Assessing SSL/TLS Certificate Centralization: Implications for Digital Sovereignty

Andrei Cordova Azevedo[1], Eder John Scheid[1],
Muriel Figueredo Franco[2], Lisandro Z. Granville[1]

[1]Institute of Informatics (INF), Federal University of Rio Grande do Sul (UFRGS)
[2]Federal University of Health Sciences of Porto Alegre (UFCSPA)
Porto Alegre, Brazil
{acazevedo,ejscheid,granville}@inf.ufrgs.br, muriel.franco@ufcspa.edu.br

GLOBECOM 2025 - 2025 IEEE Global Communications Conference | 979-8-3315-7781-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/GLOBECOM59602.2025.11432644

***Abstract*—SSL/TLS is a fundamental technology in the network protocol stack that enables encrypted data transmission and authentication of web domains. However, the current model relies on a small number of Certificate Authorities (CAs) to provide and validate certificates, thus creating a highly centralized ecosystem. In this paper, we analyze the degree of centralization of certificate provisioning from CAs in two major political groups: Brazil, Russia, India, China, and South Africa (BRICS) and the European Union (EU). We have found that over 75% of certificates for both BRICS and EU domains originate from CAs based in the United States, indicating possible risks to their digital sovereignty due to the high level of external dependency. This indicates the need for nations within those groups to research alternatives to reduce the high level of dependency on foreign CAs and increase their digital autonomy.**

***Index Terms*—Digital Sovereignty, Network Analysis, SSL/TLS, Network Measurement, Digital Certificates**

I. Introduction

The increasing centralization of services and infrastructure underlying the digital realm has become a topic of growing interest in recent years, due to the possible impacts that such a characteristic can bring upon the digital sovereignty of nations [1]. This discussion gained traction in the political sphere in the European Union (EU) and the intergovernmental organization of Brazil, Russia, India, China, and South Africa (BRICS), especially after Edward Snowden reported a mass surveillance program from the United States, leading to governmental initiatives to protect its citizens' data from external actors and ensure privacy [2].

Digital sovereignty relates to several layers, ranging from subjects such as data regulation, portability, and transfer to geopolitical aspects, including trade dependence and sustainability [3]. Network sovereignty is one of its pillars, which may include elements of traffic centralization, interoperability, neutrality of communication, hosting of critical services, and dependence of manufacturers in infrastructure [4].

Secure Socket Layer (SSL), a security protocol that was designed to ensure privacy and encryption in network communication, is one of the key technologies behind services provided to end-users in the layers of the conceptual framework of network sovereignty in the OSI model, as depicted in [3]. It evolved into a more robust protocol known as Transport Layer Security (TLS), which fixes some of the existing vulnerabilities in the SSL protocol while maintaining key features such as encrypted communication channels [5]. Most popular web browsers only recognize a select number of Certificate Authorities (CAs), leading to a concentration of certificate provisioning in the hands of a few responsible companies. This trait has also increased in the last few years, with a reduction in the mean chain of trust length, suggesting that certificate provisioning is becoming more dependent on fewer CAs [6].

Disruption of the chain of trust from SSL/TLS CAs can lead to an outage of important and popular websites, as well as critical electronic-Government (e-Gov) services, as observed in the Russia-Ukraine conflict, which provoked sanctions by Western countries, triggering mass SSL/TLS certificate revocation for Russian domains and leading the Russian government to create its own CA. [7].

In this paper, we propose an approach for the analysis of SSL certificates to verify the level of centralization of CAs for certificate provisioning, in order to evaluate its possible impacts on digital sovereignty and provide insights to foster the discussion on network sovereignty based on the SSL context. The main contributions of this paper are as follows:

- Present an approach to analyze the centralization of SSL/TLS certificate provision;
- Provide a solution to gather information from certificate chains of domains belonging to a specific region;
- Analyze the current scenario of SSL/TLS certificate provision centralization in countries from the EU and BRICS using the proposed metric.

