International Journal of Legal Information 2024, Page 1 of 11.

doi:10.1017/jli.2024.22

Data Warfare and Creating a Global Legal and Regulatory Landscape: Challenges and Solutions†

Varda Mone*, Sadikov Maksudboy Abdulajonovich**, Ammar Younas***, and Sailaja Petikam****

Abstract

The world is witnessing an increase in cross-border data transfers and breaches orchestrated by State and non-State actors. Cross-border data transfers may lead to friction among States to localize or globalize data and to provide regulatory frameworks. "Data warfare" or information-war operations are often not covered under conventional rules; however, they are categorized as acts of espionage and subject to domestic regulations. As such, the operations are used to achieve a variety of objectives, including stealing sensitive information, spreading propaganda, and causing economic damage. Notable instances of the theft of sensitive information include the recent Bangladesh government website breach, exposing 50 million records, and the Unique Identification Authority of India (UIDAI) website hack.

Regulating the "data war" under the existing principles of international law may be unsuccessful in creating robust international legal frameworks to address the associated challenges. These developments further accentuate the global divide between data-rich regions in the Global North, with strong data protection mechanisms (such as the GDPR and the California Privacy Rights Act), and regions in the Global South, where there is a lack of comprehensive data protection laws and regulatory regimes. This disparity underscores the urgent need for global cooperation for substantial international regulatory mechanisms.

This article examines the complexities surrounding data warfare; it highlights the imperative need for establishing a robust global legal framework for data protection, delving into the concept of data war. It also acknowledges the growing influence of advanced technologies like data computing and mining and their ongoing threats to the fundamental rights of individuals associated with exposed personal data. The authors address the deficiencies in international legal provisions and advocate for a global regulatory approach to data protection as a critical means of safeguarding personal freedoms and countering the escalating threats in the digital age.

Keywords: *Data Warfare*, *Data Protection*, *Privacy*, *Global Cooperation*, *International Legal Frameworks*, *Data Breaches*

† The editor thanks Sandy Hervieux, Head Librarian, Nahum Gelber Law Library, McGill University (Montreal), for her invaluable editorial assistance with this article.

* Assistant Professor, Centre of Excellence in Public Policy, Sustainability and ESG Research, Alliance School of Law, Alliance University, Bangalore, India. Email: vardamone52@gmail.com.

** Senior Lecturer, Tashkent State University of Law, Uzbekistan. Email: maksudsadikov5@gmail.com.

*** Institute of Philosophy, Chinese Academy of Science, Beijing, China, and School of Humanities, University of Chinese Academy of Sciences, Beijing, China. Email: doctorammaryonus@mails.ucas.ac.cn.

**** Professor in Law, Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences (SIMATs), Chennai, Tamin Nadu, India. Email: petikamsailaja.ssl@saveetha.com.

1. INTRODUCTION

The modern digital revolution has enabled the exponential growth of data generation and storage on an unprecedented scale. Digital data about citizens is continuously harvested across the world. This data encompasses confidential personal details as well as information voluntarily disclosed by individuals on numerous digital platforms. The collection of such digital data is often essential to provide personalized services to citizens in their daily lives, be it digital payments, e-commerce deliveries, etc. However, members of the general public have little awareness or recourse regarding the collection, storage, analysis, or use of their data by various State and non-State actors. This data is often collected systematically for objectives beyond simply providing user convenience.[1]

This rapidly proliferating trove of human data has become the new lifeblood of the global digital economy. Much of it is extracted from ordinary citizens who readily give away their data in exchange for free or subsidized online services without much concern for potential misuse or a compromise of their privacy down the line. In the absence of robust legal safeguards, enforcement protocols, and data protection mechanisms, the freely surrendered digital data of Global South citizens has effectively become a kind of "*virtual terra nullius*,"[2] ripe for unhindered digital occupation.

These developments further accentuate the global divide between data-rich regions in the Global North—like Europe, with the General Data Protection Regulation (GDPR), and North America, with laws like the California Privacy Rights Act—and regions in the Global South, spanning Asia, Africa, and Latin America, which lack enforceable laws. Big-tech conglomerates headquartered in the advanced economies of the Global North have rapidly stepped in to fill this vacuum through digital platforms and services offered across continents. These corporations have adopted dual data collection and processing protocols, orchestrating protections for the data of citizens residing in jurisdictions like the European Union (EU) and the United States (US) with enforceable data privacy laws while extracting data from nations lacking data protection laws.[3] They have a targeted approach towards countries of the Global South, with no regard or minimal respect for regulatory frameworks, where user data can be freely and opaquely mined, analyzed, and monetized at their discretionary will.

