Issue Brief

October 2025
No : 471

Cybersecurity and the Power Grid: Strategic Implications for India's Critical Infrastructure & Defence

Dr. Uday Pratap Singh,
Mayank Saraswat

Cybersecurity and the Power Grid: Strategic Implications for India's Critical Infrastructure and Defence

Dr. Uday Pratap Singh
Mr. Mayank Saraswat

Abstract

The essential framework of India's critical power grid infrastructure experiences swift digital evolution through smart technology adoption combined with IoT integration and renewable energy shifts. These technological advancements deliver potential efficiency and sustainability gains, yet simultaneously increase cybersecurity vulnerabilities within the power grid system. The study examines how India's national security and defence sector faces strategic challenges due to the power grid's role in critical infrastructure amidst changing cybersecurity threats. The paper examines India's grid modernisation efforts alongside recent cyber threats and hybrid warfare dynamics to identify vulnerabilities and propose a detailed policy framework for resilience enhancement. Experts suggest enhancing cyber security while developing decentralised grid systems alongside civil-military partnerships and international cooperative efforts. The research report determines that power grid protection is essential for maintaining India's sovereignty alongside its economic stability and military preparedness during hybrid warfare.

Keywords: Power Grid, Cyber Threats, Critical Infrastructure, Hybrid Warfare, National Security.

Critical Infrastructure and the Role of the Power Grid

Critical infrastructure refers to the critical systems and assets that are crucial for security, economic stability, public health, and safety of a country (IBM). They encompass industries like power generation and distribution, water supply, telecommunications, transportation, financial services, healthcare, and emergency response systems. Of these, the electricity grid is one of the most important components, frequently considered to be the backbone of contemporary society, as it provides the capability for the operation of almost all other vital systems.

The electrical power grid exists primarily to provide reliable and safe energy services to anyone and everyone at any time of the day (Sovacool, B.K., Carley S., Keisling L. 2024).The power grid is a necessary component of our infrastructure as it supplies electricity for the functioning of other essential systems— hospitals, water purification facilities, transport

infrastructure, data centres, and telecommunications, all relies heavily on a reliable and uninterrupted source of power. When the grid fails, disruption will be universal in many areas of society, attesting to the grid's prominence in everyday operation. At the national security level, a secure and resilient grid is critical to underpin military activity, emergency response, and government communications. Further, the economy relies significantly upon a stable electricity supply loss of supply can result in heavy financial losses within manufacturing, financial, and commerce sectors.

However, while this increasing digitisation and interconnection of the power grid, particularly through the inclusion of smart technologies and the Internet of Things (IoT), has improved efficiency, it has also increased the risk of cyberattacks. The number of connected devices (e.g., smart thermostats and appliances) is growing rapidly, with the global stock projected to double over the next five years to reach 30-40 billion devices by 2025 (IEA). A sophisticated cyber attack on the power grid would render vital services useless and create disruptions nationwide. Further, the grid is critical to disaster resilience. A resilient and flexible grid infrastructure has the potential to reduce the effects of natural disasters by restoring electricity to essential services and maintaining public safety quickly (IEA).

The shift to renewable energy systems such as wind and solar, imposes new challenges on the electric grid. The grid needs to be upgraded and made more flexible to handle decentralised and variable generation (Bryant, J. 2025). Upgrading is needed not just for sustainability purposes but also for long-term reliability and security. The World Economic Forum emphasizes investing in grid flexibility to ensure a cleaner and more resilient energy system. It highlights that an estimated $21 trillion investment in grid upgrades by 2050 is required to achieve a net-zero trajectory (Schierenbeck, A., 2025). In short, the power grid is a foundational element of critical infrastructure, supporting nearly every aspect of contemporary life and in need of ongoing investment and defence to maintain the stability and advancement of society.

Importance of Cybersecurity in the Context of Critical Infrastructure and the Power Grid

Within the realm of critical infrastructure and the power grid, cybersecurity has reached national importance. As power grids become more dependent on digital systems, smart technologies, and interconnecting networks to improve efficiency and reliability, they have become increasingly vulnerable to cyberattacks. These dangers may be initiated by nation-state actors, criminal groups, or ill-willed individuals and can potentially interfere with or shut down

critical services (GAO, 2019).A successful cyberattack on the electrical grid would result in widespread power outages, jeopardise emergency services, disrupt communication systems, and critically affect healthcare, transportation, and financial infrastructures. This would not only result in instant devastation but also long-term effects on national security and economic stability.

Cybersecurity is essential to guard the confidentiality, availability, and integrity of systems that regulate the distribution of power. Securing industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and other digital elements that monitor and regulate the distribution of electricity falls under this (Belding, G. 2019). Good cyber security efforts involve time-based threat discovery, periodic assessment of vulnerabilities, secure system development, and unified response strategies to potential breaches. In addition, cybersecurity provides secure interconnection of renewable energy sources and smart grid technology, which relies on continuous communication and data transfer.

