



# INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

## OUR SERVICES 2026



# TABLE OF CONTENTS

01	ABOUT US .....	03
02	BACKGROUND .....	03
03	AREAS OF WORK .....	05



# AREAS OF WORK

---

- AI STRATEGY AND GOVERNANCE
- DATA PROTECTION AND PRIVACY GOVERNANCE
- ADVISORY OF CYBER LAWS AND NORMS
- CYBER RESILIENCE FOR CRITICAL NATIONAL INFRASTRUCTURE
- CAPACITY BUILDING FOR LAW ENFORCEMENT
- CYBER DIPLOMACY
- GLOBAL COOPERATION IN CYBER RESILIENCE
- CYBER SAFETY OF CHILDREN AND ADOLESCENTS
- SAFEGUARDING WOMEN IN CYBER SPACE
- CYBER SAFETY AWARENESS FOR CONSUMERS
- ENSURING MENTAL WELLBEING WHILE USING TECHNOLOGY
- EDUCATION & CAPACITY BUILDING
- DIGITAL ECONOMY & INNOVATION
- TRADE PROMOTION & PARTNERSHIPS
- INDIA INVESTMENT ADVISORY
- SUSTAINABILITY & CLIMATE ACTION

# ABOUT US

---

India Future Foundation (IFF) leads initiatives to drive change in Digital, Internet Policies with an aim to foster & build Digital Ecosystems which guarantee Freedom of Expression, Trust and Safety for users.

IFF promotes online safety of Women and Children, works towards Prevention of Crimes Against Women on the Internet, creates Awareness in the Society about emerging online threats and leads action from the front to create an impact by working with Governments, Enterprises and Start-ups.

## BACKGROUND

---

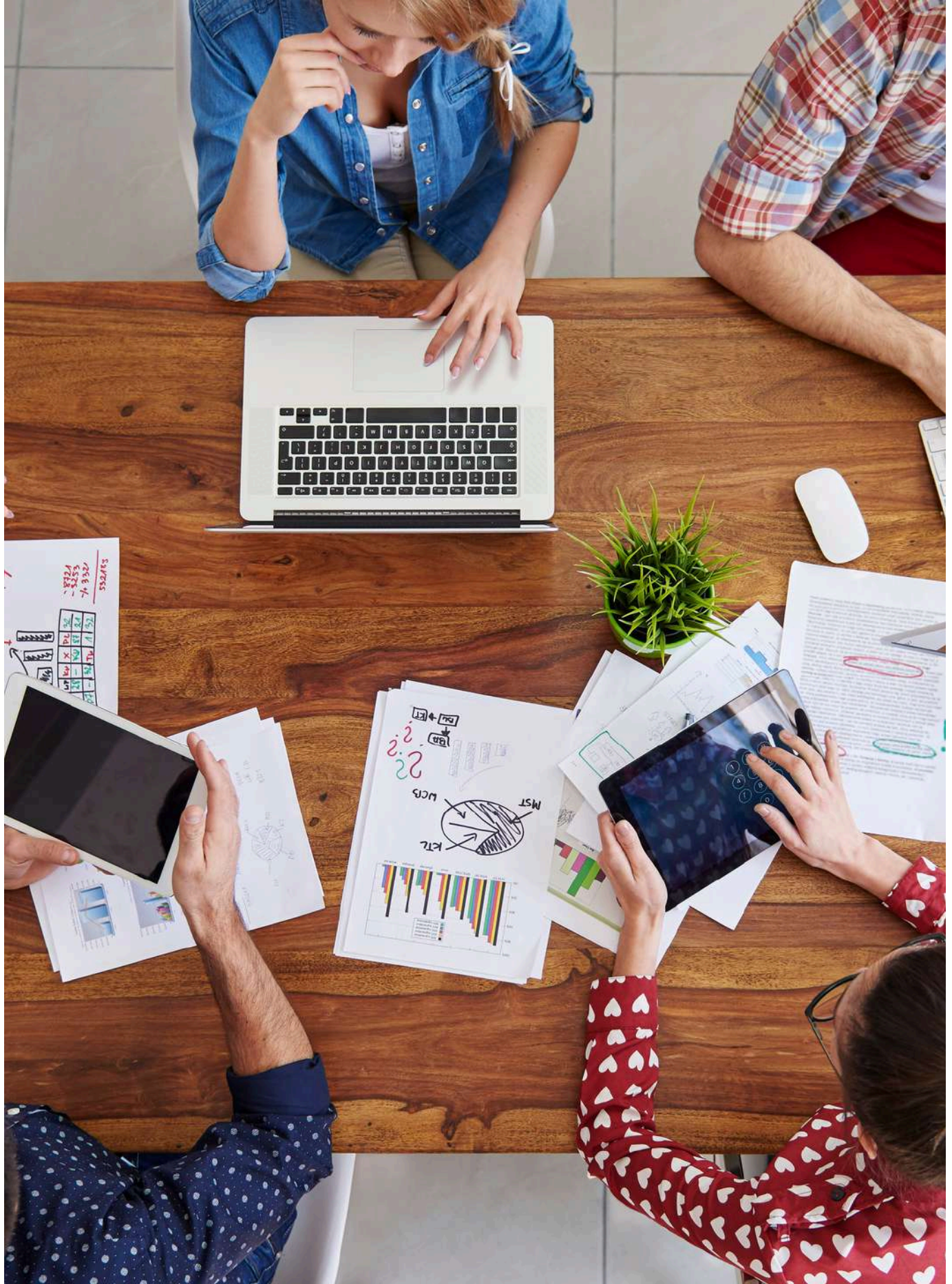
IFF was established on November 5th, 2018, as a section 8 company in India to make it Cyber Safe and Secure.