Technologically advanced nations of the Global North have partnered with Big-tech corporations to promote increased global data flows, often with little consideration for regulatory priorities or privacy protections in the Global South. Their goal is to leverage emerging technologies like artificial intelligence (AI) to stimulate economic growth and technological dominance. However, the agenda of data colonialism[4] spearheaded by Big-tech corporate giants risks infringing on human rights and eroding privacy across the Global South. As data extraction by tech conglomerates spreads from the Global North to the Global South, profound concerns have emerged surrounding violations of citizen privacy and digital rights. This regime of unrestricted data mining has crossed borders with minimal oversight, raising alarm about the potential for systemic rights abuses and the loss of personal liberties in economically disadvantaged regions.[5]

Furthermore, the general lack of cybersecurity infrastructure and the presence of vulnerabilities around national data storage in Southern countries heighten the risks of data theft as well as breaches of citizens' confidential data. This deficiency in cybersecurity capabilities can be attributed to a number of factors prevalent across the Global South. Many developing countries lack the financial resources and technical expertise required to implement sophisticated cyber defenses. They also frequently have more pressing national priorities like poverty alleviation and the provision of basic services, which supersede cybersecurity on the policy agenda. Additionally, there is lower public awareness of and demand for strong data protection in these regions. Weak governance and high levels of corruption

[1] Nigel Clark and Kristin Albris, "In the interest(s) of many: Governing data in crises," *Politics and Governance* 8, no. 4 (2020): 421–31, https://doi.org/10.17645/pag.v8i4.3110.

[2] Authors' own definition: "*virtual terra nullis*" can be defined as unoccupied digital spaces and environments with no established laws, controls, or ownership.

[3] P. Arora, "General data protection regulation—A global standard? Privacy futures, digital activism, and surveillance cultures in the Global South," *Surveillance & Society* 17, no. 5 (2019): 717–25, https://doi.org/10.24908/ss.v17i5.13307.

[4] Densua Mumford, "Data colonialism: compelling and useful, but whither epistemes?," *Information, Communication & Society* 25, no. 10 (2022): 1511–16, https://doi.org/10.1080/1369118X.2021.1986103.

[5] Beata Paragi, "Digital4development? European data protection in the global South," *Third World Quarterly* 42, no. 2 (2020): 254–73, https://doi.org/10.1080/01436597.2020.1811961.

https://doi.org/10.1017/jli.2024.22 Published online by Cambridge University Press

also undermine cyber readiness as funds intended for digital infrastructure development may be misused. The combination of these financial, technical, and institutional limitations puts national data systems in much of the Global South at heightened susceptibility to cyber intrusions. Addressing gaps in cybersecurity thus requires not just technical fixes but broader economic and policy reforms tailored to local contexts across the developing world.[6]

The insufficient legal safeguards around data in much of the Global South have already enabled numerous instances of large-scale data exploitation and breaches of human rights by both State and non-State actors. For instance, technology companies such as Cambridge Analytica have faced widespread allegations regarding the illegal harvesting of citizens' social media data to psychologically profile electorates and potentially manipulate voting patterns across various countries.[7] Similarly, Chinese technology conglomerates and government bodies have encountered numerous accusations that they are mining facial recognition and biometric data under the auspices of centralized social credit systems within China as well as abroad.[8] Reportedly, this data is being utilized to train advanced, potentially rights-violating AI systems for multiple applications.[9]

Clearly, while representing scientific progress, these technologies could enable mass surveillance and techno-authoritarian overreach if employed by corporations and governments without appropriate transparency, oversight, and adherence to ethical codes. Moving forward, the onus lies on both national regulatory bodies and international institutions to investigate claims of the unauthorized use of private data, as well as to enact evidence-based policy measures to encourage technology innovation while safeguarding consumer welfare and civil liberties. These are examples depicting the absence of robust legal safeguards compromising the fundamental constitutional and human rights of ordinary citizens across the Global South.

In recent years, emerging powers such as India and China have actively championed data localization, sparking debates between the Global South and North over data sovereignty amid rapid digitalization. Global tech conglomerates have enticed developing countries with promises of economic gains through the extensive mining of citizens' personal data.[10] Consequently, the potential for heightened "data warfare" between Southern and Northern countries has grown significantly, with allegations of State-sponsored hacking, cyberattacks, and misuse of sensitive data. For instance, recent instances suggest sophisticated nation-State espionage[11] campaigns targeting healthcare organizations, election infrastructures, and core government departments in rival countries.[12] The techniques employed range from phishing attempts to compromise critical databases, to spreading misinformation across public and social media to influence political processes.

This burgeoning landscape of malicious cross-border data operations challenges existing international legal frameworks centered on norms of territorial sovereignty, non-intervention, and attribution of responsibility. Moreover, the principles governing civilian data protection are being intentionally violated for military advantage, contravening international humanitarian law.[13] As data permeates societies and conflicts, the associated weaponization demands urgent multilateral dialogue addressing pressing questions of privacy, security, and digital rights.

---

[6] Ibid., 254.

[7] Jamie Bartlett, *The People Vs Tech: How the internet is killing democracy (and how we save it)* (London: Random House, 2018), 203–05.

[8] Ira S. Rubinstein, Ronald D. Lee, and Paul M. Schwartz, "Data mining and Internet profiling: Emerging regulatory and technological approaches," *University of Chicago Law Review* 75 (2008): 261–85, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1116728#.

[9] Yongxi Chen and Anne S. Y. Cheung, "The transparent self under big data profiling: Privacy and Chinese legislation on the social credit system," *Journal of Comparative Law* 12 (2017): 356–78, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992537.

[10] D. Svantesson, "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines," OECD Digital Economy Papers, no. 301 (Paris: OECD Publishing, 2020), https://doi.org/10.1787/7fbaed62-en.