The remainder of this paper is structured as follows. In Section II, we provide an overview of background knowledge and examine related work on digital sovereignty and SSL/TLS. In Section III, we define our approach to collect data and analyze whether there is centralization in SSL/TLS certificate provisioning, with details on the implementation. Section IV presents our evaluation and analysis of the current scenario, followed by Section V, where we discuss the key findings of our approach. Finally, in Section VI, we present our conclusions and possibilities for future work on the topic.

II. Background and Related Work

This section describes the concept of network sovereignty, outlines current research efforts on the topic, and explores the existing literature related to the analysis of transport and session layer security, specifically TLS and SSL.

A. Network Sovereignty

Digital sovereignty was initially linked to developing the national technology industry to avoid external dependencies and become self-sufficient [8]. Nowadays, it encompasses data flows, privacy, security, and communication protocols [3]. In this sense, the discussion on digital sovereignty became popular due to several data privacy and security incidents, such as the report of the mass surveillance program by the United States (US) [9]. Hence, this boosted the political discourse on the EU and BRICS to perform legal changes ensuring digital autonomy and the protection of national data [10], [11].

One of the key aspects that constitute the digital infrastructure is the network infrastructure and its communication protocols [12]. They are related to the control and governance of data flows, thus being fundamental to the topic of digital sovereignty as they dictate the autonomy over national data and critical services. [4] discusses how network sovereignty is related to the dependency of single manufacturers, as simultaneous failures of them could cause disruption of the network. It proposes a metric for evaluating network sovereignty based on the diversity of manufacturers involved in the network path between source and destination addresses. Yet, only a few works [3], [13] explore the network protocol stack and investigate its possible impacts on digital sovereignty, such as the DNS protocol. It investigates and maps internet domain names to their Authoritative Name Servers (NSes) and the organizations behind them, determining the country/region of the Autonomous Systems (AS) that operate those NSes, with results showing, among other findings, that most of the top-10 DNS providers are from the US. This brings attention to the necessity of further investigation on the topic, addressing other network protocols for analysis.

B. Transport and Session Layer Security

SSL/TLS ensures secure and encrypted data transmission, being fundamental to several services such as online banking, Electronic e-Gov services, and secure email transmission. [14] analyzes possible security issues due to the dependency on the current model of CAs, highlighting issues within the model design and implementation that relate to certificate revocation and governance of CAs. [15] explains how the mechanisms of authentication for SSL/TLS based on this CA model depends on the trustworthiness of a CA provider and addresses possible issues based on the dependency of these companies and government institutions for attesting the identity of SSL service providers.

[16] proposes an alternative using a blockchain-based model for certificate issuing and revocation while also increasing security, thus providing greater transparency of certificate validation, since they would need to be validated by a majority of trusted nodes in order to be accepted in the certificate chain. [17] discusses a possible attack on SSL where government authorities could compel CAs to emit false certificates, leading to unsecured and unencrypted communication. Thus, it highlights the possible impacts that depending heavily on foreign CAs can have. [18] performs a study of invalid SSL certificates across the web, showing that most of them originate from end-user devices that reissue new invalid certificates, but it does not perform an analysis of the possible impacts that they present to the digital sovereignty of a nation.

In the current literature, there seems to be a gap in the research on the level of dependency on foreign CAs for certificate provisioning and mapping its possible impacts on digital sovereignty. Our approach aims to fill the existing gap in the current literature by analyzing the centralization of CAs and certificate provisioning for the SSL/TLS protocol, a key technology of the network stack, and the impacts of such characteristics on digital sovereignty.

III. Measurement Approach

The approach is based on collecting popular Internet domains from countries belonging to the EU and BRICS and fetching their certificate chain to inspect characteristics such as *(i)* the organization that issued the certificates (i.e., the Certificate Authority (CA)), *(ii)* the certificate issuers' countries of origin, and *(iii)* both start and expiration date for each certificate. Table I presents sample data collected from a domain obtained from the list of popular internet domains.

