Snowden: whistle-blower behind NSA surveillance revelations (The Guardian on 09 June 2013) https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, accessed on 23 July 2024.

The global support of data localisation is well recorded. As of June 2023, approximately three out of four surveyed internet users worldwide expressed support for data localisation. Statistics reveal that 76% of Internet users support governmental domestic data localisation plans this year[24]. The powerful existence of governments in cyberspace increases Internet users' online safety, particularly considering the open nature of cyberspace. Moreover, International agreements, e.g., GATS, permit states to adopt the appropriate policies to protect important national data (Yoshinori, 2021, p. 21) contrary to the general principle of free cross-border flow of data as these agreements should never deprive states of the natural right to defend their sovereign interests.

Accordingly, Internet Giants must construct local data servers within states to comply with the national localisation requirements (Han, 2024, p. 266). This provides Internet users within a state with a complete version of their data exchanged on a given platform, which prevents the effects of foreign outages. A major factor that escalated the impacts of the CrowdStrike outage was the ultimate reliance on the tech company's capabilities and neglect to establish a national system of cyberspace infrastructure, regardless of its actual location. Thus, states should reconsider their overreliance on tech companies to maintain the functionality of critical national services.

A motivation that drove Egypt to construct its national cyberspace server center thus an outage of a centralized data server, like the CrowdStrike outage, would never affect the efficiency and functionality of national services. Each state should favour a localisation approach to achieve this objective according to its national perception. Therefore, it could be asserted that the negative global impacts caused by the CrowdStrike outage are a direct result of the anarchic unorganized system of information stored in cyberspace as elaborated on by Han (2024, 269) because when a state depends solely on a foreign enterprise to store national data within its servers, regardless of their location, the technical failures of these servers should logically deprive the state of its data leading to a complete denial of critical services, e.g., air transports and healthcare, which constitutes a major threat to national security.

Conclusion

Through a theoretical methodology, the research discussed the problem of cyber outages caused by foreign technological failures based on an incident that occurred in the real world which is the CrowdStrike outage. The severity of this outage's consequences on global services and states' national security invoked the urgent need to find a solution that prevents similar future incidents. Because of the foreign reason for the CrowdStrike outage, the research demanded states to localize their data in cyberspace. Data localisation, whether physical or digital, is the solution supported by the research to avoid similar incidents.

The research establishes its endorsement of data localisation on the obvious correlation between the latter and the concepts of sovereignty and territoriality in cyberspace. According to the correlation, data localisation is a logical implication of imposing the state's sovereignty in cyberspace. This conception implies that a state should initiate necessary policies to protect its national security endangered by technical outages. Indeed, the CrowdStrike outage inflicted severe damage to the global economy and states' national security. Therefore, the physical placement of Internet infrastructure or imposing digital sovereignty on data stored abroad manifests an inevitable solution to prevent similar negative impacts. Furthermore, to enhance the research hypothesis, it sheds light on the privileges of data localisation and justifies its indispensability to prevent outages. Since Internet Giants' stance concerning technical issues is authenticated, the research gives their opposition to data localisation considerable attention by refuting their arguments and allegations about it and emphasizing the advantages of data localisation. It is an adequate trade-off that supports the hypothesis.

[24] Petrosyan, A., Global attitudes of internet users toward data localization 2023 (Statista on 16 January 2024) https://www.statista.com/statistics/1441060/attitudes-data-localization-internet-users-global/, accessed on 27 July 2024.

Credit Authorship Contribution Statement

Abdelkarim, Y.A., contributed to the conceptualization, methodology design, data analysis, and manuscript writing of this study. The author conducted a thorough review of relevant literature, formulated the research questions, and analysed the implications of data localisation in the context of the CrowdStrike case.

Conflict of Interest Statement

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

[1] Abbas, A. E., van Velzen, T., Ofe, H., van de Kaa, G., Zuiderwijk, A., & de Reuver, M. (2024). Beyond control over data: Conceptualizing data sovereignty from a social contract perspective. *Electron Markets,* Volume 34, 20. https://doi.org/10.1007/s12525-024-00695-2

[2] Abdelkarim, Y. A. (2024). Demarcation of Cyberspace: Political and Legal Effects of Applying the Concept of Sovereign States' Interests. *Journal of Digital Technologies and Law*, 2 (2), 376–399. https://doi.org/10.21202/jdtl.2024.20

[3] Adonis, A. A. (2023). English School on Cyberspace: Examining the European Digital Sovereignty as an International Society and Standard of Civilization. In: Mazzi, F. (ed.), *The 2022 Yearbook of the Digital Governance Research Group, Digital Ethics Lab Yearbook*, Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-28678-0_7

[4] Baur-Ahrens, A. (2017). The power of cyberspace centralization: Analysing the example of data territorialization. In: Leese, M. and Wittendrop, S. (eds.) *Security/Mobility: Politics of Movement*, pp. 37-56, Manchester University Press. https://doi.org/10.7228/manchester/9781526107459.003.0003