IFF aims to apply the income and the profits derived from the organisation's grants and funds, i.e. of cyber policy advisory, cybersecurity capacity building, cyber education and awareness programs to attain the above aim.

IFF has set up its registered office in Gurugram and set up local chapters for its India operations in 4 major cities, primarily Mumbai, Chennai, Bangalore and Trivandrum.

With 2 Chevening Cyber Security Fellows as founders and members from Industry, Academia and Indian Armed Forces, IFF plans to work on cybersecurity capacity building, training and global cyber security co-operation.





AREAS OF WORK



# AI STRATEGY AND GOVERNANCE



## **Strengthening regulation, security, and public trust in India's AI ecosystem**

As Artificial Intelligence (AI) evolves from an emerging technology into a transformative force shaping India's economy and society, the need for ethical, responsible, and secure AI governance has become critical. Establishing a comprehensive national framework for AI is a shared responsibility—one that must balance innovation with accountability.

To maximise the benefits of AI in improving productivity, enhancing public services, and safeguarding India's digital future, a robust national plan is essential. Such a plan must prioritise clear regulations, strong security measures, and the building of public trust to ensure AI is developed and deployed responsibly.

India Future Foundation (IFF) is at the forefront of shaping India's AI journey by facilitating informed and inclusive discussions on how AI should be governed, developed, and used. By convening senior government officials, policymakers, and leading legal and technology experts, IFF helps create pathways for effective and future-ready AI regulation in India.

The foundation's flagship AI Horizons initiatives provide a platform for dialogue, collaboration, and policy insight, contributing meaningfully to the development of India's AI governance framework.

Our Focus Areas Include The Following:

- **Ethical & Responsible AI** – Promoting transparency, fairness, and accountability in AI systems
- **AI Regulation & Governance** – Supporting the development of clear and adaptive policy frameworks
- **AI & Public Trust** – Strengthening confidence through safeguards, oversight, and explainability
- **AI Security & Risk Management** – Addressing threats related to misuse, bias, and data protection
- **AI in Public Services** – Leveraging AI to enhance efficiency, inclusion, and service delivery



# DATA PROTECTION AND PRIVACY GOVERNANCE





## **Strengthening data protection, trust, and accountability across India's digital ecosystem**

In an era where data is a valuable resource, strong regulations are essential to protect personal information and maintain public trust. The Digital Personal Data Protection (DPDP) Act, 2023 marks a major step in shaping India's secure and responsible digital future.