[11] Simon Hendery, "Cisco firewalls targeted in sophisticated nation-state espionage hack," SC Media, Apr. 25, 2024, https://www.scmagazine.com/news/cisco-firewalls-targeted-in-sophisticated-nation-state-espionage-hack.

[12] "FBI, CISA, and Partners Release Advisory Highlighting North Korean Cyber Espionage Activity," Cybersecurity and Infrastructure Security Agency (CISA), July 25, 2024, https://www.cisa.gov/news-events/alerts/2024/07/25/fbi-cisa-and-partners-release-advisory-highlighting-north-korean-cyber-espionage-activity.

[13] Makau Wa Mutua, "Savages, Victims, and Saviors: the Metaphor of Human Rights," *Harvard International Law Journal* 42, no. 1 (2001): 201–45, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1525547.

https://doi.org/10.1017/jli.2024.22 Published online by Cambridge University Press

Creative regulatory solutions safeguarding national interests while still encouraging technology innovation could prove essential to stability in this volatile domain.

As aforementioned, the principles governing the protection of civilian data landscapes are being intentionally violated for military gain, contravening international humanitarian law. Parties to armed conflicts are increasingly utilizing adversarial data maliciously to create a disproportionate impact while denying the enemy access to systems that could enable humanitarian relief. Moving forward, the international community must advance nuanced dialogue between States and tech companies to promote ethical norms and confront complex questions surrounding national security, privacy, and digital rights. Creative regulatory solutions safeguarding sovereignty while encouraging technology innovation could prove essential to mitigating emerging data-driven threats. The decentralized nature of such cyber activities often carried out by State proxies transcends conventional conflict thresholds, thereby limiting traditional *jus ad bellum* frameworks reliant on use-of-force principles.[14]

To regulate data warfare, there is a need to look beyond these traditional mechanisms towards alternate pathways offered within international law. As will be discussed later, options such as the regulation of data and attribution of responsibility in case of the unregulated use of data must focus on the wrongful act doctrine[15] to provide more flexible avenues for affected States to respond to and deter harmful data operations.

Simultaneously, the uneven concentration of advanced cyber capabilities in the hands of select Global North countries has exacerbated vulnerabilities across emerging digital economies in the Global South, which face systemic data protection gaps. This underscores an urgent need for international regulations that prioritize citizen rights and State and non-State responsibilities regarding cyberspace usage. The upcoming sections will delve into these concerns of rights preservation and equitable rule-setting that underpin policy responses to the rising global threat posed by uncontrolled data warfare.

The current imbalance of power around global data flows has its roots in the history of colonialism. Global South countries focusing on basic developmental priorities have been comparatively slow to institute holistic data protection frameworks in the rapidly evolving digital context. For decades, countries across Asia, Africa, and Latin America have relied on multinational companies for the provision of digital services and infrastructure. But such overreliance on self-regulation by Big-tech corporates headquartered in North America and Europe has proven profoundly detrimental to upholding the data rights and digital liberties of ordinary Global South citizens.[16]

Technologically advanced countries of the Global North have actively weaponized data globalization trends to concentrate economic and technological power domestically.[17] The presence of dominant technology monopolies and powerful multinational corporations, especially in the Western sphere, has significantly influenced the shaping of digital regulations to serve those entities' continued market interests and expansionist goals. The imbalance enables these large corporate entities to maintain control over global data value chains while restricting oversight of their data-mining activities, especially across the Global South. For example, major US cloud-computing providers could freely access the personal data of software and internet users in India for many years—up until data localization laws mandated domestic data storage and addressed longstanding sovereignty and privacy concerns. However, Northern governments have also been accused of exhibiting digital protectionism through policy lobbying when proposed regulations threaten specific corporate expansion plans. This illustrates the selective and hypocritical use of globalization calls by advanced economies to maintain existing power dynamics that benefit their corporations.

[14] Qifan Wang, "Applicability of Jus in Bello in Cyber Space: Dilemmas and Challenges," *International Journal of Cyber Warfare and Terrorism* 4, no. 3 (2014): 43–62, https://doi.org/10.4018/ijcwt.201407010.

[15] The wrongful act doctrine, also known as the law of State responsibility, is a principle in international law that holds countries accountable for actions that violate international legal obligations. It establishes when a State can be considered responsible for breaching international law and outlines the consequences of such breaches. This doctrine provides a framework for attributing responsibility to States for their internationally wrongful acts, which could include harmful data operations, and allows for legal recourse and potential reparations.

[16] D. Wildi, "Applicability of the Jus in Bello to Cyber Operations Against Civilian Data: A Legal Grey Zone in the Protection of Data," GSI Working Papers 2023/04, Geneva: Global Studies Institute (2023): 1–38, https://archive-ouverte.unige.ch/unige:172625.