As attacks on infrastructure become more cyber-savvy, governments and utilities need to prioritise cybersecurity in the form of policy, regulation, and investment in cutting-edge defence technologies. The power grid's—and, by extension, the entire critical infrastructure web's resilience hinges on a pre-emptive strategy for cybersecurity that prevents threats and reduces risk before damage can be done (IEA). In short, without strong cybersecurity, the advantages of modernising and digitising the electricity grid might be offset by vulnerabilities that put the heart of national infrastructure at risk of severe threats.

India's Power Grid Modernisation and Digital Integration

India has launched a bold initiative to modernise its power infrastructure to build a safe, resilient, green, and digitally advanced energy system. The focal point of this overhaul is the National Smart Grid Mission (NSGM), launched by the Ministry of Power in 2015, to drive the adoption of smart grid technology throughout the nation (NSGM). The objective is to incorporate Information and Communication Technology (ICT) into conventional power systems to improve efficiency, reliability, and consumer participation. A foundation of this effort is the National Smart Metering Program, which targets the installation of 250 million smart meters by 2025–26. In late 2024, more than 222 million smart meters have been approved, with about 16.83 million installed (Powerline, 2023). The meters provide real-time

visibility, dynamic pricing, and enhanced billing accuracy, forming the building blocks of a more efficient and responsive grid.

Incorporating renewable sources viz. solar and wind power, in the grid is also an imperative component of the process. Better distributed generation handling through smart grids assures stability as well as optimum distribution of energy. Emerging technologies like SCADA systems, DMS, and OMS are being utilised for the strengthening of grids as well as restoring supplies with faster efficacy in the face of interruptions. To enable these technological developments, the Smart Grid Knowledge Centre (SGKC) was formed to train and build the capacity of utilities and stakeholders. SGKC provides experiential learning on smart grid technologies such as microgrids, power quality analysis, and smart home systems, creating a competent workforce that can operate and maintain the upgraded grid (Powergrid, 2025).

Phase I of the roadmap for smart distribution, which will be completed by 2026, addresses building blocks like feeder and distribution transformer metering, Advanced Metering Infrastructure (AMI), and consumer indexing. Phase II, which is planned to be completed by 2030, looks at implementation at a wider level, with the implementation of SCADA, DMS, and OMS across different voltage levels to achieve comprehensive coverage and improved grid management (Powergrid, 2025). By taking such collective actions, India stands to reshape its power sector as a digitally interconnected and robust infrastructure that can accommodate the increasing demand for energy while embracing a sustainable culture.

Overview of India's National and Regional Grids

India's power grid is one of the world's largest and most complex, arranged on a national grid that has five regional grids—Northern, Eastern, Western, Southern, and North-Eastern. These regional grids were built as separate entities initially, but were interconnected to form a unified national grid, the final large-scale integration being done in May 2014 instead of the targeted December 2013, when the Southern Grid was synchronised with the remaining system (Business Line, 2017). The country's national grid is regulated by the Power System Operation Corporation (POSOCO), which manages grid stability, scheduling, and load dispatch throughout the country.

This integration supports better resource sharing, better load balancing, and better management of generation and transmission capacity. It can facilitate the export of power from surplus regions to deficit ones, enhancing aggregate energy security and reliability. The power system operates at a frequency of 50 Hz and employs high-voltage transmission cables,

including an expanding network of High Voltage Direct Current (HVDC) connections, for effective long-distance power transfer with low losses (Powerline, 2017). Each regional grid still retains operational autonomy under respective Regional Load Despatch Centres (RLDCs), but they coordinate closely to maintain national balance and avoid outages.

As there is an expansion of renewable energy resources like wind and solar, the integrated grid is tasked with playing a crucial part in managing the intermittency and variability of power sources. The high regional interconnections make it easier to spread renewable generation, thereby guaranteeing a supply even in instances where localised generation dips. Briefly, India's national and regional grid infrastructure is the backbone of its power sector, supporting reliability, efficiency, and the transition towards a cleaner energy future.

Recent Trends in Smart Grids, Automation, and IoT Integration in India's Power Sector

India's power industry is undergoing a deep change through the integration of smart grids, automation, and Internet of Things (IoT) technologies. These technologies are aimed at enhancing the efficiency, reliability, and sustainability of India's energy infrastructure (Sinha, J., 2019). One of the major aspects of this transformation is the extensive deployment of Smart Metering and Advanced Metering Infrastructure (AMI). As of 16 October2024, over 14.5 million smart meters have been installed in India. The pace of installation has been increasing, with nearly 4.8 million smart meters installed in the 2023-24 period —three times the number installed in the previous year (Powerline, 2024).India has set an ambitious target to install 250 million smart meters by 2027, under the Revamped Distribution Sector Scheme (RDSS). The government has earmarked ₹97,631 crore for smart meter installations under the RDSS, aiming to modernise the country's energy infrastructure and empower consumers to monitor and manage their electricity usage more effectively (Anand, S., 2024). Such smart meters enable real-time data reading, remote monitoring, and dynamic pricing, which allow consumers to control their power usage more effectively.

