INTERNATIONAL ENVIRONMENTAL LEGAL RESEARCH JOURNAL

VOLUME 3 AND ISSUE 1 OF 2025

INSTITUTE OF LEGAL EDUCATION

INTERNATIONAL ENVIRONMENTAL LEGAL RESEARCH JOURNAL

APIS – 3920 – 0011 | ISSN - 2584-1904

(OPEN ACCESS JOURNAL)

Journal's Home Page – https://ielrj.iledu.in/

Journal's Editorial Page - https://ielrj.iledu.in/editorial-board/

Volume 3 and Issue 1 (Access Full Issue on - https://ielrj.iledu.in/category/volume-3-and-issue-1-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INTERNATIONAL ENVIRONMENTAL LEGAL RESEARCH JOURNAL

VOLUME 3 AND ISSUE I OF 2025

APIS – 3920 – 0011 | ISSN - 2584-1904

Published by

Institute of Legal Education

https://iledu.in

CLIMATE RESILIENCE AND CYBERSECURITY: LEGAL CHALLENGES IN THE DIGITALIZATION OF RENEWABLE ENERGY SYSTEMS

AUTHOR - ATCHAYA A, GUEST LECTURER, GOVERNMENT LAW COLLEGE, TIRUCHIRAPPALLI.

BEST CITATION - ATCHAYA A, CLIMATE RESILIENCE AND CYBERSECURITY: LEGAL CHALLENGES IN THE DIGITALIZATION OF RENEWABLE ENERGY SYSTEMS, *INTERNATIONAL ENVIRONMENTAL LEGAL RESEARCH JOURNAL,* 3 (1) OF 2025, PG. 74-82, APIS – 3920 – 0011 | ISSN - 2584-1904. DOI - https://doi.org/10.65393/WLCA9228

ABSTRACT

The worldwide shift to cleaner energy sources, primarily renewable energy, has not only increased the urgency to fight global warming, but it has also been inextricably linked to the growing use of digital technologies such as Artificial Intelligence (AI), Smart Grids, and the Internet of Things (IoT). The aforementioned technologies have made energy production, its transmission and storage more efficient and flexible. At the same time, the digitalization of renewable energy systems brings in its wake new cyber threats which energy security and climate resilience might be unable to withstand. This article discusses the relationship between cybersecurity and climate resilience during renewable energy transition, illustrating it with technological developments like predictive climate analytics, AI-driven energy optimization, and data-based grid management. It assesses how these technologies render critical energy infrastructure vulnerable to cyber threats, such as grid manipulation, ransomware, and data breaches. By analyzing environmental monitoring platforms and power systems attacks in the real world, the study looks into both emerging threats and the risk of the climate impacting digital infrastructure during severe weather conditions. The legal aspect considers how fit the international and national treaties are in dealing with these intertwined challenges. It mentions the Information Technology Act (2000), cybersecurity regulations for specific sectors, and the work done by NCIIPC and CERT-In, as well as international measures like the Budapest Convention and EU NIS Directive. It points out the regulatory shortcomings related to digital sovereignty, AI-governed energy systems, and transnational data flow in global climate policy. It further analyses the impact of organizations like UNEP, IRENA, and UNFCCC in aligning cybersecurity with climate objectives.

KEYWORDS: Renewable Energy Cybersecurity, Climate Resilience, Smart Grids and IoT, Critical Infrastructure Protection, Digital Sovereignty, AI Accountability in Energy Systems

I. INTRODUCTION:

The global call for climate action has resulted in a drastic shift to renewable energy sources that have never before occurred. This pivotal change, however, will not only contribute but is also strongly linked to the digitalization of the energy infrastructure. The adoption of AI, Smart Grids, and IoT technologies together have changed the very basics of the renewable energy lifecycle – generation, distribution, and storage – and have also promised new heights in efficiency and flexibility[161]. On the other hand, the downside of this digitalization is the emergence of new cyber vulnerabilities that are posing threats to the very infrastructure that is meant to be our defence in the battle against climate change. The same technologies that