[17] D. Anastasiou and R. Schäler, "Translating vital information: Localisation, internationalisation, and globalisation," *Syn-thèses journal* 3, no. 11 (2010): 11–25.

https://doi.org/10.1017/jli.2024.22 Published online by Cambridge University Press

Because of the data protection gaps discussed above, there is a great division in regulatory mechanisms present in the Global South and North. When we discuss relevant institutions, there are two at the international level: the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunications Union (ITU), which are both responsible for policy formation for cyberspace.[18] No Global South nation has meaningful representation in these international bodies, which are dominated by advanced Northern economies. This institutional imbalance has allowed Global North countries to continue furthering their digital, neo-colonial ambitions of data extraction and technological dominance over the Global South through legal as well as extralegal means. The resulting power disparity has deepened the divide between the Global South and North, facilitating a form of digital colonialism. Given these circumstances, it is now imperative to develop a comprehensive global legal framework to address these imbalances and protect the interests of all nations in the digital realm.

Efforts are needed to propose a legal regulatory landscape to minimize gaps in data regulation and data warfare. The current system has enabled powerful technology corporations, predominantly from the Global North, to universally extract data with minimal regulation. This unconstrained data extraction paradigm has profoundly challenged economic justice, eroded national sovereignty, and infringed on core human rights across the Global South. Fundamental reforms are thus direly needed to transform the very foundations that govern global data flows. A new architecture aligning stakeholder priorities and governance with twenty-first-century digital realities can no longer be postponed if the interests of emerging economies and citizens' rights are to be secured within evolving information ecosystems. Through collaborative policy evolution, the interests of both States and technology firms can be balanced with user rights to catalyze equitable growth.

2. Assessing Data Warfare through the Lens of International Law

Recent major data breaches have included the Bangladesh government website breach,[19] the UIDAI website hack,[20] and the 2017 Equifax breach, which compromised the information of 163 million individuals.[21] In 2023, Philippine law enforcement and Indonesia's Directorate General of Immigration also faced breaches, revealing data security vulnerabilities, especially those of government entities.

These incidents indeed underscored data vulnerabilities, especially in the Global South. Moreover, the exponential growth of cross-border data flows, sparked by the digital revolution, has escalated tensions among States advocating for data localization versus globalization through regulatory frameworks. Notably, data warfare operations characterized as espionage fall under domestic rather than international law. However, they are increasingly serving more pernicious goals—that is, enabling information theft, spreading propaganda, and inflicting economic damage.

In essence, high-profile breaches reveal systemic data security issues that particularly affect developing countries. Meanwhile, differing data sovereignty perspectives pit States against one another amid expanding worldwide data transfers. Yet, data operations employed for subversive objectives sidestep international governance despite growing real-world harms. This analysis contextualizes the complex challenges involved in regulating data weapons and warfare on a global scale.[22]

In this context, "data warfare" refers to the use of information and communication technologies (ICTs) by States to manipulate, disrupt, or destroy data systems of other States, organizations, or individuals for political, military, or economic ends. Encompassing activities like hacking, malware attacks, and spreading disinformation, data warfare poses threats to national security alongside human rights and global stability implications. With

[18] Jean-Marie Chenou and Juan Sebastián Rojas Fuerte, "The Difficult Path to the Insertion of the Global South in Internet Governance," in *Internet Governance in the Global South*, ed. David Oppermann (São Paulo: International Relations Research Center, 2018), 42–73, https://tinyurl.com/tuvdzsh5.

[19] Syed Ishtiaque Ahmed et al., "Privacy vulnerabilities in the practices of repairing broken digital artifacts in Bangladesh," *Information Technologies & International Development* 13 (2017): 186–99, https://epublications.marquette.edu/mscs_fac/628.

[20] A. K. Tyagi, G. Rekha, and N. Sreenath, "Is your privacy safe with Aadhaar?: An open discussion," in *Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (IEEE, 2018), 318–23.

[21] Caitlin Kenny, "The Equifax data breach and the resulting legal recourse," *Brooklyn Journal of Corporate, Financial and Commercial Law* 13 (2018): 215–38, https://brooklynworks.brooklaw.edu/bjcfcl/vol13/iss1/10.

[22] Martin C. Libicki, *What is information warfare?* (Washington, D.C.: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 1995), 97.

https://doi.org/10.1017/jli.2024.22 Published online by Cambridge University Press

interconnected digital systems, societies are vulnerable. While international law principles around territorial sovereignty, non-intervention, and State responsibility regulate data operations, limitations exist in applying conventional *jus ad bellum* and *jus in bello* frameworks. Attribution challenges and a lack of cyberattack rules hinder enforcement. Alternative pathways like countermeasures and the wrongful act doctrine need exploration. Ultimately, evolved international frameworks and cooperation prioritizing data protection are critical to counter emerging data warfare threats. Therefore, looking at the applicability of existing international law principles to data warfare can reveal governance gaps that need to be addressed.[23]