Artificial Intelligence (AI) is also crucial in grid optimisation. With predictive maintenance and fault identification, AI reads sensor and equipment data to predict failure, enabling proactive maintenance and minimising downtime. This not only enhances efficiency but also prolongs the lifespan of critical assets (Elets News, 2024). In the sphere of asset and automation management, companies like Power Grid have innovated solutions like the Power Grid Digital Application for Routine Patrolling and Assessment of Network (PG-DARPAN)

and Asset Life Management System (PALMS). This software uses IoT and cloud technologies for real-time network monitoring and determination of asset condition.

In addition, demand response programs and Virtual Power Plants (VPPs) are being used to increase grid stability and facilitate the integration of renewable power. For instance, Tata Power has joined forces with Auto Grid to introduce AI-based demand response programs in Mumbai, which seeks to incentivize both commercial and residential consumers to curtail consumption during peak times (Tata Power).Another key development is the integration of edge computing and 5G technology in enhancing the responsiveness and scalability of IoT applications. Edge computing enables processing nearer to the source, thus reducing latency, while 5G connectivity enables the integration of a huge variety of devices necessary for massive-scale IoT deployment.

Collectively, these advances represent a shift towards a smarter, more sustainable Indian power grid that can better cope with the changing needs of energy consumption and contribute to the long-term sustainability goals of the country.

Cybersecurity Threats to the Power Grid in India

India's power grid, as with most countries, is becoming ever more susceptible to cybersecurity attacks through the accelerated digitisation of infrastructure, the use of smart grid technologies, and the growth in interconnected systems. As the grid transforms with technologies like smart meters, IoT devices, SCADA systems, and real-time monitoring platforms, so too does it create a larger attack surface for nefarious forces.

One of the greatest dangers is the possibility of state-sponsored cyberattacks. Interestingly, a report by Recorded Future in 2021 traced a Chinese government-affiliated threat group to a series of incidents that hit India's power industry, including its grid in Mumbai, which was hit by an unprecedented blackout in 2020 (Insikt Group, 2021). While the Indian government had not formally held a blackout resulting from a cyberattack, it raised some alarm regarding the country's grid and its exposure to foreign cyber threats aimed at disturbing critical infrastructure.

Ransomware attacks are a growing threat to India's energy sector, with hackers breaking into systems, encrypting vital data, and offering to release it for a payment. Utilities and distribution utilities, especially those with old IT systems or poor cybersecurity measures, are particularly at risk of such attacks. Besides ransomware, malware, and phishing operations

frequently target operators of control systems and maintenance workers, giving attackers potential access to sensitive operational systems. Insider threats and human mistakes also present great threats, especially within companies that have limited cybersecurity training or awareness. Misconfigured systems, faulty password habits, and a lack of network segmentation can unwittingly provide vulnerabilities for cyber breaches or permit malicious attackers to escalate access inside networks.

The increasing dependence on Internet of Things (IoT) devices and remote access technologies adds additional vulnerabilities, as insecurely managed endpoints and networked devices can be used to interfere with operations, compromise data integrity, or even perform clandestine surveillance (Sinha, J., 2019).Adding to these risks is the reality that numerous Indian state utilities are only just beginning to transition towards international cybersecurity standards, which creates gaps in compliance, threat detection, and incident response capabilities.

For neutralising these vulnerabilities, the Government of India has launched a variety of strategic responses. One is the creation of the National Critical Information Infrastructure Protection Centre (NCIIPC) within the National Technical Research Organisation (NTRO), which takes care of prioritising and safeguarding assets integral to national security. Power sector-specific cyber-audits, the release of CERT-In advisories, as well as some capacity-building efforts, have been launched to drive cybersecurity readiness as well (Powerline, 2025). However, consistent investment in cybersecurity infrastructure, ongoing awareness training, real-time monitoring systems, and strict enforcement of regulations will continue to be necessary to protect the country's power grid against the expanding list of cyber dangers.

Strategic Implications for National Security: Cybersecurity Threats to India's Power Grid

Cyber threats to India's power grid have deep strategic consequences for national security, given the fact that the grid is the backbone of almost all critical infrastructure systems. An effective cyberattack on the grid—whether via malware, ransomware, phishing, or state-sponsored operations—is capable of leading to widespread blackouts, economic disruption, panic among the population, and undermining emergency and defence operations. Since electricity drives hospitals, transport systems, communication networks, banking infrastructure, and defence installations, any disruption can cripple critical services and seriously compromise public safety and government operations.

The growing digitisation of the power industry, via smart grids, IoT devices, SCADA systems, and real-time monitoring platforms, while improving operational efficiency, also creates new cyber vulnerabilities. These digital interfaces, if not properly secured, provide potential entry points for attackers to cause disruptions, steal sensitive information, or manipulate system behaviour. During a coordinated cyberattack, the attackers may take advantage of these vulnerabilities to trigger cascading failures across industries, eroding both internal stability and global confidence in India's cyber resilience.