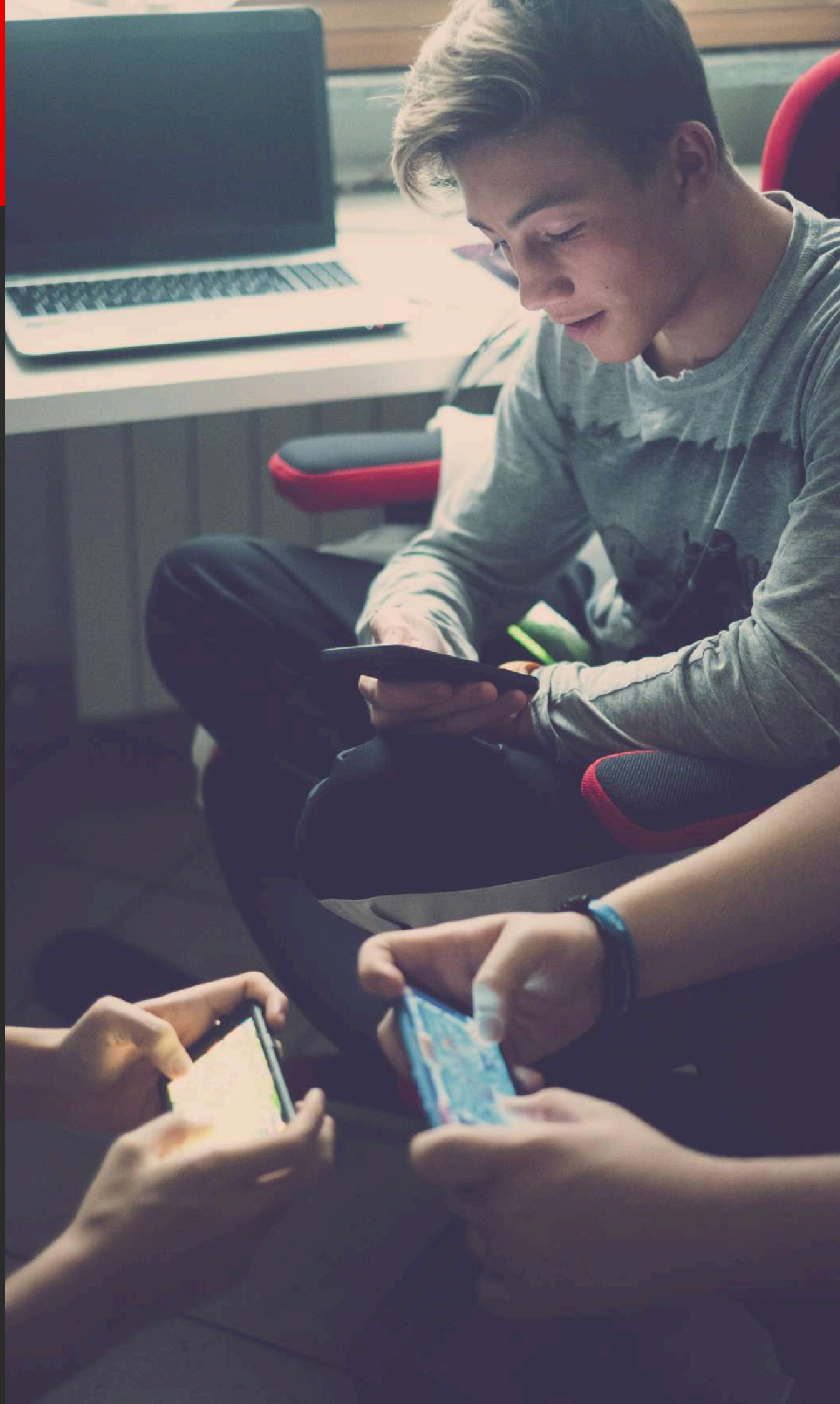
The India Future Foundation (IFF) supports organisations in understanding the requirements of the DPDP Act through expert-led workshops, panel discussions, and information sessions. These engagements help businesses and institutions navigate data privacy responsibilities with clarity and confidence.

IFF's sessions bring together senior government advisors, legal experts, business leaders, and Chief Information Security Officers (CISOs), enabling meaningful dialogue on compliance, governance, and best practices. The aim is to help organisations build data practices that are secure, trustworthy, and future-ready.

Key Focus Areas Include The Following:

- Overview of the DPDP Act, 2023
- Organisational roles and compliance responsibilities
- Consent, data handling, and protection measures
- Data security and breach preparedness
- Building trust in India's digital economy

# ADVISORY OF CYBER LAWS AND NORMS





## **Balancing innovation, regulation, and user safety in India's digital entertainment ecosystem**

The rapid growth of India's online gaming industry presents complex and evolving challenges for regulators, platforms, and consumers alike. As this sector expands, there is a growing need to strike the right balance between encouraging innovation and ensuring strong safeguards for user safety, data privacy, and online security.

India Future Foundation (IFF) plays a leading role in fostering informed dialogue on these critical issues. By convening experts and stakeholders, IFF helps shape policy conversations that are practical, inclusive, and future-ready.

IFF's initiatives focus on examining regulatory developments, understanding industry impact, and strengthening trust in India's digital entertainment ecosystem.

Sessions and discussions are designed to provide clarity on emerging regulations and support the development of a safe, responsible, and thriving online gaming environment in India.

Our Discussions & Dialogues Include The Following:

- **Online Gaming Rules** – Understanding proposed regulations and their impact on platforms, users, and innovation.
- **OTT Services & Digital Content Regulation** – Exploring policy frameworks governing digital entertainment services.
- **User Safety & Responsible Gaming** – Addressing consumer protection, harm prevention, and ethical design.
- **Data Privacy & Online Security** – Safeguarding user data and ensuring compliance with evolving digital laws.
- **Legal & Policy Perspectives** – Insights from leading legal experts, academicians, and senior policy advisors.
- **Industry Viewpoints** – Contributions from business leaders and executives from top technology companies.

# CYBER RESILIENCE FOR CRITICAL NATIONAL INFRASTRUCTURE





## **Strengthening national resilience, stability, and digital security**

At India Future Foundation (IFF), we support India's cyber defence ecosystem by addressing the growing risks faced by Critical National Infrastructure. These vital systems are increasingly targeted by sophisticated and persistent cyber threats, making strong, forward-looking security strategies essential for national stability and economic growth.

Our initiatives build awareness, preparedness, and collaboration by bringing together CISOs, senior government officials, industry leaders, and cybersecurity experts. Through focused discussions and practical insights, we help strengthen decision-making and response capabilities across critical sectors.

Our sessions combine real-world threat intelligence, sector-specific risk analysis, and strategic guidance, supporting organisations in defending essential national assets against emerging cyber threats.

Sessions can be delivered through specialised meetings, high-level workshops, or sector-focused engagements tailored to specific industries.