[161] UNEP, Clean Energy & Climate Change Convergence (2023); INT'L RENEWABLE ENERGY AGENCY, RENEWABLE POWER GENERATION COSTS IN 2024 (2024).

are speeding up the process of decarbonisation are also the ones paving the way for cyberattacks that could cause energy insecurity and reduce the planet's resilience to climate change. The risks of grid manipulation, ransomware attacks, and data breaches are all still very much real for renewable energy systems, especially given that they are becoming more intertwined with and reliant on digital networks[162]. The intersection between climate action and cybersecurity issues has turned out to be one of the most urgent but, at the same time, least researched areas of global environmental governance. The Budapest Convention on Cybercrime and the EU's NIS Directive, which are both international legal instruments, may be seen as partial help but still not enough. At the same time, the Indian Information Technology Act, 2000, which is an example of national legislation, is very old compared to the current digital ecosystem and has no separate provisions for cybersecurity in digitalized renewable systems[163]. Although the NCIIPC and CERT-In are the regulators that have made institutional efforts, still critical gaps remain concerning cross-border data ruling, responsibility for the AI-controlled systems, and the incorporation of cybersecurity into the climate policy base. This article discusses the various challenges that come along with the intersection of cybersecurity and climate resilience.

II. TECHNOLOGICAL INNOVATIONS AND THE DIGITAL RENEWABLE ENERGY ECOSYSTEM

A. THE CONVERGENCE OF RENEWABLE ENERGY AND DIGITAL TECHNOLOGIES:

In comparison to the global energy market, which is mostly driven by fossil fuels, the solar photovoltaic capacity, wind energy, and battery storage technologies, have been deployed rapidly all over the world, given that they are economically competitive with fossil fuels[164]. Grid integration, efficiency, and scalability of renewable systems are not on the low side anymore, as they are increasingly reliant on digital technologies that were not even thought of when most of the current cybersecurity laws were being drafted. The use of predictive climate analytics allows the very precise forecasting of renewable energy generation patterns. Machine-learning algorithms identify the best places for solar, wind, and storage resources by analysing large amounts of data consisting of solar irradiance, wind speed, and climate development projections, thus enabling better planning and control of the power grid. These systems are able to reduce the uncertainty of renewable energy supply and at the same time, they contribute to the stability of the power grid, thereby making the large-scale integration of renewables economically viable[165]. In the same way, the AI-driven energy optimization has the ability to change the energy distribution continuously in real-time depending on the expected demand, weather conditions, and the situation in the grid, thus leading to less energy wastage and better use of renewable resources.

Smart Grids converge IoT sensors, smart metering infrastructure (AMI), and automated control systems thus forming communication networks with two-way between producers, distributors, and consumers. This design allows for demand-side management, co-location of energy resources, and micro grids that promote resilience through decentralization[166]. Data-centric grid management hinges on the constant checking of thousands of connected devices, gathering and dissecting data in

[162] Dragos, Inc., Critical Infrastructure Cyber Threats in Renewable Energy (2024); Michael Assante & Robert M. Lee, The Industrial Control Systems Cyber Security Program: Stakeholder Perspectives, SANS INST. (2015).
[163] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); Council of Europe Convention on Cybercrime, Nov. 23, 2001, ETS No. 185, 2296 U.N.T.S. 167 [hereinafter Budapest Convention]; Directive (EU) 2022/2555 of the European Parliament and of the Council, Dec. 14, 2022, 2022 O.J. (L 333) 80 [hereinafter NIS2 Directive].
[164] INT'L ENERGY AGENCY, WORLD ENERGY OUTLOOK 2024: GLOBAL RENEWABLE ENERGY EXPANSION ACCELERATES (2024), https://www.iea.org/reports/world-energy-outlook-2024
[165] SAP, THE SMART GRID: HOW AI IS POWERING TODAY'S ENERGY (2021); Verma & Rao, Deep Learning Applications in Decentralized Smart Grid Architectures, 39 J. ADVANCES MATHEMATICS & COMPUTER SCI. 140 (2024).
[166] Id.; see also IRENA, Enhancing Resilience: Climate-Proofing Power Infrastructure (2025), at https://www.irena.org/Publications/2025/Dec/Enhancing-resilience-Climate-proofing-power-infrastructure