Geopolitically, cyber attacks on the power grid increases the threat of asymmetric warfare, whereby enemy forces, especially state-supported agents, would employ cyberattacks as an inexpensive, high-payoff means for destabilising the country without resorting to open armed conflict. The already reported foreign cyber entities' targeting of Indian grid infrastructure has already demonstrated the power systems' potential to become battlefields in cyberspace, with the purpose of coercion, deterrence, or strategic signalling. During 2020, when border tensions surged, hackers with suspected Chinese state affiliations, infiltrated India's power grid control networks. The clandestine malware Shadow Pad enabled infiltration into ten key power sector organisations, including 4 of the 5 Regional Load Dispatch Centres , which manages national electricity stability (Verma, A, 2025). An equally disturbing event took place in 2019 when malicious software infiltrated Tamil Nadu's Kudankulam Nuclear Power Plant administrative network; the D Track spyware maintains connections to the Lazarus Group, which operates as a North Korean state-sponsored hacking entity ((Verma, A, 2025).Also, the vulnerability of the grid compromises deterrence stance and reveals India's critical infrastructure defence system shortcomings. It further makes India's dreams of being a digital and economic power in the world complicated, as continuous cyber insecurity has the potential to undermine investor confidence and impede smart infrastructure drives such as Digital India and Smart Cities (Sharma, V., 2025).

In response to these dangers, the national security strategy will have to focus on cybersecurity in the power industry through strong policies, increased collaboration between intelligence organisations and utility companies, real-time cyber threat information sharing, and the enhancement of the National Critical Information Infrastructure Protection Centre (NCIIPC). It is only through strong cyber defence mechanisms, strategic vision, and global cooperation that India can protect its power grid and, by extension, its national security interests in the digital era.

Energy as a Domain in Hybrid Warfare: Implications for India's Power Grid

The power grid emerges as a critical element within hybrid warfare strategies that blend conventional military methods with cyberattacks and disinformation campaigns alongside economic disruptions (Arnold, C.D., 2020). The power grid of India represents a critical weakness that adversaries can target during hybrid warfare operations. Hybrid warfare involves deploying diverse military tactics, including conventional battles, irregular combat, cyberattacks, and informational warfare to reach strategic goals, while the energy sector stands as a prime target due to its critical role in national security and economic stability.

India's power grid transformation through digital technologies like smart grids, SCADA systems, IoT devices, and real-time monitoring system positions the energy sector as both a national development enabler and a hybrid warfare tool. Adversaries exploit cyberattacks on power grids to induce economic paralysis and social unrest while creating military disadvantages without traditional force deployment. India's power grid faces escalating risks from cyberattacks as demonstrated by the 2020 Mumbai blackout and ongoing threats from foreign state-sponsored cyber operations, which reveal how energy infrastructure becomes a target in hybrid warfare. An intricately planned cyberattack can incapacitate extensive portions of the power grid, which would disrupt industrial operations alongside government services while compromising healthcare systems and national defence networks.

Through hybrid warfare tactics, adversaries attempt to control energy resources to cause power outages, which disrupt industrial outputs and sway public opinion by causing blackouts during crucial periods such as elections, national emergencies, or military operations. Energy flow disruptions initiate cascading failures across transportation and telecommunication sectors, which amplify their detrimental impacts. Through attacks on India's power grid, enemies can disrupt economic stability and diminish strategic strength without engaging in traditional warfare.

The power grid becomes a strategic target in hybrid warfare due to its reliance on external energy sources and susceptibility to supply interruptions. Countries dependent on energy imports or lacking robust energy security face potential coercion or attacks that destabilise their sovereign authority. The integration of renewable energy sources alongside decentralised systems such as solar and wind power introduces potential vulnerabilities in India's power grid that adversaries may exploit due to these elements operating in less-regulated

sectors. Renewable energy systems, when integrated into power grids, create management complexities while increasing vulnerability to distribution disruptions.

India needs to focus on strengthening its energy infrastructure resilience to effectively combat hybrid warfare threats. The strategy involves bolstering cybersecurity measures to protect against threats from state and non-state entities while simultaneously funding grid upgrades for faster post-attack recovery and developing strong contingency plans to handle energy supply interruptions (Energy Central, 2023). National security demands an intricate multi-domain strategy that necessitates close collaboration among intelligence agencies, cybersecurity experts, energy regulators, and military planners to predict and counter energy-based threats in hybrid warfare. India needs to investigate strategic energy security measures, including diversification of energy sources and boosting domestic production to decrease dependence on foreign energy providers and reduce potential weaknesses during hybrid attacks.

Impact of Cybersecurity Threats on the Power Grid on India's Defence Sector

India's power grid faces cybersecurity threats that have extensive implications for the defence sector as military operations, national defence readiness, and strategic capabilities depend on grid stability. Power grids represent foundational components that support critical defence infrastructure elements such as communication networks, transportation systems, surveillance operations, command-and-control frameworks, and military bases. Within hybrid warfare scenarios, adversaries intentionally attack power grids to execute broader strategies to weaken India's defence systems and interrupt military activities.