TABLE I: Certificate Information Example

Data Type	Example
Domain	`www.wikipedia.org`
Subject	`CN=*.wikipedia.org`
Issuer	`CN`=DigiCert TLS Hybrid ECC SHA384 2020 CA1 `O`=DigiCert Inc `C=US`
Serial	7f2f35c87a877af7aefe947993525bd
Not Before	2021-04-14 00:00:00
Not After	2031-04-13 23:59:59

The subject field identifies the entity that owns the certificate. It can contain information such as the Common Name (CN), representing the domain name of the entity; Organization (O), to identify the organization that holds the certificate; and Country (C), for the country of the entity. The *Issuer* field represents the CA that issued the certificate, and contains the same fields: CN, for the name of the CA; O, for the CA organization; and C, for the country of origin of that CA. *Serial* is a unique identifier for the emitted certificate within the responsible CA, and it ensures that a certificate can be tracked and revoked individually. *Not Before* and *Not After* fields define, respectively, the earliest date and time when the certificate becomes valid, and the latest date and time that a certificate should be considered valid. After this period, a certificate can no longer be considered as trusted.

Figure 1 depicts a sample of the SSL/TLS certificate ecosystem using popular website domains.

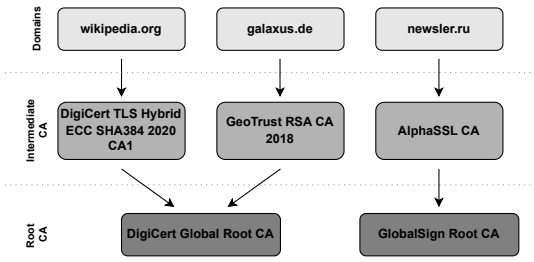

Fig. 1: SSL/TLS Certificate Chain Example

Each HTTPS domain should present an SSL/TLS certificate, which is the leaf certificate. It is issued to a website through an Intermediate CA and contains information about the server's public key and the owner of the server, and it is signed by a trusted root CA, forming a verifiable trust chain.

The defined approach presented in this section allows us to analyze the overall status of centralization of SSL/TLS certificate provision for domains in the political blocks of BRICS and EU, and to further investigate its possible impacts on the network sovereignty of the countries that compose them. Figure 2 depicts the framework of the proposed methodology.

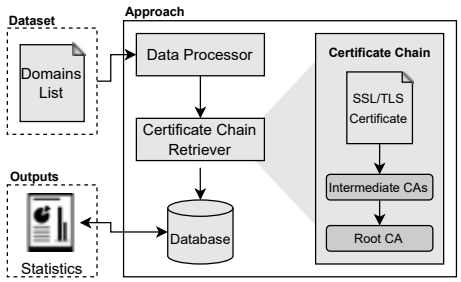

Fig. 2: Overview of the Approach

The first step of Figure 2 consists of obtaining a list containing popular domains from countries within those political blocks. These types of lists are commonly used in research to perform measurements of the web and to evaluate prototypes [19], [20]. The second step encompasses obtaining the chain of certificates from each domain in the list of popular websites and storing this data. After processing the list of domains and storing their certificate chains, statistics can be retrieved from the data obtained.

The implementation of the proposed framework and the results of the evaluation performed are publicly available at https://github.com/andrei-azevedo/ssl-centralization-analysis. In our solution, we relied on the Chrome User Experience Report (CrUX) dataset, which contains the top million most popular websites reported by Google Chrome [21]. Although there are other lists (*e.g.*, Alexa Top Million and Tranco Top Million), the CrUX list seems to be the most accurate for assessing web popularity [19]. To retrieve the certificate chain from domains, our solution creates a socket connection to each of them through the SSL Python library, which allows us to access SSL/TLS encryption and certificate facilities. A mechanism of retry is implemented in case any error occurs during the certificate retrieval. If the errors persist, then the domain gets excluded from the final database.