INTERNATIONAL ENVIRONMENTAL LEGAL RESEARCH JOURNAL
VOLUME 3 AND ISSUE I OF 2025
APIS – 3920 – 0011 | ISSN - 2584-1904
Published by
Institute of Legal Education
https://iledu.in

terabytes to optimize energy flows, find faults, and avoid cascading failures. Such innovations have changed the game of renewable energy from a support source to a competitive alternative that can even take the baseload demand in some areas. The International Energy Agency estimates that next-generation energy technologies will be a key factor in the creation of carbon-free industries and energy sources by the year 2050[167]. However, this inter-reliance on interconnected networks, software, and data creates huge vulnerabilities to cyber threats that are not covered by the existing legal frameworks.

B. INDIA'S RENEWABLE ENERGY TRANSITION AND DIGITALIZATION IMPERATIVE:

Unprecedented growth has marked India's renewable energy sector. The country has now become among the top generators of renewable energy, largely due to the investment in expanding solar and wind capacities. Nevertheless this rapid deployment has not been followed by equal level of investment in the cybersecurity frameworks that are digitalized renewable systems[168]. Transition to smart grids and advanced digital systems has reduced operating costs and better management of energy, however, they have also made power systems susceptible to cyberattacks that could lead to widespread outages. There is no escape from digitalization requirement. With the rise of renewables and the phasing out of fossil fuels, grid operators will have to depend more on digital systems for stability, forecasting of renewable generation and demand response management. This has resulted in the swift adoption of IoT devices, AI-based control systems, and cloud data management that sometimes lacking the necessary accompanying security measures, thus, creating a window of critical vulnerability during the transition phase.

III. CYBERSECURITY THREATS TO DIGITAL RENEWABLE ENERGY INFRASTRUCTURE

A. CATEGORIES AND MECHANICS OF CYBER THREATS:

The digitalized renewable energy sector has to deal with a variety of cyber threats, and those threats must be analyzed in a categorized way:

Grid Manipulation and Control System Attacks - these attacks go after SCADA (Supervisory Control and Data Acquisition) systems and Industrial Control Systems (ICS) which govern the functioning of renewable power plants and other related entities in power generation. By gaining access to these systems, the culprits can control power generation, change power flows, or cause instability in the frequency of the electricity grid[169]. The case of the 2015 Ukrainian power grid attack is a vivid demonstration of this kind of threat. Attackers employed BlackEnergy malware to gain remote access to SCADA systems, and they seized this opportunity to carry out the opening of breakers at distribution substations in Kyiv and in the Ivano-Frankivsk region, which resulted in power cuts that affected more than 230,000 customers[170]. Planning attacks that involved access to the network for observation and then carrying out the attack for about ten minutes were typical of the attackers who had done the reconnaissance for months, discovering the weaknesses that were critical. Another attack that took place in December 2016 showed that the attackers had gone smarter. The Industroyer malware that they used was able to take down protective relays and could inflict damage when the operators were attempting to restore power[171]. The attackers already knew about the cyber operations' physical impact and were henceforth optimizing their attacks for maximum damage.