Operational Disruptions to Military Installations

Modern military operations depend extensively on electrical power to sustain command centres alongside communication networks and radar systems, as well as air defence mechanisms and essential operational infrastructure. The power grid faces potential large-scale blackouts from cyberattacks, which would disable facility operations. Real-time communication between military units might become disrupted while troop and equipment movements face delays and defence systems become inoperable. The nation's immediate operational capabilities suffer while its strategic preparedness for future challenges diminishes, creating vulnerabilities to external threats.

Loss of Communication and Coordination

Electric power dependency defines the communication networks within India's defence sector systems. A cyberattack-induced power grid failure would disconnect military headquarters from field units, making wartime or emergency coordination exceedingly difficult. The military encounters significant difficulties in force direction and intelligence sharing, as well as tactical execution without stable ongoing communication systems. Strategic assets, including satellites and UAVs (unmanned aerial vehicles), alongside drones, might experience connectivity loss, which diminishes their surveillance, reconnaissance, and targeting capabilities.

The Disruption of Transportation Networks and Supply Chains

Military logistical activities, including vehicle maintenance and fuelling operations alongside base and supply chain power requirements, rely heavily on grid power. An assault on the power grid through cyber means has the potential to obstruct defence supply transportation while disrupting maintenance operations and delaying troop movements. The transport and logistics industries, which depend on electric trains and vehicles, may experience severe disruptions that obstruct the swift deployment of military forces in conflict scenarios.

Effect on National Security Monitoring and Surveillance

Modern surveillance networks that track cross-border movements, detect penetration, and monitor national security threats rely on electricity. Surveillance systems such as radar posts, sensor nets, and spy satellites need an uninterrupted power supply to operate at optimal levels. An attack on the power grid could paralyze these systems, allowing enemies to infiltrate across borders without detection or launch surprise attacks. Loss of surveillance ability reduces the efficacy of defence means, and it becomes easier for belligerent forces to locate vulnerabilities.

- ***Threat to Nuclear and Sensitive Military Installations***

  India's nuclear power plants, weapons platforms, and other sensitive military installations rely on a secure power supply for safe operations and security procedures. A cyberattack on the power grid can provide opportunities for adversaries to attack these installations, cause disruptions in power to security systems, and interfere with their operational safety. In addition, the military's ability to operate in remote or strategic locations like mountain passes, border areas, and naval bases could also be impaired if power disruptions affect the operation of mobile or localized energy systems servicing military installations in these regions.

- **Psychological Impact and National Morale**

  A major cyber-attack against India's power grid is likely to have a psychological effect on India, including the military, in that it would be seen as an attack on national security and sovereignty. Power cuts, if coordinated at a time when there is heightened military operation or political crisis, can erode public confidence and morale. This can make it increasingly challenging for defence forces to remain cohesive and prepared during wars or crises.

Challenges in Recovery and Response

If the power grid is attacked through cyber, the defence industry would be forced to resort to backup power sources such as generators or backup systems. However, these systems are subject to scale, duration, and reliability limitations. The military would struggle to carry on operations until the grid re-establishes connectivity, which would retard response time and hinder fast recovery efforts. Moreover, defence facilities that are part of bigger, interconnected grid systems may experience delays in restoring power, especially if they depend on outside sources of energy that can be disrupted by the attack.

Strategic Measures for Mitigating the Impact on Defence

To reduce such threats, energy security has to be a part of the country's national defence plan. Upgrading the cyber-defence of the grid, using decentralised and fault-tolerant energy systems (microgrids), and implementing quick response to repair the grid, in case of an attack, are steps in the right direction. In addition, enhancing the energy autonomy of key military installations by employing backup power systems, on-site generation (e.g., solar panels, diesel generators), and energy storage technologies will assist in mitigating weaknesses in event of a grid failure. Moreover, the defence community must collaborate with civilian energy suppliers to develop reciprocal response procedures, thereby facilitating coordinated action in the protection of both military and civilian energy infrastructure.

The cyber threats to India's power grid have significant strategic consequences for the defence sector, with implications for military preparedness, operational effectiveness, and national security. Enhancing the power grid's resilience and the defence sector's capability to function in a cyber-contested environment is critical to India's ability to maintain its defence posture and protect its sovereignty from the evolving hybrid warfare strategy.

Recommendations for Securing India's Power Grid and Strengthening its National Defence

To reduce cyber threats to India's power grid and its implications for national security, India requires the following strategic recommendations, which can help to mitigate risks, enhance resilience, and ensure stability of both the energy and defence sectors:

Strengthen Cybersecurity Frameworks and Regulations

India needs to enhance its cybersecurity regulations and guidelines for the infrastructure of criticality by creating a comprehensive, unifying cybersecurity policy for the power grid sector in particular. It needs to be compatible with global best practices, including the NIST Cybersecurity Framework, and have its applicability in both the public and private sector organizations operating in the power industry. To ensure continuous protection, frequent cybersecurity audits and penetration, testing should be done as per policies of the National Critical Information Infrastructure Protection Centre (NCIIPC) and other security organizations responsible for it, so that they can detect vulnerabilities and assist in countering them in time (Chandrakar, A., 2025).Further, with the grid becoming smarter with IoT, SCADA, and AI integration, the government must enforce stringent cybersecurity protocols, such as data encryption, secure access controls, and strong security controls for all devices and systems connected.