IV. Evaluation and Analysis

The measurements were performed considering the CrUX dataset from February 2025. In total, we have analyzed approximately 232,490 domains from both BRICS and EU out of a total of 851,793 domains from the dataset, obtained after filtering the ones that were inaccessible or unresponsive. This represents approximately 16% of EU domains and 10% of BRICS domains. From those, 214,282 certificates were obtained successfully for analysis.

A. Geographic Concentration of CAs

Tables II and III summarize, respectively, the Top-5 countries of origin of root certificates obtained for the BRICS and EU domains.

TABLE II: Top-5 Root CAs for BRICS

Country	Root CAs
US	63
BR	27
RU	12
BE	9
GB	9

TABLE III: Top-5 Root CAs for EU

Country	Root CAs
US	68
PL	17
FR	16
ES	13
DE	12

In both, there is a clear concentration of US-based CAs, demonstrating that there are few key responsible companies for the ecosystem, as discussed in [6].

Figures 3 and 4 demonstrate the Top-5 countries of CAs that issue SSL certificates for domains from BRICS and EU, respectively.

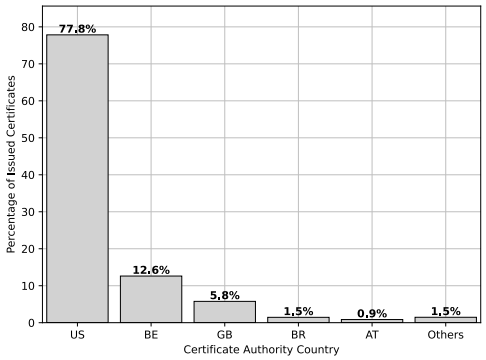

Fig. 3: Top-5 Countries Issuing SSL Certificates for BRICS Domains

The results indicate an extremely high concentration of certificate provisioning for domains in both BRICS and the EU from CAs hosted in the United States (US), being responsible for 77.8% and 75.9%, respectively. This characteristic is in accordance with other protocols previously investigated in the literature, such as DNS providers [3] that are also highly concentrated in the US.

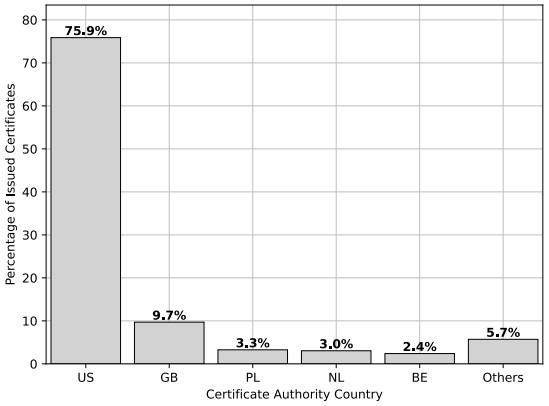

Fig. 4: Top-5 Countries Issuing SSL Certificates for EU Domains

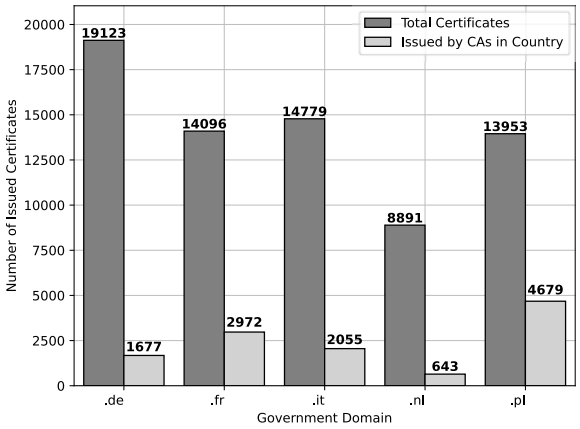

Fig. 6: Certificate Issuing in EU countries

B. Analyzing Digital Sovereignty

Figures 5 and 6 provide more in-depth insight into the distribution of SSL certificate issuances within BRICS and EU countries, as well as in-group certificate issuance.