[167] INT'L ENERGY AGENCY, DIGITAL INNOVATION IN THE POWER SECTOR (2023).
[168] Ministry of Power, Government of India, Smart Grid Vision & Roadmap for India (2015); CEEW, Making Advanced Metering Infrastructure Resilient: Boosting Cyber Security for India's Electricity Power Grids (2024).
[169] Michael J. Assante & Robert M. Lee, The Industrial Control Systems Cyber Security Program: Stakeholder Perspectives, SANS INST. 1 (2015).
[170] ROBERT M. LEE, MICHAEL J. ASSANTE & TIM CONWAY, THE INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM (ICS-CERT) ADVISORY ON THE 2015 UKRAINE POWER GRID ATTACK 1 (2016); DRAGOS, INC., 2015 UKRAINE POWER GRID CYBERATTACK: ANALYSIS AND INSIGHTS (2019).
[171] DRAGOS, INC., INDUSTROYER (CRASHOVERRIDE): ANALYSIS OF THE 2016 UKRAINE POWER GRID ATTACK 1 (2017).

INTERNATIONAL ENVIRONMENTAL LEGAL RESEARCH JOURNAL
VOLUME 3 AND ISSUE I OF 2025
APIS – 3920 – 0011 | ISSN - 2584-1904
Published by
Institute of Legal Education
https://iledu.in

Ransomware Attacks **-** have progressively targeted/ranged upon critical energy infrastructures. The criminal threat actors in question encrypt and lock the entire data operational, that disables the management of the electricity grid and thus the operators are left with two options either to pay the ransom or to involve the long and costly process of restoring the systems from backups" which could take several days or weeks, during that time period the stability of the grid is at risk[172]. As per the new data 67% of organizations from sectors like energy, oil and gas, and utility, were hit by ransomware attacks in 2024, with a median ransom demand of more than $7 million for the critical infrastructure. The Colonial Pipeline ransomware incident in 2021, even though not directly targeted at the renewable infrastructures, showcased the huge economic and social impact that cyber-attacks on energy systems can cause, and thus the need for a proper on cyber, not only prevention but also timely detection measures.

Data Breaches and Information Theft **-** present unique risks that are particular to renewable energy systems. The operational data generated by these systems is enormous and includes grid vulnerabilities, energy consumption patterns, renewable resource availability forecasts, and personal information of end-users. Theft of this data can support various attacker's goals: tactical intelligence for future attacks, competitive advantage through stolen intellectual property, or even extortion campaigns[173].

Supply Chain Vulnerabilities **-** further aggravate the situation. The renewable energy sector is increasingly relying on global supply chains for its equipment and software. Devices with unnoticeable vulnerabilities or infiltrated software may continually weaken the systems. IoT gadgets are usually very long-lived in their operations but have very little security update periods, hence creating a very long vulnerability time.

B. CLIMATE-RELATED RISKS TO DIGITAL INFRASTRUCTURE:

Apart from cyber security risks digital renewable energy systems, climate change itself presents as a particular threat. This is a vicious circle where the very technologies meant to help the planet cope with the climate crisis end up being susceptible to adverse climate events. Natural disasters such as floods, hurricanes, tornadoes, and heatwaves can damage in a very direct way digital infrastructures ranging from server farms, substations, communication networks, to data centres[174]. The rise in the number of such disasters caused by global warming can lead to scenarios where the interaction of cyber and physical weaknesses results in system failures. When there are natural disasters, the need for energy generally goes up and at the same time, the amount of power that is being generated from wind and solar may decrease significantly causing the situation to be stressful. The digital systems that are controlling this stress become really easy targets for either attack or failure because the operators are being occupied by emergency management which might even lead to security protocols being relaxed for the time being. Data centres and the electronic equipment that facilitates the running of renewable energy systems are greatly influenced by temperature extremes. One of the impacts of climate change, the thermal stress, can lead to the faster deterioration of hardware and hence higher system failure rate.

III. LEGAL FRAMEWORKS - NATIONAL AND INTERNATIONAL ARCHITECTURE

A. THE INDIAN LEGAL FRAMEWORK:

The Information Technology Act, which has been implemented in the year 2000 and it is the primary law of the Indian cybersecurity

[172] FBI & CISA, Ransomware: The Increasing Threat to Critical Infrastructure, JOINT ADVISORY (2021).
[173] RESECURITY, RANSOMWARE ATTACKS AGAINST THE ENERGY SECTOR ON THE RISE: NUCLEAR AND OIL & GAS ARE MAJOR TARGETS IN 2024 (2024); SOPHOS, THE STATE OF RANSOMWARE IN CRITICAL INFRASTRUCTURE 2024 (2024).
[174] IRENA, supra note 6, at 15-22.