Enhance Resilience through Decentralisation and Microgrids

To enhance the strength of its power grid, India needs to invest in decentralised power systems like local microgrids that can run independently or in parallel to the main grid. Such microgrids, fuelled by renewable energy sources like solar and wind power, would provide safe backup power to key defence establishments, government offices, hospitals, and emergency centres during grid failures. By decreasing dependence on a single, centralised power grid, this method would reduce the risk of large-scale blackouts and provide continuity of essential services. Furthermore, encouraging decentralisation of renewable energy production throughout the nation, would also enhance energy security and reduce the effect of possible cyberattacks or physical attacks on the master grid (IEA).

Improve Coordination between Defence and Energy Sectors

Given increased cybersecurity risks to India's power grid and the possible ramifications for national security, it is essential to intensify coordination between the defence and energy

sectors. Periodic joint cybersecurity drills between the Ministry of Power, power sector utilities, and the Indian Armed Forces must be held with regularity to mimic cyberattacks on strategic energy infrastructure. These exercises will improve coordination, streamline incident response procedures, and assist in identifying vulnerabilities across both sectors. In addition, India must build integrated national command and control structures that integrate real-time power grid operational information with defence operations, allowing for instant military preparedness and operational continuity even in case of a grid failure.

Invest in Threat Detection, Monitoring, and Incident Response

To further enhance the security of its critical infrastructure, India will need to invest in state-of-the-art threat detection, surveillance, and rapid incident response systems. Deploying sophisticated, AI-powered cybersecurity solutions that can scan the power grid in real time will help detect abnormalities early, which could be indicative of cyberattacks, thus enabling prompt and targeted intervention. Concurrently, the establishment of a unified National Cyber Defence Centre, focused on cyber threat intelligence and incident response, will be pivotal to an integrated and efficient cyber defence. Operating 24x7, this centre will need to engage closely with the Indian Computer Emergency Response Team (CERT-In), to process threats in time and render them harmless before they can inflict catastrophic damage.

Develop Energy Independence for Critical Defence Installations

To provide business continuity in the event of grid collapse, India has to give top priority to energy independence and ensure power availability to important military facilities. This includes providing all important defence establishments with strong, standalone sources of energy like diesel generators, solar power, and battery storage, along with hybrid systems that can easily transition to alternative power supply when there is an emergency. Simultaneously, it is important to reinforce the security of power supply lines to sensitive military locations, such as nuclear power plants and missile defence systems, through the adoption of isolated, encrypted, and secure transmission lines that are less vulnerable to outside threats and cyberattacks. The integration of small modular reactors (SMRs) is a key component of this strategy. SMRs, such as the Bharat Small Reactor (BSR) and Bharat Small Modular Reactor (BSMR), offer compact and reliable power sources, enhancing the energy security of military bases and critical infrastructure (Yadav, S. 2024).

Foster Public-Private Partnerships for Infrastructure Security

Public-private partnerships (PPPs) will be a cornerstone in protecting India's energy and defence infrastructure from cyber threats. By facilitating cooperation among government organisations, public sector undertakings (PSUs), and private sector corporations, India can leverage resources to create and deploy cutting-edge cybersecurity technologies, boost real-time threat detection, and adopt efficient response measures (Saraswat, V.K., 2019). Also, encouraging private companies to innovate and develop cybersecurity products tailored to the power grid, such as physical infrastructure protection, remote monitoring systems, SCADA protocols, and distributed energy resources, will enhance the country's cyber resilience even more.

Enhance Awareness and Capacity Building

Growing awareness about cybersecurity and capability development in the defence and power sectors is needed to secure India's critical infrastructure. There needs to be wide-scale training and awareness sessions for employees at power grid facilities, defence establishments, and other sensitive locations, imparting them the right skills to identify and respond to threats such as phishing, ransomware, and other cyber threats. Meanwhile, the Indian military must spend funds on special cyber military training of troops and on establishing specialised cyber defence units that can handle and counter cybersecurity threats to critical national infrastructure.

International Cooperation on Cybersecurity

Global cooperation is necessary to make India's cybersecurity stance robust enough to counter cross-border attacks against critical infrastructure. India must positively participate in cyber diplomacy by partnering with friendly and neighbouring nations to exchange threat information, best practices, and cybersecurity norms, especially for the energy sector. Further, India should play an active role in influencing global norms on cybersecurity in international platforms to ensure that the new global standards are tailored to its national security interests and help towards a more secure and robust digital environment (Statecraft Analysis, 2024).