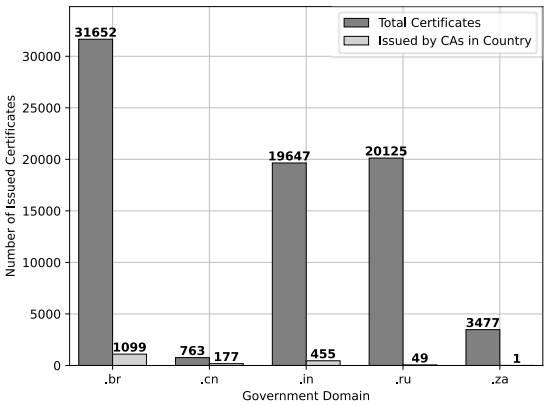

Fig. 5: Certificate Issuing in BRICS Countries

Brazil presents the most certificates among BRICS (31,652 certificates). Yet, only 1,099 were issued inside the country, representing 3.47% of the total amount. This low in-country certificate issuing is seen in other BRICS nations, such as India (2.32%), Russia (0.24%), and South Africa (0.02%). The biggest discrepancy is in China, with 23.20% of the certificates from domains in the dataset being issued in the country.

It is possible to see that, for the top-5 countries with domains present in the dataset, the EU presents a higher level of in-country certificate issuing. Poland and France show the highest percentage, with 33.53% and 21.08%, respectively, while the lowest is in the Netherlands with 7.24%.

C. Certificate Validity Ranges

The validity period of certificates plays a key role in the availability, reliability, and security of domains. It directly impacts the frequency of the renewal process, the potential for disruption of services, and outdated data encryption, thus posing a concern to the digital sovereignty of a nation. Figure 7 depicts the current scenario of certificate issuing by company and validity range.

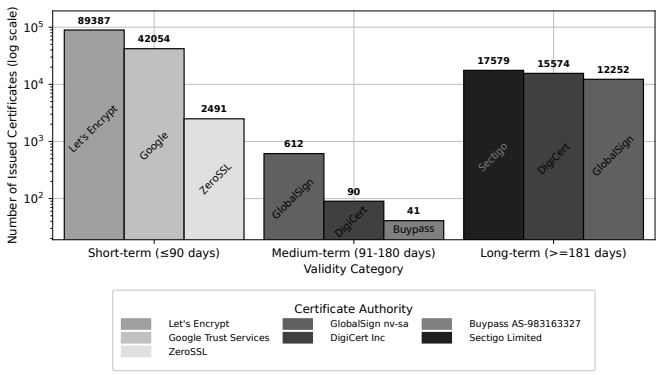

Fig. 7: Certificate Validity Range in BRICS and EU

Let's Encrypt is the most dominant provider, possibly due to its characteristics, being a free CA that issues certificates with a 90-day validity period to encourage automated renewal practices [22], [23]. It is followed by Google Trust Services and ZeroSSL in short-term certificates. As they are free of fees and offer an automated renewal process, they are more accessible and thus widely popular than other CAs across the internet. Enterprise-grade certificates with longer validity and additional security features are often adopted by big enterprises and government sectors due to regulatory and compliance requirements, in addition to complex IT infrastructure. Further, Figure 7 reinforces that the certificate ecosystem is dominated by a few key CAs. In total, 180,080 certificates are represented by seven unique CAs, accounting for 84% of the 214,282 collected certificates, thus indicating a clear over-centralized environment for certificate issuing. This raises concerns about the digital sovereignty of analyzed regions, as disruption of services from these dominant CAs

due to errors, revocation policies, or even regulatory actions could affect a great amount of both BRICS and EU domains.

In this evaluation, we have focused our analysis on leaf certificates emitted for the domains and their CA. Thus, we have not thoroughly investigated the characteristics of intermediate and root CAs, leaving it as an opportunity to extend this work in the future.