INTERNATIONAL ENVIRONMENTAL LEGAL RESEARCH JOURNAL
VOLUME 3 AND ISSUE I OF 2025
APIS – 3920 – 0011 | ISSN - 2584-1904
Published by
Institute of Legal Education
https://iledu.in

system[175]. Sections 70 and 70A, added through amendments, give explicit power to the central government to declare computer resources as "Protected Critical Information Infrastructure," the unauthorized access to which can lead to a prison term of up to ten years and large fines[176].

The National Critical Information Infrastructure Protection Centre (NCIIPC), set up by the IT Act, is the main agency that is responsible for protecting all kinds of information infrastructures especially in the energy sector. It does so by identifying the critical infrastructure assets, providing security standards, gathering threat intelligence, issuing vulnerability advisories, and coordinating incident response[177].

Likewise, CERT-In, which is cited under Section 70(B) of the IT Act, acts as the national incident response centre and delivers incident response services, security advisories, and threat intelligence dissemination round the clock to the Indian cyber community[178]. Critical sectors have been allocated six ***Computer Emergency Response Teams (CERTs)*** by the Government, with the power system security being the most focused one[179]. Besides that, the Central Electricity Authority (CEA) has set forth technical guidelines to be adhered to by the power systems which would include the requirement of ISO 27001 certification as the preferred Information Security Management System[180].

Nevertheless, this framework has some considerable discrepancies:

- The IT Act is obsolete, and it does not cover digital technologies or AI applications in energy systems, trading on block chain basis, and decentralized micro gridding.
- The Digital Personal Data Protection Act, 2024, which became effective in July 2024, has a narrow focus on personal data protection, thus categorically excluding non-digitized data, and as a result, operational and grid infrastructure data are not well protected.[181].
- Cross-institutional barriers still exist among the Ministry of Power, Ministry of New and Renewable Energy, NCIIPC, CERT-In, and CEA, which results in the gaps where the cyber safety issues in renewable systems are not addressed by anyone in the first place.
- While data localization requirements are justified in terms of the sovereignty perspective, they might lead to some technical inefficiencies in the management of renewable energy systems on a global scale.

B. INTERNATIONAL LEGAL INSTRUMENTS:

The Budapest Convention on Cybercrime is the main international framework that brings cybercrime law of the signer countries to a common level. The Convention, which was opened to signature in 2001, made it obligatory for the parties to consider as crimes illegal access, illegal interception, data interference, system interference, and the like[182]. Furthermore, the Convention laid down the procedural powers for investigation and mechanisms for international cooperation such as the quick data preservation and having 24/7 contact points for immediate international help[183]. India's decision not to ratify the Budapest Convention is a huge drawback. By

[175] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), https://www.meity.gov.in/static/uploads/2024/03/ITbill_2000.pdf.
[176] Id. At Section 70, 70A; see also NCIIPC, Understanding the Role of NCIIPC Legally (2025).
[177] Nat'l Critical Info. Infrastructure Prot. Ctr. (NCIIPC), Roles and Functions, https://nciipc.gov.in (last visited Dec. 15, 2025).
[178] Indian Computer Emergency Response Team (CERT-In), The Indian Computer Emergency Response Team (CERT-In), RFC 2350 Submission (2013); CERT-In, Operational Overview, https://www.cert-in.org.in (last visited Dec. 15, 2025).
[179] Ministry of Power, Government of India, Cyber Security in Power System (2018).
[180] Central Electricity Authority, Technical Standards and Cyber Security Requirements for Power Sector (2015).
[181] Digital Personal Data Protection Act, 2023, No. 49, Acts of Parliament, 2023 (India) (entered into force July 23, 2024); PRS Legislative Research, The Digital Personal Data Protection Bill, 2023 (2025), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.
[182] Budapest Convention, supra note 3, arts. 2-11.
[183] Id. arts. 14-32; COUNCIL OF EUROPE, EXPLANATORY REPORT TO THE CONVENTION ON CYBERCRIME (2001).

not formally acceding, India is excluded from the Convention's mutual legal assistance procedures, and hence loses access to mechanisms for quick international cooperation in investigating cyberattacks, which involve foreign threat actors, on renewable energy infrastructure[184].