Establish a National Grid Security Framework

To have uniform and transparent security of key infrastructure in the energy sector, the government can strengthen the National Grid Cybersecurity Framework, which can complement both private and public power grid operators. The framework should comprise strict guidelines dealing with the resilience of the grid, real-time surveillance, incident

reporting protocols, and specified response schedules, with special attention to defence contingencies. Also, a more extensive Critical Infrastructure Protection Framework must be created to detect, categorise, and prioritise assets according to their strategic significance and vulnerability to ensure that most critical elements of the national infrastructure requires highest security and monitoring.

By proactively securing its power grid and enhancing the resilience of its energy infrastructure, India will be able to better safeguard its defence sector, secure national security, and retain operational readiness in the face of changing cyber threats. Embracing a multi-faceted approach—encompassing technological advancements, better coordination between the energy and defence sectors, enhanced international cooperation, and massive investments in cybersecurity—will allow India to protect its key infrastructure from hybrid warfare techniques and geopolitical threats. Enforcing these all-encompassing measures will ensure a secure, robust, and future-proofed energy system that can repel both traditional and cyberattacks.

Conclusion

India's power grid protection and resilience are of utmost significance in guaranteeing national security, economic prosperity, and strategic readiness. Being the skeleton of all key infrastructure, ranging from defence to healthcare, transport, telecommunications, and finance systems, the power grid supports operations of contemporary society. With growing incorporation of smart devices, IoT, and renewable energy systems, India's power grid is evolving into a more efficient and networked structure. But attendant on this digital evolution are major cybersecurity threats that can be leveraged by adversaries, state or otherwise, to destabilise the country in peace or war.

Cyber attacks against the grid, as indicated by recent events such as the 2020 Mumbai blackout, have uncovered systemic vulnerabilities and demonstrated the grid's nascent importance in hybrid warfare. In those cases, the tactic is to disable critical services, create fear, disrupt military operations, and undermine public confidence, all without using traditional forces. As such, India needs to take a strategic, layered approach to defending its power grid that exceeds technical band-aids. This involves the establishment of a strong national cybersecurity system, periodic audits, and threat simulations, as well as investments in AI-driven threat detection, decentralised microgrids, and energy independence for defence establishments. Defence-energy sector coordination has to be institutionalised through mutual

exercises, cooperative intelligence, and combined command setups. In addition, public-private partnerships can facilitate faster development and rollout of cutting-edge security solutions best-suited for India's specific needs.

At the same time, capacity-building programmes and awareness drives for utility employees, defence personnel, and policymakers are crucial to developing a strong human firewall against cyberattacks. India should also proactively become a part of setting global cybersecurity norms and forming coalitions for intelligence sharing, response to incidents, and the defence of infrastructure. In the end, the security of the power grid is as much a technical as a strategic imperative. By linking its energy modernisation objectives with defence interests at the national level, India can provide for continuity of operations, discourage cyberattacks, and solidify its position as a strong, sovereign, and digitally enabled nation in a world full of complex, dynamic security threats.

Works Cited

AI Transforming Power Distribution for Efficiency and Reliability (2024, July 22). *Elets News Network*. https://egov.eletsonline.com/2024/07/ai-transforming-power-distribution-for-efficiency-and-reliability/.

Anand, S. (2024, October 15). India targets 250 million smart meters by 2027, $20 billion opportunity in energy Management. *ET Energy World*. https://energy.economictimes.indiatimes.com/news/power/india-targets-250-million-smart-meters-by-2027-20-billion-opportunity-in-energy-management/114162408.

Arnold, C.D. (2020, August 12). Energy security in the era of hybrid warfare, Geopolitics & Energy Security. *NATO Energy Source*. https://www.atlanticcouncil.org/blogs/energysource/energy-security-in-the-era-of-hybrid-warfare/.

Belding, G. (2019, August 5). Critical Infrastructure ICS/SCADA Security Overview. *Infosec*. https://www.infosecinstitute.com/resources/scada-ics-security/ics-scada-security-overview/.

Brisk Pace: Smart metering market set for exponential growth (2024, November 13). *POWERLINE*. https://powerline.net.in/2024/11/13/brisk-pace-smart-metering-market-set-for-exponential-growth/.

Bryant, J. (2025, January 16). Decentralized Energy Systems: Enhancing Grid Flexibility and Reliability. *European Energy Future Forum*.https://www.europeanfutureenergyforum.com/decentralized-energy-systems-enhancing-grid-flexibility-and-reliability/.

China-linked Group Red Echo Targets the Indian Power Sector Amid Heightened Border Tensions (2021, February 28). *INSIKT GROUP*. https://www.recordedfuture.com/fr/research/redecho-targeting-indian-power-sector.

Changing Power Dynamics: HVDC reshaping India's energy future. (2017, November 2). *POWERLINE*.https://powerline.net.in/2017/11/02/changing-power-dynamics/.