Our Focus Areas Include The Following:

- **Critical National Infrastructure Protection** – Understanding risks and national impact.
- **Advanced Cyber Threats & Threat Actors** – Identifying targeted and persistent attacks.
- **CISO Strategy & Leadership Workshops** – Strengthening cyber defence planning.
- **Public-Private Collaboration** – Enhancing coordinated national responses.
- **Sector-Specific Cyber Risks** – Addressing industry-focused threats.
- **Incident Prevention & Preparedness** – Reducing large-scale disruption risks.
- **Emerging Cyber Defence Strategies** – Preparing for future digital threats.

# CAPACITY BUILDING FOR LAW ENFORCEMENT





## **Strengthening investigation capabilities and technological readiness**

As the world becomes increasingly digitised, criminals are also leveraging advanced technologies to carry out nefarious activities. To stay ahead of such elements—and to ensure that cases are investigated thoroughly and taken to their logical conclusion—law enforcement agencies and the judicial system must remain updated with the latest technological developments.

At India Future Foundation (IFF), we work to bridge this critical skill gap by delivering specialised training programmes that build awareness and technical capacity among law enforcement and judicial personnel. Our programmes are designed to ensure that investigators remain one step ahead of technology-driven criminal activities.

Through collaborations with organisations such as the United Nations Office on Drugs and Crime (UNODC) and industry partners like Paytm, IFF has conducted hands-on training workshops across India, including New Delhi, Lucknow, Pune, and Jaipur.

Our Training Programmes Cover The Following:

- **Cyber & Technology-Enabled Crimes** – Understanding emerging digital crime patterns.
- **Open-Source Intelligence (OSINT)** – Leveraging publicly available data for investigations.
- **Call Detail Record (CDR) & Internet Protocol Detail Record (IPDR) Analysis** – Interpreting telecom and internet-related records.
- **Dark Web Investigations** – Understanding structure, access, and criminal use.
- **Social Media Investigations** – Tracking digital footprints and online behaviour.
- **Cryptocurrency & Financial Crimes** – Identifying and tracing crypto-based transactions.

# CYBER DIPLOMACY





## **Strengthening cyber relations, governance, and strategic trust between nations**

In an increasingly connected digital world, traditional diplomacy alone is no longer sufficient to address complex cyber challenges. Cyber diplomacy enables nations to use diplomatic engagement and international cooperation to manage cyberspace, regulate emerging threats, and promote responsible state behaviour.

IFF supports governments and institutions with practical tools, strategic frameworks, and capacity-building initiatives to strengthen cyber governance, enhance international partnerships, and align cyber efforts with foreign policy objectives.

Our Focus Areas Include The Following:

- **Cyber Diplomacy Strategy & Policy Development** – Designing national cyber diplomacy frameworks aligned with foreign policy goals.
- **International Cyber Cooperation** – Strengthening bilateral and multilateral cyber partnerships.
- **Internet Governance & Global Norms** – Supporting participation in international cyber governance processes.
- **Managing Offensive Cyber Capabilities** – Promoting responsible state behaviour and confidence-building measures.
- **Countering Cyber Espionage & State-Sponsored Threats** – Enhancing diplomatic responses to cyber incidents.
- **Digital Trust & Stability** – Building norms for a secure, open, and resilient cyberspace.
- **Capacity Building for Foreign Ministries** – Training diplomats and policymakers on cyber issues.
- **Strategic Dialogues & Track 1.5 Engagements** – Facilitating discussions between governments, experts, and stakeholders.

# GLOBAL COOPERATION IN CYBER RESILIENCE





## **Strengthening collaboration, trust, and shared responsibility in cyberspace**

In today's hyper-connected world, online threats have made geographical borders increasingly irrelevant. The safety of one nation is closely linked to the safety of all, reinforcing the idea that no one is truly secure if even one remains vulnerable. This reality makes international cooperation and cyber diplomacy essential to building effective and resilient cyber defence systems.

Strong cybersecurity cannot be achieved in isolation. It depends on continuous collaboration between countries and partners to share knowledge, expertise, and best practices. Working together enables collective resilience and more effective responses to evolving cyber threats.

India Future Foundation (IFF) actively supports this collaborative approach by participating in leading international forums and global engagements. Through these platforms, IFF contributes to cross-border dialogue, knowledge sharing, and capacity building.

IFF's work reflects the practical application of modern cyber diplomacy—combining diplomatic engagement with technical expertise to address cyber challenges and support cooperation on global norms and governance in cyberspace.

Through its partnerships with international organisations and stakeholders across regions, IFF strengthens global digital security while reinforcing India's role as a responsible and trusted contributor to international cyber stability.

# CYBER SAFETY OF CHILDREN AND ADOLESCENTS





## **Strengthening Awareness, Responsibility, and Safety in India's Digital Ecosystem**

India's rapid digital growth, driven largely by mobile Internet, has made online access widespread—but awareness about safe and responsible usage remains limited. Children and adolescents, as the most active users, face increased risks on social media and digital platforms.