On the other hand, ***the NIS and NIS2 Directives of the European Union*** pave the way for the regulation of cybersecurity in different sectors to be done in a modernized way. The first one, namely the NIS Directive, was enacted in the year 2016, and thus, it demands the so-called "operators of essential services" which cover over the mentioned sectors of energy, transport, banking, health, and water to have sound technical and organizational measures in place, through which they can not only guard but also detect and react to cyber incidents[185]. But the second and updated NIS2 Directive, which is going to be effective in 2024, really toughens the previous measures up by introducing lower limits for coverage (including smaller operators), obliging 24-hour incident reporting (as opposed to the previous longer timeframes), and also making huge administrative fines of up to,10 million or 2% of global turnover possible[186].

The NIS2 Directive is such a perfect example of a complete sector-based approach that India has still to make a similar move. It not only clearly states the duties, but it also classifies the incidents in terms of their seriousness, lays down the time limits for reporting, and assigns the supervision directly to the competent national authorities. This model might be considered as a source of inspiration for the formulation of cybersecurity regulations for the Indian renewable energy sector.

International Standards - ISO 27001 and NIST Framework: These standards, while not legally binding, are underpinned by industry practice and contractual obligations, which have virtually made them a necessity. ISO 27001:2022 gives a systematic way for companies to set up Information Security Management Systems, especially important for power firms handling sensitive information[187]. The NIST Cybersecurity Framework, which was developed because of Executive Order 13636, offers a risk-based strategy characterized by five core functions—"Identify, Protect, Detect, Respond, and Recover"—which is increasingly being embraced by power companies[188].

C. CLIMATE GOVERNANCE AND ENVIRONMENTAL LAW INTEGRATION:

It is really striking that still there is no concerted effort in cyberspace governance to integrate climate actions through the mechanisms of both the cybersecurity law and renewable energy policy. The United Nations Framework Convention on Climate Change (UNFCCC) along with its offspring Paris Agreement give global assurances in terms of climate but only allow scant mention of the cybersecurity aspects of renewable energy systems[189]. The International Renewable Energy Agency (IRENA) and the United Nations Environment Programme (UNEP) have initiated to discuss security of renewable energy, however, their efforts cannot be said to be connected to the formal cybersecurity governance[190]. The two aspects, energy security and climate security, cannot be separated; to put it simply, without the protection of the digital that supports renewable energy systems, the goal of climate resilience cannot be realized. Nonetheless, currently, there is no international

[184] Budapest Convention, supra note 3, art. 38(1) (ratification procedures); see generally CYBIL PORTAL, The Budapest Convention on Cybercrime: Benefits and Impact in Practice (2023).
[185] Directive (EU) 2016/1148 of the European Parliament and of the Council, Aug. 6, 2016, 2016 O.J. (L 194) 1 [hereinafter NIS Directive].
[186] NIS2 Directive, supra note 3, art. 32.
[187] ISO/IEC 27001:2022, Information Security Management Systems (2022); ISMS.Online, ISO 27001 for the Energy Industry (2024).
[188] NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.1 (2018); U.S. DEP'T OF ENERGY, ENERGY SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION GUIDANCE (2015).
[189] United Nations Framework Convention on Climate Change, May 9, 1992, 1771 U.N.T.S. 107; Paris Agreement, Dec. 12, 2015, 54 I.L.M. 740 (2015).
[190] IRENA & UNFCCC, Memorandum of Understanding on Strategic Partnership (2019); UNEP, Climate Action and the Energy Transition Survey 2024 (2024).