Critical Infrastructure Protection: Actions Needed to Address Significant Cyber security Risks Facing the Electric Grid (2019, September 25). U.*S. Government Accountability Office, GAO-19-332*. https://www.gao.gov/products/gao-19-332.

Cyber Resilience. *IEA.* https://www.iea.org/reports/power-systems-in-transition/cyber-resilience.

India's power transmission system embracing modern technology to combat cyber attacks (2023, March 15). *ENERGY CENTRAL NEWS*. https://energycentral.com/news/indias-power-transmission-system-embracing-modern-technology-combat-cyber-attacks.

IoT: An emerging reality in Indian DISCOMs (2019, November 29). *Electrical India*. https://www.electricalindia.in/iot-an-emerging-reality-in-indian-discoms/.

National Smart Grid Mission. *Ministry of Power, Government of India*. https://www.nsgm.gov.in/en/nsgm.

Safeguarding Cyberspace: Indian Foreign Policy and Cybersecurity (2024, March 22). *Statecraft Analysis*. https://statecraftanalysis.com/safeguarding-cyberspace-indian-foreign-policy-and-cybersecurity.

Saraswat,V.K. (2019). Cyber Security. *Niti Aayog*. https://niti.gov.in/sites/default/files/201907/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf.

Schierenbeck, A. (2025, January 20). The cost of inaction: Grid flexibility for a resilient, equitable digital energy future. *World Economic Forum*. www.weforum.org/stories/2025/01/grid-flexibility-for-resilient-equitable-digital-energy-future/.

Sharma, V. (2025, March 8). Cyber security guidelines for smart city infrastructure. *Odisha TV*. https://odishatv.in/news/national/cyber-security-guidelines-for-smart-city-infrastructure-257433.

Smart Grid Knowledge Centre (SGKC). *POWERGRID*. https://www.powergrid.in/index.php/en/smart-energy.

Smart Metering: Advancements Progress under the NSGM. (2025, February 3). *POWERLINE*.https://powerline.net.in/2025/02/03/smart-metering-advancements-progress-under-the-nsgm/.

Strengthening Defences: Mitigating cybersecurity challenges in the power sector (2025, February 2). *POWERLINE*. https://powerline.net.in/2025/02/02/strengthening-defences-mitigating-cybersecurity-challenges-in-the-power-sector/.

Southern States connected to national power grid (2017, November 25). *Business Line*. https://www.thehindubusinessline.com/economy/Southern-States-connected-to-national-power-grid/article20707253.ece .

Sovacool, B.K., Carley S., Keisling L. (2024). Energy justice beyond the wire: Exploring the multidimensional inequities of the electrical power grid in the United States. *Energy Research & Social Science, Vol. 111*. https://www.sciencedirect.com/science/article/pii/S2214629624000653.

Tata Power joins hands with Auto Grid to Expand AI-enabled Smart Energy Management System in Mumbai. *Tata Power*. https://www.tatapower.com/news-and-media/media-releases/tata-power-joins-hands-with-autogrid-to-expand-ai-enabled-smart-energy-management-system-in-mumbai.

Verma, A. (2025, April 16). Defending Digital India: Strategic Response to Cross-Border state-sponsored cyber offensives. *ET Government*. https://government.economictimes.indiatimes.com/news/digital.

What is critical infrastructure? *IBM*. https://www.ibm.com/think/topics/critical-infrastructure.

Yadav, S. (2024, June 26). India's Nuclear Power Expansion To Give Major Boost to Defence Capabilities. *Sputnik India*. https://sputniknews.in/20240626/indias-nuclear-power-expansion-to-give-major-boost-to-defense-capabilities-7709163.html.

About the Author

Dr. Uday Pratap Singh is an Assistant Professor in the Department of Defence and Strategic Studies at Iswar Saran Degree College, University of Allahabad, Prayagraj. He holds both a Master's degree and a D.Phil. in Defence and Strategic Studies from the University of Allahabad. He was awarded the Gold Medal for securing the top position in the M.Sc. and received the Award for Excellence (2016) from the University of Allahabad. He is a keen researcher specializing in International Strategic Relations and National Security. He serves as a Subject Matter Expert at the Centre for Joint Warfare Studies (CENJOWS) and as a Distinguished Fellow at the Forum for Global Studies, New Delhi. He has published numerous research papers in reputed national and international journals on diverse defence and security issues. His notable books include Indo-European Union Strategic Cooperation (2016), Prayogik Sainya Vigyaan (2019), and Russia-Ukraine War: Strategic Conundrum (2025), published by Pentagon Press.

Mayank Saraswat is a Senior Research Fellow at the Department of Defence and Strategic Studies, Iswar Saran Degree College, University of Allahabad, Prayagraj, with a specialization in contemporary security and strategic affairs. His research focuses on military reforms, regional security, and non-traditional security challenges. He has published papers on several significant issues, such as the Agniveer scheme, the role of Gorkhas in Indian defence, Indo-Nepal strategic relations, the global impact of the Russia–Ukraine war, and human security. His work aims to bridge academic research with practical policy insights in India's defence and security discourse.