V. Discussions and Key Observations

Several insights can be obtained from the experiments performed in this work. It was possible to observe that SSL/TLS certificate provisioning is highly centralized, with most certificates in both BRICS and the EU being issued by CAs based in the US.

A. Impacts of SSL/TLS Centralization

Although there is a clear sign of centralization in certificate provisioning, this characteristic is not inherently bad. Most popular browsers, such as Mozilla's, have a strict policy of security audits to validate and recognize CAs [24]. Moreover, trusting a malicious CA could cause severe impacts on the Web PKI, allowing the possibility of intercepting communication between a user and the web server [25]. Popular major CAs, such as Let's Encrypt, tend to be in accordance with security protocols and best practices to ensure a high level of adoption and to be fully trusted by popular web browsers.

Another aspect is that, as depicted in Section IV, the most popular CA in both BRICS and the EU is a company that provides free certificates with an automated renewal process. Other large commercial CAs usually charge fees for issuing premium certificates, often used in websites that contain sensitive data or payment systems due to their increased security. Further, nations may lack the necessary means to invest in or build their own secure and widely accepted CA infrastructure, thus leading to this external dependency on foreign CAs due to economic reasons.

Yet, this dependency on a small set of CAs increases the chances of geopolitical risks, as depicted in Section I. Another example is the case of *DigiNotar*, a popular Dutch CA that suffered a security breach, allowing attackers to perform Man-in-the-Middle attacks, a popular form of communication interception in SSL/TLS protocol [26], leading the Dutch government to find alternative CAs. Thus, relying heavily on a small set of CAs subjected to the possibility of cybersecurity threats, can endanger the security and sovereignty of a nation.

B. Concerns and Alternatives

With the increasing political tension between the US, EU, and nations in BRICS, more cases of SSL/TLS certificate revocation could be provoked by sanctions. The creation of national/regional CAs from impacted countries could lead to their isolation from the global web, as they still depend on the trust of popular web browsers.

Recent literature suggests that a possible alternative could be the use of blockchain-based PKI systems, creating a decentralized trust system and reducing the risks of sanction-based certificate revocation and security breaches [16], [27]. Yet, it would also require adopting such systems by existing services and web browsers, which can be difficult due to technical and economic challenges.

Thus, the risks highlighted by the findings in this work need to be addressed while also considering the dual nature of SSL/TLS certificate provisioning centralization. A long-term strategy is required to ensure stability and security over key services and systems that rely on the SSL/TLS protocol.

C. Limitations

The usage of the CrUX dataset has been proven accurate to represent popular domains in recent work [21]. Yet, due to the limitations of China in terms of global internet access, popular Chinese websites might not be accurately captured within CruX, causing a low number of Chinese domains in our dataset. As of February 2025, Chrome presents approximately 44% of the browser market share in China [28]. Although it is very popular, there is still a low amount of statistics in these reports for Chinese domains. Further, the dataset could be improved by fetching popular domains with a more significant representation of websites from EU and BRICS domains, as highlighted in section IV. Future work could investigate if this aspect is also present in other datasets, such as the Tranco list.

It is also important to mention that while trying to retrieve the certificate chain from domains in the dataset, some failed and were not included in the final list. Most of the domains failed due to a `ECONNRESET` error. This occurs when the TCP connection is closed from the server side due to one or more protocol errors. For instance, several errors were due to "*unsafe legacy renegotiation disabled*". This protocol error occurs when the server attempts to use an outdated and insecure TLS renegotiation method. Such a feature is disabled by default in OpenSSL, due to its possible security impacts, as it allows Man-in-the-Middle attacks (CVE-2009-3555). Yet, the list of failed domains only represents, for BRICS and EU respectively, **9%** and **5.2%** of their total domains present in the list and thus does not invalidate the results and contributions provided in this work.