A. Applicability of International Law Principles to Data Warfare

The applicability of international law principles, such as non-intervention, territorial sovereignty, and State responsibility, to data warfare presents both challenges and gaps in the current legal framework. The nature of data warfare, characterized by anonymous and covert cyber operations, makes it difficult to attribute State responsibility for these actions. For instance, recent leaks revealed that the US National Security Agency (NSA) hacked international fiber-optic cables to intercept vast amounts of data, including from allied States like Germany.[24] Such inter-State data breaches that have exploited infrastructure vulnerabilities underscore the growing threats tied to data weapons. Yet prevailing juridical ambiguity around transit rights in global digital networks enables States to deny sovereignty infringements. This data targeting through clandestine intelligence programs remains rampant worldwide despite the absence of accountability mechanisms to meaningfully deter extraterritorial surveillance, economic espionage, and unauthorized extraction occurring regularly among State actors. Therefore, the fundamental principles of territorial sovereignty and non-intervention may prove insufficient to address the complex transboundary impacts generated by data warfare operations in the absence of comprehensive reforms. As a result, exploring alternative pathways within international law, such as comprehensive global legal mechanisms and the wrongful act doctrine, may offer potential solutions for addressing State responsibility in the context of data operations.[25] However, comprehensive international legal frameworks that specifically address the various aspects of data warfare, including data protection and privacy, are needed to effectively counter the threats posed by this form of warfare.

1) Principle of non-intervention

The basic premise of international law, the principle of non-intervention that prohibits States from interfering in the internal affairs of other States, faces significant challenges in its application to data warfare.[26] While non-intervention traditionally governs physical military interventions, data operations can still severely impact security and State economies. However, the intangible and interconnected nature of cyberspace makes enforcement and the attribution of State responsibility and accountability difficult because data operations are complex due to the involvement of State and non-State actors. Consequently, traditional notions of sovereignty and non-intervention require careful adaptation to address the distinct challenges posed by this emerging form of intangible, borderless conflict centered around networks and data. Overall, applying principles of non-intervention to data warfare raises complex questions about redefining sovereignty and accountability in cyberspace.

2) Principles of territorial sovereignty

The borderless and extraterritorial nature of cyberspace poses profound challenges for applying principles of territorial sovereignty and State accountability frameworks to data warfare.[27] Traditional conceptions of

[23] Rebecca Crootof, "International Cyber-torts: Expanding State Accountability in Cyberspace," *Cornell Law Review* 103 (2017): 565–644, https://scholarship.law.cornell.edu/clr/vol103/iss3/2.

[24] Susan Landau, *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies* (Cambridge, MA: MIT Press, 2011).

[25] Libicki, *What is information warfare?*, 97 (n 22).

[26] Roxana Vatanparast, "Data governance and the elasticity of sovereignty," *Brooklyn Journal of International Law* 46 (2020): 1–36, https://brooklynworks.brooklaw.edu/bjil/vol46/iss1/1.

[27] Andrew Keane Woods, "Litigating data sovereignty," *Yale Law Journal* 128, no. 2 (2018): 328–406, https://www.yalelawjournal.org/article/litigating-data-sovereignty.

https://doi.org/10.1017/jli.2024.22 Published online by Cambridge University Press

jurisdictional control and authority break down, given the ability of data operations to instantaneously traverse territorial boundaries and involve multiple State and non-State actors simultaneously. The anonymity and deception endemic to the cyber domain further obfuscate the attribution of responsibility. Consequently, existing international law primarily focuses on physical conflicts and has considerable gaps in both regulating and deterring emerging data warfare threats. Effective policy responses necessitate reinforced cooperation to implement alternate governance mechanisms upholding enhanced global data protection standards, redefined principles of sovereignty and accountability, and expanded remedies under international law. News has emerged of Israel imposing digital sieges upon Palestinians by restricting internet access and surveilling activists during military operations.[28] Such weaponization of civilian data infrastructures perpetuates humanitarian crises by severely disrupting essential connectivity and access to aid services for victims of war.[29] This underscores gaps in international law regarding data rights protections for vulnerable groups.

3) Principle of State responsibility as one of the core areas of concern

The principle of State responsibility is one of the core areas of concern, where attribution of responsibility for wrongful State action is complex due to the anonymity and subterfuge intrinsic to cyberattacks that conceal the true perpetrators and their motives. This hinders applying longstanding international law principles centered on State accountability.[30] Established frameworks like *jus ad bellum* and *jus in bello* struggle to adequately regulate data warfare. *Jus ad bellum*, premised on clear armed intervention thresholds, cannot effectively address the ambiguities inherent in data warfare. Similarly, applying *jus in bello* principles becomes challenging due to the fluid nature of data warfare methods and means. Still, alternate governance pathways grounded in the wrongful act doctrine show some promise for addressing attribution challenges.

Overall, the unique nature of data warfare reveals gaps in the international legal system regarding State responsibility, which necessitates the development of novel, cooperative policy solutions tailored to cyber complexity. For enforcement of State responsibility, there must be an effective way forward for data operations. Having analyzed the applicability and limitations of existing international law principles for regulating data warfare, it is pertinent to specifically assess the shortcomings of the conventional frameworks of *jus ad bellum* and *jus in bello*.[31] Examining their deficiencies in addressing data operations can further reveal crucial gaps in the international rules-based order regarding cyberspace governance.[32]

3. SHORTCOMINGS IN THE APPLICATION OF THE PRINCIPLES OF *JUS AD BELLUM* AND *JUS IN BELLO*

The normative framework of *jus ad bellum* governs the use of force, and the framework of *jus in bello* regulates the conduct of parties during armed conflict. These two frameworks have significant gaps in addressing data warfare. The *jus in bello* framework was developed in the context of physical warfare and may not adequately address the unique aspects of cyber warfare and data manipulation. The principles of proportionality, distinction, and necessity, which are central to *jus in bello* may not suit the complexities of data warfare, where the effects and consequences are often intangible and difficult to measure.[33] If data warfare falls into the defined modes of prohibited methods and means of warfare, then the *jus in bello* principle may be invoked, although it is premature to

[28] Mona Shtaya,"Nowhere to hide: The impact of Israel's digital surveillance regime on the Palestinians," Middle East Institute, Apr. 27, 2022, https://www.mei.edu/publications/nowhere-hide-impact-israels-digital-surveillance-regime-palestinians.