INTERNATIONAL ENVIRONMENTAL LEGAL RESEARCH JOURNAL
VOLUME 3 AND ISSUE I OF 2025
APIS – 3920 – 0011 | ISSN - 2584-1904
Published by
Institute of Legal Education
https://iledu.in

legal instrument that fully encompasses this intersection.

IV. REGULATORY GAPS, CHALLENGES, AND INDIA-SPECIFIC DIMENSIONS

A. THE CYBERSECURITY-CLIMATE GOVERNANCE GAP:

There is a basic lack of connection between the laws governing cybersecurity and those governing climate change. This gap is due to a number of reasons:

Sectoral Fragmentation: Cybersecurity regulations are mainly aimed at safeguarding information technology and critical infrastructure while climate governance draws attention to emissions reductions and the safeguarding of nature. The outcome is that renewable energy systems are operating under unclear legal rules where industry standards do not exist, and they are obliged to make their compliance fitting with different and often opposing requirements among various regulatory areas.

Data Governance Complexity: The regulatory authorities are different and they do not have consistent sets of rules that govern operational, personal, and environmental data. The Digital Personal Data Protection Act, which is particularly concerned with the issue of personal data, leaves operational data "vital for the security of energy infrastructure" exposed to the risk of not having sufficient legal protection[191]. Besides, energy companies often find themselves in the middle of conflicting and overlapping requirements coming from the different regulatory bodies such as CERT-In, NCIIPC, the CEA, and now the DPDP Board.

International Coordination Deficits: Cyberattacks on energy infrastructure often have transnational impact, but the international legal mechanisms for inquiry, prosecution, and remediation are still not well developed. The non-ratification of the Budapest Convention by India hampers its participation in international cooperation through formal means. On the other hand, regional alternatives like bilateral treaties or informal intelligence sharing arrangements do not possess the legal clarity and enforcement mechanisms that come with formal treaties.

AI Accountability Vacuum: As AI systems take over more and more critical energy functions" from grid balancing to demand forecasting to anomaly detection" legal responsibility for their decisions remains ambiguous. In case of a cyber-incident or extreme weather event, when an AI system makes a wrong decision, which causes grid disruption or energy supply loss, the question arises what legal liability belongs to which party? This question remains essentially unaddressed in existing legal frameworks[192].

B. DIGITAL SOVEREIGNTY AND CROSS-BORDER DATA GOVERNANCE:

The renewable energy systems depend upon cloud computing and international transfers of data. Nevertheless, different national laws concerning data localization, national security, and data sovereignty pose challenges. India's focus on data localization "the mandate that particular categories of sensitive data must be stored in India" while valid from a sovereignty angle, could lead to a technical inefficiency and fragmentation of global energy management systems[193]. The lack of internationally accepted standards for cross-border data governance in energy systems leads to the situation where the data necessary for the best grid control is stored in separate places due to compliance with the law, resulting in reduced system efficiency and resilience at a time when these qualities are most important.

V. INDIA'S CYBERSECURITY RESPONSE AND INSTITUTIONAL CAPACITY

A. CURRENT STATUS AND INSTITUTIONAL FRAGMENTATION:

[191] Digital Personal Data Protection Act, 2023, supra note 21, at 2(c) (definition of "personal data" excluding non-digitized data).

[192] AMPLYFI, AI-Optimized Smart Grids: How EU and US Utilities Are Transforming Energy Management 12-14 (2025) (discussing data poisoning and AI liability gaps).

[193] Digital Personal Data Protection Act, 2023, supra note 21, at 8 (cross-border data transfer restrictions).