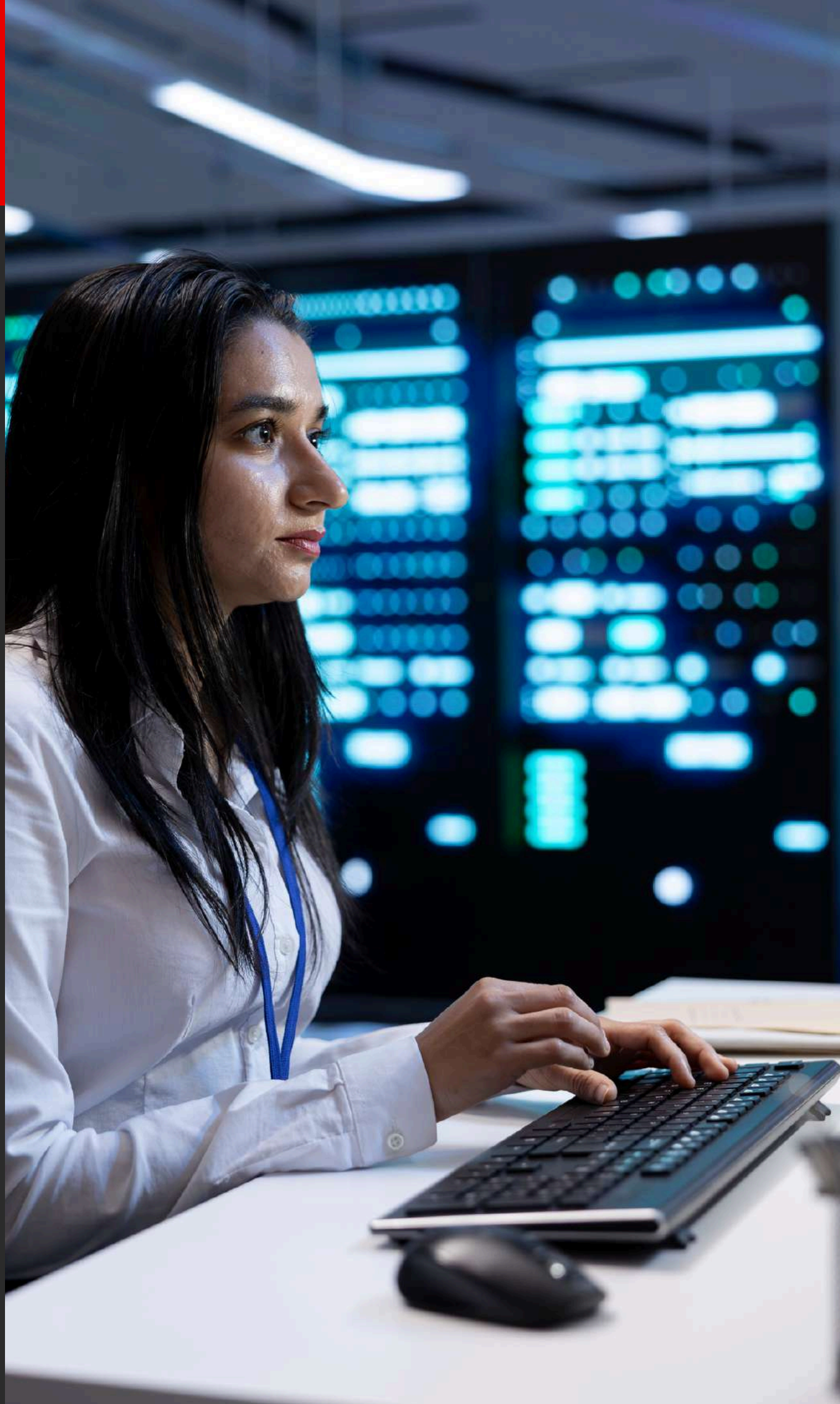
With online learning expanding screen time, exposure to cyber abuse, exploitation, and harmful content has grown. At the same time, cyber offences against children are becoming more frequent and sophisticated, making legal awareness and responsible digital behaviour essential.

To address these challenges, India Future Foundation (IFF) conducts workshops, seminars, and training programmes to promote digital safety and equip children, parents, educators, and stakeholders with the knowledge and skills needed for safer online engagement.

Our Awareness Programmes Focus On:

- **Responsible Internet & Social Media Usage** – Building healthy digital habits from an early age.
- **Online Safety & Child Protection** – Identifying risks of abuse, exploitation, and grooming.
- **Cyber Laws & Legal Awareness** – Understanding rights, responsibilities, and consequences.
- **Digital Wellbeing** – Managing screen time, stress, and online behaviour
- **Prevention of Cyber Crimes Against Children** – Awareness-driven protection strategies.
- **Empowering Young Users** – Encouraging informed, confident, and ethical digital citizenship

# SAFEGUARDING WOMEN IN CYBER SPACE





## **Strengthening safety, confidence, and resilience in the digital space**

Women increasingly use the Internet to build and strengthen personal relationships. However, research shows that young women, particularly those aged 18–24, face disproportionately high levels of online harassment. Nearly 26% have experienced online stalking, while 25% have been targets of online sexual harassment. The rapid spread of information through mobile devices has created new risks, making digital awareness essential.