VI. Conclusion and Future Work

This work has analyzed the SSL/TLS certificate provisioning centralization degree and its implications for digital sovereignty in BRICS and the EU. The findings show a significant reliance of nations within those groups on a small set of foreign Certificate Authorities (CAs), with over 75% of certificates in both groups being issued by US CAs. We also show that, in comparison with each other, the EU has a higher percentage of in-group issued certificates than BRICS. Additionally, our analysis also reveals that, even for the first level of certificates in the certificate chain, provisioning is concentrated in a few major companies in both groups, reinforcing the dominance of this small set of CAs in the Web PKI ecosystem. While this centralization is not inherently a bad trait, it can also pose substantial risks related to

geopolitical control, economic dependence, and cybersecurity threats, directly impacting the digital sovereignty of nations.

The cases discussed in this work and the findings highlight that over-reliance on a small set of centralized CAs, especially in the cases of BRICS and the EU, can severely impact their key digital infrastructures and governmental services. Disruption provoked by security issues or political sanctions can lead to a mass revocation of certificates, causing accessibility issues and endangering national security. Regional CAs that comply with global security standards imposed by web browsers and organizations can increase the resilience of nations within such groups. However, they remain dependent on the recognition of popular web browsers, risking digital isolation. This highlights the challenges these groups face, which must try to reduce their dependence on external service providers while maintaining interoperability with the global web. Thus, alternatives should be researched to increase the resilience of their digital autonomy and decrease their dependency on foreign CAs.

Future work could expand the analysis to other levels of the certificate chain, thus investigating the current data in more depth and considering new datasets. Also, it is interesting to address other key network protocols and infrastructure, to provide a better understanding of how different layers of the network stack impact the digital sovereignty of nations and thus provide a foundation for political discussions on digital sovereignty and autonomy.

ACKNOWLEDGMENTS

This work was partially supported by the São Paulo Research Foundation (FAPESP) under grant number 2020/05152-7, the PROFISSA project, and is part of CNPq process 316662/2021-6. It is also part of the INCT of Intelligent Communications Networks and the Internet of Things (ICoNIoT), funded by CNPq (proc. 405940/2022-0) and the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) Finance Code 001 and 88887.954253/2024-00.

REFERENCES

[1] J. Pohle and T. Thiel, "Digital Sovereignty," *Journal of Internet Regulation*, vol. 9, no. 4, pp. 76–88, 2020.

[2] Z. Bauman, D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon, and R. B. J. Walker, "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology*, vol. 8, no. 2, pp. 121–144, 05 2014.

[3] A. Azevedo, E. Scheid, M. Franco, D. Boeira, L. Zembruzki, and L. Granville, "The Role of Network Centralization in Shaping Digital Sovereignty: An Analysis Under the DNS Lens," *International Journal of Network Management*, vol. 35, no. 1, p. e2309, 2025, e2309 nem.2309.

[4] S. Janardhanan, M. Samonaki, P. Einar Heegaard, W. Kellerer, and C. Mas-Machuca, "Network Sovereignty: A Novel Metric and its Application on Network Design," 2024.

[5] S. Turner, "Transport Layer Security," *IEEE Internet Computing*, vol. 18, no. 6, pp. 60–63, 2014.

[6] M. Döberl, Y. F. von Wangenheim, C. M. Bruhner, D. Hasselquist, M. Arlitt, and N. Carlsson, "Chain-Sawing: A Longitudinal Analysis of Certificate Chains," in *2024 IFIP Networking Conference (IFIP Networking)*, 2024, pp. 131–139.

[7] B. Toulas, "Russia creates its Own TLS Certificate Authority to Bypass Sanctions," 2022, https://www.bleepingcomputer.com/news/security/russia-creates-its-own-tls-certificate-authority-to-bypass-sanctions/.

[8] S. Couture and S. Toupin, "What does the Notion of "Sovereignty" Mean When Referring to the Digital?" *New Media & Society*, vol. 21, no. 10, pp. 2305–2322, 2019.

[9] D. Polatin-Reuben and J. Wright, "An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet," in *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)*. San Diego, CA: USENIX Association, Aug. 2014.