The overlapping functions of different organizations like the Ministry of Power, Ministry of New and Renewable Energy, NCIIPC, CERT-In, and the Central Electricity Authority are not backed by clear coordination mechanisms, which results to fragmentation[194]. The fragmentation of security measures has led to a situation where unsecure participants are able to compromise larger systems. The Indian renewable energy industry consists of large foreign corporations that have very advanced cybersecurity programs and also many smaller companies that have very little or no cybersecurity infrastructure at all. Heterogeneity of the companies in the industry leads to cascading vulnerabilities of the whole energy network or a breach of a smaller operator can all result in the downfall of the whole renewable energy network. The awareness of different kinds of cybersecurity threats in the digitalized renewable energy systems is still very low among the policymakers and the operators. There has been an increase in the awareness of threats to the conventional power systems, however, the very specific vulnerabilities of AI-managed smart grids, distributed energy resources, and block chain-based trading platforms have not been properly understood in India's energy sector.

B. EMERGING POSITIVE DEVELOPMENTS:

CERT-In has released guidelines meant for the specific sectors to protect the critical infrastructure that is the power sector. The Central Electricity Authority has integrated cybersecurity requirements into the technical standards. There have been six CERTs that are dedicated to the power infrastructure sector which have been created. The major power plants such as NTPC, NHPC, and PGCIL have already introduced the ISO 27001 controls[195]. Nonetheless, there is still a lack of uniformity in the implementation throughout the sector. The smaller operators and the renewable energy companies, especially those that are working in the area of distributed generation, are far behind in terms of their cybersecurity maturity.

VI. POLICY RECOMMENDATIONS

1. Sectoral Cybersecurity Regulation -India ought to create obligatory cybersecurity policies particular to renewable energy firms, requiring security audits and penetration testing of all generation, distribution, and storage facilities, risk-based incident reporting, setting minimum encryption and authentication standards for IoT and smart-grid devices, and imposing strict supply-chain security requirements on all subcontractors.

2. AI accountability and governance - The law has to unambiguously distribute the responsibility for AI system decisions during cyber incidents, establish meaningful human supervision for automated grid control, put transparency requirements on algorithms operating critical infrastructure, and require periodic security and bias audits of AI utilized in the energy sector.

3. International cooperation and treaties - India's ratification of the Budapest Convention on Cybercrime would enable better cross-border investigation of cyber incidents in the energy sector and the cooperation with IRENA, UNEP, and UNFCCC thus, systematically embedding cybersecurity into the global climate and energy governance.

4. Institutional strengthening - A National Renewable Energy Cybersecurity Centre dedicated to the sector's standard-setting and enforcement as well as the coordination of threat intelligence, incident response, and the building of technical skills should be established, thereby merging the current scattered across several agencies responsibilities.

5. Cross-border data governance - India should be at the forefront in pushing for global standards that not only allow for the necessary cross-border data flows for the efficient operation of grids but also ensure that sensitive

[194] Ministry of Power & Ministry of New and Renewable Energy, Government of India, Institutional Coordination Framework for Renewable Energy Cybersecurity (2024).
[195] Ministry of Power, supra note 19; CEEW, supra note 8.

infrastructure data is protected, thus, navigating the digital sovereignty vs system efficiency dilemma via technical and diplomatic engagement in the global forums.

VI. CONCLUSION

Climate resilience and cybersecurity became interrelated issues in the process of transforming to renewable energy. The technology used for quick decarbonisation also brought new weaknesses which are threats to energy security. Present legal structures, both at the national and international level, are still basically incapable of dealing with this crossroad. India has a special urgency. Being a country that is determined to increase its renewable energy and yet be exposed to intricate cyber dangers, plus being a developing nation with its institutional capacity still limited, India should come up with creative legal and policy strategies that leave behind the fragmented sectoral regulation and promote integrated governance frameworks acknowledging that energy security and climate security are one and the same objective. The wind power and solar energy revolution is already happening. The policy makers' challenge is to "secure it" legally, technologically, and institutionally for the good of present and future human beings. If there are no broad frameworks that include cybersecurity in the climate action and energy governance, then the renewable energy's promise of being the solution for climate change will stay as technically feasible but institutionally vulnerable.