Women are more vulnerable both online and offline. The anonymity offered by digital platforms has contributed to a rise in cyberbullying, including body shaming and targeted abuse. These behaviours often result in emotional distress and long-term psychological impact.

Cyber-crimes against women are committed with various intentions, including illegal gain, revenge, insult to modesty, extortion, blackmail, sexual exploitation, defamation, incitement of hate, and theft of personal information. In many cases, such crimes also contribute to serious mental health challenges.

India Future Foundation (IFF) works towards promoting a safe, gender-responsive, and equitable cyber space. Through webinars and workshops, conducted in collaboration with UN Women and various NGOs, IFF aims to safeguard women against online abuse, exploitation, and cyberbullying.

Our Focus Areas Include The Following:

- **Online Harassment & Cyberbullying** – Understanding risks and prevention strategies
- **Cyber Stalking & Sexual Harassment** – Recognising warning signs and response mechanisms
- **Digital Anonymity & Misuse** – Awareness of hidden online threats
- **Cyber Crimes Against Women** – Addressing extortion, blackmail, and defamation
- **Mental Wellbeing Online** – Managing stress and psychological impact
- **Safe Internet Practices** – Encouraging responsible and informed digital behaviour

# CYBER SAFETY AWARENESS FOR CONSUMERS





## **Strengthening awareness, trust, and confidence in the digital world**

In today's rapidly evolving digital age, personal safety extends beyond physical spaces into the online world. A secure digital environment empowers people to learn, work, create, and connect with confidence, while building trust in the technologies that shape modern life.

With increasing digitisation, cyber safety awareness has become a critical necessity. Every user of technology must be equipped with the knowledge to navigate the online space responsibly, securely, and ethically, ensuring a healthy and safe cyber ecosystem for all.

India Future Foundation (IFF) works towards creating a safer digital world through focused cybersecurity workshops, awareness programmes, and conferences. These initiatives support safe online learning, remote work, community engagement, and digital transactions by promoting responsible digital behaviour.

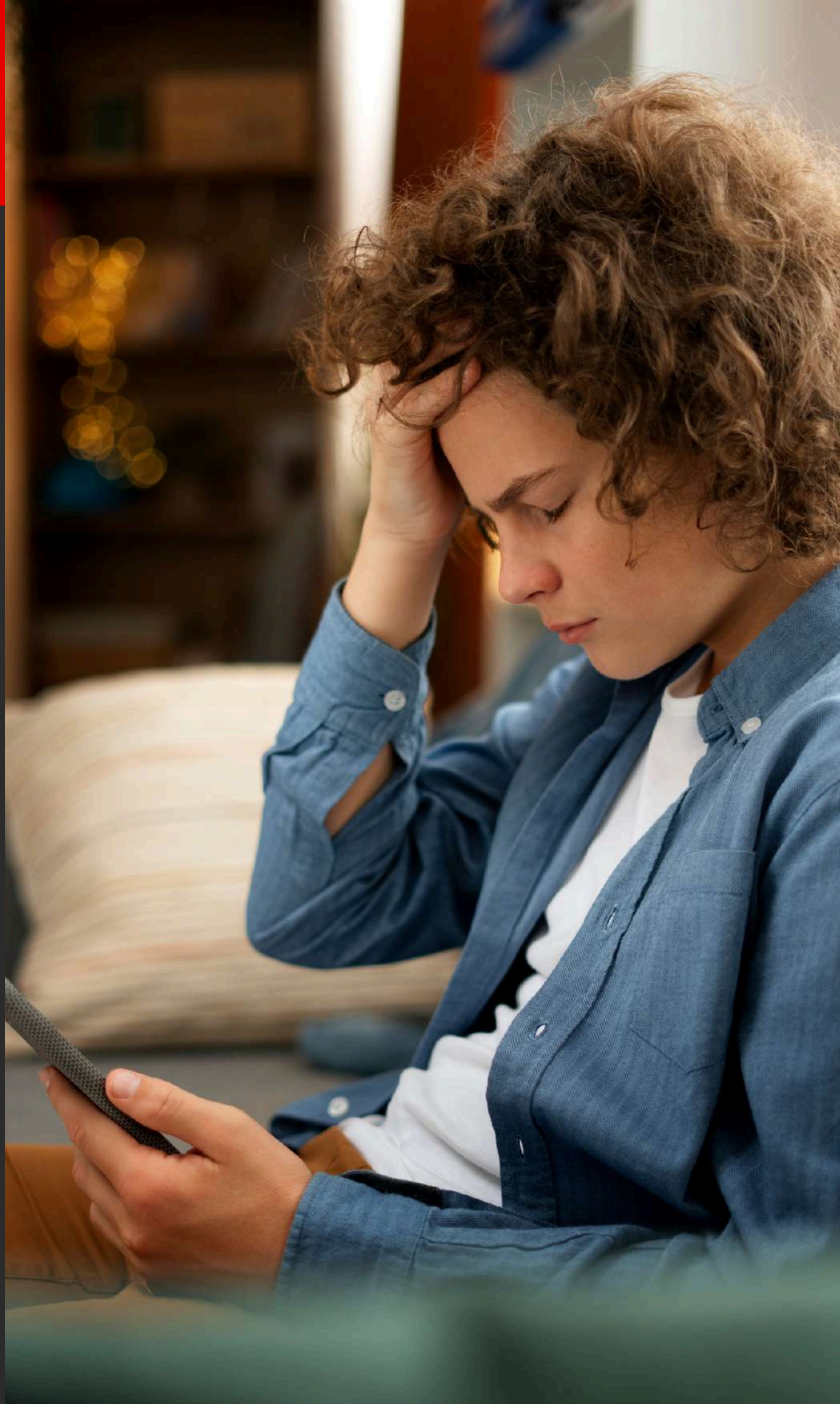
Our sessions combine current cyber trends, real-world case studies, and practical guidance, helping participants understand risks, improve awareness, and adopt safe digital practices.