[29] Daryna Antoniuk, "Pro-Palestinian operation claims dozens of data breaches against Israeli firms," The Record, Dec. 29, 2023, https://therecord.media/cyber-toufan-data-breaches-israel-iran-palestinians.

[30] Gabor Rona and Lauren Aarons, "State responsibility to respect, protect and fulfil human rights obligations in cyberspace," *Journal of National Security Law & Policy* 8 (2015): 503–30, https://jnslp.com/wp-content/uploads/2017/10/State-Responsibility-to-Respect_2.pdf.

[31] Marco Roscini, "Worldwide Warfare- 'Jus Ad Bellum' and the Use of Cyber Force," *Max Planck Yearbook of United Nations Law* 14 (2010): 85–130.

[32] Jeanette Yau, "The wild, wild web: explaining variation in ASEAN member-state cyber policy" (PhD diss., University of British Columbia, 2022).

[33] Margarita Cisneros, "Cyber-warfare: jus post bellum" (PhD diss., Naval Postgraduate School, Monterey California, 2015).

https://doi.org/10.1017/jli.2024.22 Published online by Cambridge University Press

conclude this. Additionally, in cases of violation, attributing State responsibility for data operations is challenging due to the nature of cyberattacks, which can be launched by non-State actors using intermediary servers and techniques to conceal their origins. The inadequate accounting of data warfare's unique attributes demonstrates the need for evolved global perspectives attuned to the digital domain.[34]

A. *Jus ad bellum*

Traditional international law principles governing the use of force face profound challenges regulating data warfare. This is due to the absence of physical harm that blurs thresholds for defining acts of war, coupled with the intrinsic anonymity of cyber operations, which in turn hinders attribution and accountability. Consequently, established principles of *jus ad bellum* premised on clear aggression identification cannot adequately address the modern intricacies of data attacks. In cases where the State invokes the right of self-defense specified in article 51 of the UN Charter[35] for responding to cyber threats and attacks, clarity is greatly missing.[36] Overall, the intangibility and surreptitious nature of the data warfare domain exposes gaps in existing legal frameworks on proportional defense and State responsibility. Such gaps necessitate developing tailored governance approaches attuned to the realities of inter-State conflict in the digital era.[37]

B. *Jus in bello*

Traditional international humanitarian law principles governing parties' wartime conduct require significant modification to address data warfare contours. Principles of proportionality and distinction premised on delineating civilians from combatants and balancing harm versus military advantage fail, given the interconnectedness and intangibility of the cyber domain where reverberating effects are indeterminate. Attribution challenges further test the application of these principles and undermine accountability. Ultimately, the unprecedented complexities of non-physical data operations expose gaps in established *jus in bello* models suited for conventional warfare but not the surreptitiousness of cyberattacks.[38] Absent updated legal clarification and norms, States are hampered in upholding responsibilities around mitigating civilian harm, escalation control, and restraint in data warfare.

Indeed, applying international principles to data operations may be inadequate, as most instances do not reach the adequate threshold to qualify the situation. It is necessary to assess data warfare's lawfulness beyond these warfare frameworks under principles governing internationally wrongful acts. Victim States also require additional options like comprehensive data protection frameworks beyond self-defense for recourse against data operations.

As such, the limitations of international law principles and traditional frameworks in regulating data warfare point to clear gaps in the current global rules-based order regarding cyberspace governance. Without a specific treaty or international consensus on even defining data warfare, deficiencies exist in establishing legal mechanisms attuned to the digital domain. Therefore, identifying and examining the specific gaps in the existing international law architecture is imperative before calling for urgent global cooperation to formulate substantial regulations and prioritize data protection to counter data warfare.[39]

These gaps in existing international regulations for data warfare underscore the particularly urgent need for a global legal framework that protects vulnerable countries in the Global South. With minimal data protections and recourse mechanisms, developing countries across Africa, Asia, and Latin America are hotbeds for unlawful data extraction and algorithmic human rights violations. Their citizens' data privacy and sovereignty face systemic threats from both Northern State actors and powerful Big-tech corporate conglomerates operating with little oversight. Formulating universal data regulations therefore emerges as an ethical and human rights imperative before

[34] Libicki, *What is information warfare?* (n 22), 74.

[35] Matthew C. Waxman, "Cyber Attacks as 'Force' Under UN Charter Article 2(4)," *International Law Studies* 87 (2011): 43–57, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1075&context=ils.

[36] Charter of the United Nations, June 26, 1945, 1 U.N.T.S. XVI, art. 55.