[10] L. Belli, "BRICS Countries to Build Digital Sovereignty," *CyberBRICS: Cybersecurity regulations in the BRICS countries*, pp. 271–280, 2021.

[11] L. Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU," *Philosophy & Technology*, vol. 33, pp. 369–378, 2020.

[12] T. Maurer, I. Skierka, R. Morgus, and M. Hohmann, "Technological Sovereignty: Missing the Point?" in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn, Estonia, May 2015, pp. 53–68.

[13] D. Boeira, E. J. Scheid, M. F. Franco, L. Zembruzki, and L. Z. Granville, "Traffic Centralization and Digital Sovereignty: An Analysis Under the Lens of DNS Servers," in *IEEE/IFIP Network Operations and Management Symposium (NOMS 2024)*, Seoul, South Korea, 5 2024, pp. 1–9.

[14] J. A. Berkowsky and T. Hayajneh, "Security issues with Certificate Authorities," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 2017, pp. 449–455.

[15] T. Fadai, S. Schrittwieser, P. Kieseberg, and M. Mulazzani, "Trust me, I'm a Root CA! Analyzing SSL Root CAs in Modern Browsers and Operating Systems," in *2015 10th International Conference on Availability, Reliability and Security*, 2015, pp. 174–179.

[16] Z. Wang, J. Lin, Q. Cai, Q. Wang, J. Jing, and D. Zha, "Blockchain-Based Certificate Transparency and Revocation Transparency," in *Financial Cryptography and Data Security*, A. Zohar, I. Eyal, V. Teague, J. Clark, A. Bracciali, F. Pintore, and M. Sala, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 144–162.

[17] C. Soghoian and S. Stamm, "Certified Lies: Detecting and Defeating Government Interception Attacks against SSL (Short Paper)," in *Financial Cryptography and Data Security*, G. Danezis, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 250–259.

[18] T. Chung, Y. Liu, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, and C. Wilson, "Measuring and Applying Invalid SSL Certificates: The Silent Majority," in *Proceedings of the 2016 Internet Measurement Conference*, ser. IMC '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 527–541.

[19] K. Ruth, D. Kumar, B. Wang, L. Valenta, and Z. Durumeric, "Toppling Top Lists: Evaluating the Accuracy of Popular Website Lists," in *Proceedings of the 22nd ACM Internet Measurement Conference*, ser. IMC '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 374–387.

[20] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczynski, and W. Joosen, "Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," in *Proceedings 2019 Network and Distributed System Security Symposium*. Internet Society, 2019.

[21] Chrome for Developers, "Google Chrome User Experience Report (CrUX)," 2022, https://developer.chrome.com/docs/crux.

[22] F. B. Manolache and O. Rusu, "Automated SSL/TLS Certificate Distribution System," in *20th RoEduNet Conference: Networking in Education and Research (RoEduNet 2021)*, 2021, pp. 1–6.

[23] Let's Encrypt, "90-day Lifetimes for Certificates," 2015, https://letsencrypt.org/2015/11/09/why-90-days/.

[24] Mozilla, "CA Certificate Program," 2025, https://wiki.mozilla.org/CA.

[25] J. Braun, F. Volk, J. Classen, J. Buchmann, and M. Mühlhäuser, "CA trust management for the Web PKI," *Journal of Computer Security*, vol. 22, no. 6, pp. 913–959, 2014.

[26] N. van der Meulen, "DigiNotar: Dissecting the First Dutch Digital Disaster," *Journal of Strategic Security*, vol. 6, no. 2, pp. 46–58, 2013.

[27] A. Yakubov, W. Shbair, A. Wallbom, D. Sanda, and R. State, "A Blockchain-Based PKI Management Framework," in *The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018*, 2018.

[28] StatCounter, "Browser Market Share in China," 2025, https://gs.statcounter.com/browser-market-share/all/china.

All links were visited in March 2025.