[5] Center for Information Policy Leadership - CIPL (2023). The "Real Life" Harms of Data Localization Policies, *Discussion Paper* No. 1. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf

[6] Duggal, P. (2019). Data Localization: A Review of Proposed Data Localization in India, with Learnings for the United States. *Data Catalyst.* https://datacatalyst.org/wp-content/uploads/2020/06/Data-Localization-Pavan-Duggal.pdf

[7] Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Science Press and Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-0320-3

[8] Han, S. (2024). Data and statecraft: Why and how states localize data. *Business and Politics*, 26, 263–288. https://doi.org/10.1017/bap.2023.41

[9] Hellmeier, M., Pampus, J., Qarawlus, H., & Howar F. (2023). Implementing Data Sovereignty: Requirements & Challenges from Practice, *ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security,* August 29–September 01, 2023, Benevento, Italy, 143, pp. 1-9. https://doi.org/10.1145/3600160.3604995

[10] Hellmeier, M. & von Scherenberg, F. (2023). A Delimitation of Data Sovereignty from Digital and Technological Sovereignty, *Thirty-first European Conference on Information Systems (ECIS 2023)*, Kristiansand, Norway, Research Paper No. 306. https://aisel.aisnet.org/ecis2023_rp/306

[11] Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society.* https://doi.org/10.1177/2053951720982012

[12] Injadat, M., Salo, F., & Bou Nassif, A. (2016). Data mining techniques in social media: A survey. *Neurocomputing.* http://dx.doi.org/10.1016/j.neucom.2016.06.045

[13] Japaridze, T. (2023). Cyber Sovereignty: Should Cyber Borders Replicate Territorial Borders? In: Berghofer J., et al. (eds) *The Implications of Emerging Technologies in the Euro-Atlantic Space*, Springer Nature Switzerland https://doi.org/10.1007/978-3-031-24673-9_13

[14] Kim, N. S. & Telman D. A. (2015). Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent. *Missouri Law Review,* 80(3), 723-770. https://scholarship.law.missouri.edu/mlr/vol80/iss3/7

[15] Lambach, D. (2020). The Territorialization of Cyberspace. *International Studies Review*, 22(3), 482–506. https://doi.org/10.1093/isr/viz022

[16] Medine, D. (2024). Data Localization: A "Tax" on the Poor, Center for Global Development Working Paper No. 674. https://www.cgdev.org/sites/default/files/data-localization-tax-poor.pdf

[17] Salamatian, S., Douzet, F., Salamatian, K., & Limonier, K. (2021). The geopolitics behind the routes data travel: A case study of Iran. *Journal of Cybersecurity*, Volume 7, Issue 1. https://doi.org/10.1093/cybsec/tyab018

[18] Sheppard, L. R., Yayboke, E., & Ramos, C. G. (2021). The Real National Security Concerns over Data Localization. *CSIS BRIEFS*. https://www.csis.org/analysis/real-national-security-concerns-over-data-localization

[19] Simmons, B. and Hulvey, R. (2023). Cyber Borders: Exercising State Sovereignty Online. *Temple Law Review,* 95, 617–640. https://scholarship.law.upenn.edu/faculty_scholarship/3158

[20] Tsagourias, N. (2018) Law, borders and the territorialization of cyberspace. *Indonesian Journal of International Law*, 15(4), 523-551. http://dx.doi.org/10.17304/ijil.vol15.4.738

[21] von Heinegg, W. H. (2013). Territorial Sovereignty and Neutrality in Cyberspace. *International Law Studies*, 89, 123-156. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1027&context=ils

[22] Wu, E. (2021). Sovereignty and Data Localization. *The Cyber Project,* Belfer Center for Science and International Affairs. Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf

[23] Yoshinori, A. (2021). Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures? *Public Policy Review*, 16, 5. https://www.mof.go.jp/english/pri/publication/pp_review/ppr16_05_02.pdf

[24] Zekos, G. I. (2022). Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-94736-1

[25] Zinovieva, E. (2024). Evolution of the Concept "Territorial Sovereignty" in the Digital Age. In: Bolgov, R. et al. (eds.), *Proceedings of Topical Issues in International Political Geography (TIPG 2022), Springer Geography*, Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-50407-5_15

Cite this article

Abdelkarim, Y. A. (2024). Exploring the preventive contribution of data localisation against information technology outages: The CrowdStrike case. *Journal of Research, Innovation and Technologies*, Volume III, 2(6), 95-107. https://doi.org/10.57017/jorit.v3.2(6).01

Article's history:

Received 1st of July, 2024; Revised 25th of July, 2024;
Accepted for publication 20th of August, 2024; Available online: 27th of August, 2024
Published as article in Volume III, Issue 2(6), 2024