[37] Michael Walker Brunner, "The Jus Ad Bellum in Cyberspace: A New Framework," *Penn State Journal of Law & International Affairs* 11, no. 2 (2023): 54–95, https://elibrary.law.psu.edu/jlia/vol11/iss2/5.

[38] Wildi, "Applicability of the Jus in Bello to Cyber Operations" (n 16), 3.

[39] Dorothy E. Denning, Information warfare and security, vol. 4 (Boston: Addison-Wesley, 1999).

https://doi.org/10.1017/jli.2024.22 Published online by Cambridge University Press

these Global South vulnerabilities are exploitatively weaponized for economic or geopolitical objectives that further compromise citizens' rights and trust in digital systems.

4. DATA VULNERABILITIES AND PROTECTION GAPS IN THE GLOBAL SOUTH

Data protection and privacy issues have gained critical importance in the digital age with profound global implications. However, discourses surrounding data vulnerabilities and regulatory gaps have predominantly centered on the Global South. Developing robust national and regional regulatory regimes in these regions alongside elevating representation in international governing bodies appears vital to reclaiming lost policy space.

Fundamentally, most Global South countries need to enact data protection laws instituting citizen oversight and consent mechanisms regarding commercial or governmental data collection practices. Reliance on self-regulation by technology firms without public accountability has repeatedly failed citizens, prioritizing corporate interests over digital rights. Insufficient avenues for legal redress against the unauthorized mining of personal data or breaches thereof, further tilts power equations in favor of States and companies.

Moreover, underdeveloped cybersecurity capacities contribute towards heightened data breach risks facing Southern nations already grappling with lax oversight. Even as advancing data localization through indigenous technologies offers promise, holistic policy interventions encompassing legal, socio-cultural, and technical dimensions tailored to local realities are obligatory to truly empower Global South actors in securing data sovereignty. The explicit emphasis should remain on framing regulatory solutions around citizen-centric priorities rather than State or corporate preferences alone.[40]

Only a combination of legal, policy, and socio-technical interventions tailored to local contexts can empower Global South countries to reclaim data sovereignty without compromising citizens' rights and liberties. This mechanism would eventually facilitate the creation of a universal legal framework for data governance and regulation.

5. THE NEED FOR EVOLVED INTERNATIONAL FRAMEWORKS AND GLOBAL COOPERATION

The allegations of large-scale data exploitation leveled at technology giants like Huawei and Cambridge Analytica represent the tip of the iceberg with regard to emerging digital threats.[41] They showcase how, in the absence of robust privacy safeguards, sensitive citizen data can be weaponized by both State and non-State actors to further geopolitical and economic ambitions without oversight. This trend of data weaponization has only accelerated in recent years through dangerous practices grouped under the umbrella term "data warfare."[42]

As described above, data warfare involves leveraging cyber capabilities for offensive operations targeting information systems to achieve political or military objectives. It encompasses State-sponsored threats like spreading manipulated information to incite conflict, compromising critical infrastructure through malware, and stealing confidential data to enable hybrid warfare tactics. The decentralized nature of the internet provides convenient cover for such digital intrusions, with the severe real-world implications often evident much later. Prominent examples include the 2016 Russian information operations' targeting of US elections through Facebook and Twitter and the 2020 APT29 State-backed hacks' exploitation of software vulnerabilities to infiltrate US government agencies.[43]

In addition to strengthening domestic safeguards, the challenges of the digital age necessitate evolved international frameworks and deeper global cooperation to holistically regulate data activities. Progress can be achieved by binding States to collective data protection and privacy standards through multilateral agreements, setting up international compliance mechanisms, and prioritizing equitable representation in global cyberspace governance.

[40] Abu Bhuiyan, "Global South and Supranational Internet Policymaking," in *Internet Governance and the Global South: Demand for a New Framework*, ed. Abu Bhuiyan (London: Palgrave Macmillan, 2014), 1–19, https://doi.org/10.1057/9781137344342_1.

[41] "Emerging cyber threats in 2023 from AI to quantum to data poisoning," CSO Online, Sep. 7, 2023, https://www.csoonline.com/article/651125/emerging-cyber-threats-in-2023-from-ai-to-quantum-to-data-poisoning.html.

[42] Karen E. C. Levy and David Merritt Johns, "When open data is a Trojan Horse: The weaponization of transparency in science and governance," *Big Data & Society* 3, no. 1 (2016), https://doi.org/10.1177/2053951715621568.

[43] US Cybersecurity and Infrastructure Security Agency, "AA22-110A: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," May 2, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a.

https://doi.org/10.1017/jli.2024.22 Published online by Cambridge University Press

The evolving nature of data warfare poses significant challenges to the existing international legal frameworks. These frameworks[44] should focus on enhancing data protection and privacy, establishing norms and rules for responsible behavior in cyberspace, and facilitating effective attribution and responsibility for data operations. Such efforts would require collaboration among States, international organizations, and Big-tech corporations to establish global standards and mechanisms that can effectively regulate and counter data warfare. The establishment of these frameworks and cooperation on a global scale would provide a comprehensive approach to address the complexities and transboundary nature of data warfare, safeguarding the stability, security, and integrity of the international system.[45]

The importance of international cooperation in addressing data warfare cannot be overstated. As data warfare poses unique and complex challenges, a collaborative approach is essential to effectively combat this emerging threat. International cooperation allows for the sharing of information, resources, and expertise, enabling countries to collectively develop comprehensive strategies and policies to address data warfare. Moreover, cooperation promotes the establishment of common norms and standards, facilitating the development of international frameworks for data protection and privacy. Without international cooperation, individual States would struggle to adequately protect their data infrastructure and respond to data attacks in a timely and effective manner, making it imperative for nations to work together in this interconnected digital age.