Sessions can be delivered as 1 to 1.5 hour workshops or integrated awareness programmes, tailored to the needs of organisations and communities.

Our Programmes Include The Following:

- **Cyber Safety Awareness** – Understanding safe and responsible use of technology.
- **Online Privacy & Data Protection** – Protecting personal data and digital identity.
- **Cybercrime & Online Frauds** – Recognising threats and preventive measures.
- **Social Media Safety & Digital Footprint** – Managing online presence responsibly.
- **Misinformation & Fake Content** – Identifying manipulation and false information.

# ENSURING MENTAL WELLBEING WHILE USING TECHNOLOGY





## **Strengthening awareness, balance, and emotional resilience in the digital age**

In today's rapidly evolving digital landscape, technology has become an integral part of everyday life. From communication and learning to work and social interaction, digital tools now influence nearly every aspect of how we live.

The COVID-19 pandemic further accelerated this transformation, making work from home a widely adopted norm. While this shift ensured continuity and convenience, it also led to unintended consequences—longer working hours, continuous screen exposure, physical strain such as back pain, and increased digital dependency.

For many individuals, mobile phones are the first thing checked in the morning and the last thing used at night. Over time, this constant engagement can contribute to mental health challenges, including stress, anxiety, and depression.

Key Focus Areas Include The Following:

- **Digital Wellbeing** – Encouraging balanced technology use
- **Mental Health Awareness** – Reducing stigma and promoting dialogue
- **Emotional Support Systems** – Supporting both individuals and caregivers
- **Positive Use of Technology** – Leveraging digital tools for wellbeing
- **Community Engagement** – Building inclusive and supportive environments

# EDUCATION & CAPACITY BUILDING





## **Strengthening national resilience, institutional capability, and future-ready education**

In an increasingly digital world, capacity building and targeted education are critical to national development. The India Future Foundation (IFF) works across state institutions and the education sector to enhance digital readiness, security awareness, and long-term resilience.

IFF focuses on strengthening specialised capabilities within law enforcement and the judiciary, while also supporting the transformation of education through innovative technologies and strategies. Through tailored workshops and training programmes, IFF builds investigative, institutional, and academic capacity to address evolving digital challenges.

Our Programmes Include The Following:

- **Law Enforcement & Judicial Training** – Enhancing investigative and adjudicatory capacity in digital environments.
- **Digital Forensics** – Building practical skills for evidence collection, analysis, and attribution.
- **Open-Source Intelligence (OSINT)** – Leveraging publicly available data for intelligence and investigations.
- **Dark Web Investigations** – Understanding hidden online ecosystems and emerging criminal methodologies.
- **AI in Education** – Exploring applications of artificial intelligence to improve learning outcomes.
- **Academic Leadership Workshops** – Supporting institutional strategy and digital governance.
- **Administrative Efficiency through AI** – Using technology to streamline educational operations.
- **Cyber Awareness & Policy Readiness** – Aligning institutions with evolving digital risks and regulations.
- **Capacity Building for Educators** – Empowering teachers and administrators with future-ready skills.

# DIGITAL ECONOMY & INNOVATION





## **Advancing innovation while building robust digital governance**

In India's fast-growing digital economy, innovation and strong governance are key to sustainable growth. The India Future Foundation (IFF) works at this intersection by promoting emerging technologies while supporting the regulatory frameworks needed for a secure and trusted digital ecosystem.

Through expert-led workshops, IFF brings together policymakers, regulators, and legal specialists to shape India's AI governance roadmap, ensuring progress aligns with ethical, transparent, and responsible principles. At the same time, IFF demonstrates practical AI applications to boost productivity, especially across government and public sectors.

This focus on innovation is balanced with strong attention to compliance, particularly through IFF's work on explaining the Digital Personal Data Protection (DPDP) Act, 2023, helping organisations meet data privacy obligations and build long-term digital trust.