International organizations can play a crucial role in developing comprehensive frameworks to address data warfare. Organizations such as the UN, the ITU, and ICANN can bring together member States to collaborate on the creation of international standards and norms for data protection and privacy. These organizations can facilitate dialogue, share best practices, and provide guidance on issues related to State responsibility, attribution, and the regulation of data operations. By promoting global cooperation and coordination, international organizations can help fill the existing gaps in international law and ensure a more robust and effective response to the threats posed by data warfare.[46] By fostering cooperation, sharing best practices, and harmonizing laws and regulations, the international community can work towards creating a safer and more secure digital environment.

While building robust national and regional data protection frameworks attuned to local contexts remains a sovereign priority, a balanced global regulatory approach is also crucial to comprehensively address data vulnerabilities. Leveraging collective bargaining power will allow Global South nations to negotiate more equitable data policies with Big-tech firms that dominate the digital landscape. Reducing dependence on foreign infrastructure through investing in local capabilities can mitigate data vulnerability risks. While holistic data protection frameworks are essential, global cooperation beyond national-level action is urgently required for a multifaceted solution to safeguard digital rights. A nuanced combination of local and global action can enable comprehensive protection in the Global South against unlawful data extraction and systemic rights violations.

Deterrent pathways do exist for victim States, including imposing economic sanctions for data privacy violations enabled by a global framework. Yet preventing technology militarization and updating State responsibility require complex multilateral cooperation essential to securing digital citizen rights amidst expanding threats. The lack of legal precedents combined with the interests of powerful State and corporate entities developing cyber arsenals currently obstruct effective rule-setting or enforcement protocols. But continuing inertia risks normalizing chaotic outcomes at odds with global justice and stability. Public debates around humanitarian safeguards along with transparency and confidence-building measures provide initial pathways for guarding common spaces like the internet against predatory forces in the absence of alternatives, buying requisite time for democracies to respond through ethical but pragmatic policies, and balancing requisite security against individual dignities and the collective good.

6. CONCLUSION AND FINAL RECOMMENDATIONS

Data protection and privacy have assumed immense significance in the increasingly digitized global landscape, necessitating urgent policy and legal interventions. This analysis set out to highlight deficiencies in

[44] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

[45] Asaf Lubin, "The rights to privacy and data protection under international humanitarian law and human rights law," in *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives*, eds. Robert Kolb, Gloria Gaggioli, and Pavle Kilibarda (Cheltenham, UK: Edward Elgar, 2022), 463–92, https://doi.org/10.4337/9781789900972.00035.

[46] Ingo Take, "Regulating the Internet infrastructure: A comparative appraisal of the legitimacy of ICANN, ITU, and the WSIS," *Regulation & Governance* 6, no. 4 (2012): 499–523, https://doi.org/10.1111/j.1748-5991.2012.01151.x.

https://doi.org/10.1017/jli.2024.22 Published online by Cambridge University Press

the existing international law architecture regarding comprehensive data governance, using the emergent threat of data warfare as an illustrative case study. The discussions underscored the limitations of traditional *jus ad bellum* and *jus in bello* approaches in regulating malicious data operations, instead arguing for alternative pathways like countermeasures and the wrongful act doctrine. However, the realization of their potential necessitates attribution reforms and evolved perspectives on State responsibility.

The systemic deficiencies in the current international legal order, coupled with localized paradigms that enable unrestrained data exploitation, call for urgent cooperative reforms focused on safeguarding collective rights. A comprehensive global data governance framework grounded in a rights-based digital charter offers the most prudent pathway on this front. Specifically, provisions recognizing citizens' consent and control priorities regarding data trajectories can construct uniform safeguards upholding citizens' rights against State and corporate overreach. Moreover, civil society-led transparency initiatives like solidarity pacts provide indispensable complementary monitoring mechanisms assessing rights implementation, given the realization challenges associated with formal treaties alone.

The intrinsically borderless nature of data flows necessitates collective binding governance standards transcending the pitfalls of fragmented regulatory paradigms that presently permit events within domestic jurisdictions to engender global harms without accountability. Constructing consensus on such a rights-centric framework doubtlessly obliges sincere engagement between multiple stakeholders, including governments, corporations, and technical experts. But the threats posed by unregulated data weaponization can only be deterred through cooperation prioritizing people over profits or power. Core tenets of human dignity and emerging digital rights now stand imperiled across communities worldwide due to unrestrained malign data activities by self-interested State and non-State actors. Therefore, the solutions must be grounded in collective action and centered on ethical data governance and usage paradigms guided by rights-based priorities.

https://doi.org/10.1017/jli.2024.22 Published online by Cambridge University Press