Key Areas of Engagement Include The Following:

- **AI Governance & Policy** – Supporting ethical, responsible, and transparent AI frameworks.
- **Technology Adoption** – Showcasing practical AI use cases in government and public sector.
- **Digital Regulation** – Strengthening understanding of emerging digital laws.
- **Data Protection & Privacy** – Decoding DPDP Act, 2023 for institutional readiness.
- **Trust & Digital Confidence** – Enabling a safe and reliable digital ecosystem.

# TRADE PROMOTION & PARTNERSHIPS





## **Strengthening international trust for a resilient digital commerce ecosystem**

In today's interconnected world—and increasingly in the future—the success of trade promotion and strategic partnerships will rely heavily on digital connectivity and international trust. The India Future Foundation (IFF) works to build this trust by fostering alliances that support a thriving and secure digital commerce ecosystem.

IFF's approach focuses on long-term collaboration, knowledge sharing, and strengthening institutional capacity—both within India and with international partners.

Key Areas of Engagement The Following:

- **Building Digital Trust** – Strengthening confidence in digital systems to support sustainable international trade and cooperation.
- **Strategic Partnerships** – Fostering alliances essential for the growth of a resilient digital commerce ecosystem.
- **Industry Collaboration** – Long-standing engagement with leading experts from the software and technology sector.
- **Capacity-Building Workshops** – Delivering targeted workshops aimed at strengthening India's digital infrastructure.
- **International Cooperation** – Working with global organisations, including the United Nations Office on Drugs and Crime (UNODC), on specialised law enforcement training.
- **Global Security Initiatives** – Supporting the implementation of international cyber and security frameworks.
- **Cyber Resilience Building** – Sharing Indian expertise to help partner nations strengthen their cyber capabilities.
- **Enabling Secure Trade** – Creating a predictable and secure digital environment for cross-border trade.
- **Global Digital Leadership** – Reinforcing India's position as a responsible and trusted actor in the global digital economy.

# INDIA INVESTMENT ADVISORY





## **Strengthening strategy, risk awareness, and growth across global markets**

In today's interconnected world, where businesses operate across time zones and borders, companies face a complex mix of political, financial, and legal challenges. To succeed in diverse geographies, organisations must clearly understand these challenges and respond with well-planned strategies.

At India Future Foundation (IFF), we support companies by providing timely investment advisories and strategic insights that help them navigate complex regional environments. Our work builds awareness, preparedness, and confidence—ensuring informed decision-making that supports sustainable growth and profitability.

Our advisories combine country-specific analysis, sectoral insights, and practical recommendations, enabling companies to manage risk, identify opportunities, and strengthen their presence in new and existing markets.

Studies can be delivered as focused advisories or detailed reports, tailored to specific companies, sectors, or regions

Our Advisory & Research Areas Include The Following:

- **Investment Advisories** – Understanding regional risks and opportunities.
- **Country-Specific Analysis** – Assessing political, economic, and legal landscapes.
- **Market Entry & Expansion Studies** – Supporting growth into new territories.
- **Sector-Focused Research** – Insights tailored to specific industries.
- **Strategic Risk Assessment** – Preparing companies for complex operating environments.
- **Profitability & Growth Planning** – Aligning strategy with long-term success.

# SUSTAINABILITY & CLIMATE ACTION





## **Strengthening national security, resilience, and trust across India's green energy ecosystem**

As India accelerates its transition towards renewable and sustainable energy, a critical vulnerability has emerged – the cybersecurity of green and digital infrastructure. From smart grids and renewable power systems to public utilities, these assets are increasingly dependent on digital technologies, making them potential targets for cyber threats.

The India Future Foundation (IFF) is addressing this challenge at the intersection of climate action and national security. IFF works on the principle that a successful green transition is only possible when the digital systems that support it are secure, resilient, and trusted.

IFF's initiatives focus on identifying cyber risks, strengthening governance frameworks, and building institutional capacity to protect India's sustainable infrastructure from evolving digital threats. By integrating cybersecurity into climate and energy policy discussions, IFF ensures that technological progress does not come at the cost of national security.

IFF's workshops on green energy cybersecurity serve as a key example of this commitment. These sessions bring together senior government officials, senior legal experts, and industry representatives to deliberate on emerging risks, regulatory gaps, and practical safeguards for critical infrastructure.

Sessions are designed as expert-led workshops and policy discussions, tailored to the needs of government bodies, regulators, and industry stakeholders.

Key Focus Areas Include The Following:


- **Cybersecurity of Smart Grids & Energy Systems** – Protecting digitally connected power infrastructure from cyber attacks.
- **Critical Infrastructure Protection** – Safeguarding public utilities essential to national functioning.
- **Climate-Tech & National Security** – Understanding cybersecurity as a pillar of India's green transition.
- **Policy & Regulatory Frameworks** – Strengthening laws and compliance mechanisms for sustainable infrastructure.



**INDIA FUTURE  
FOUNDATION**

## Contact Us

---

 [www.indiafuturefoundation.com](http://www.indiafuturefoundation.com)

