(Estd. 1870)
United Service Institution
of India

CyberPeace

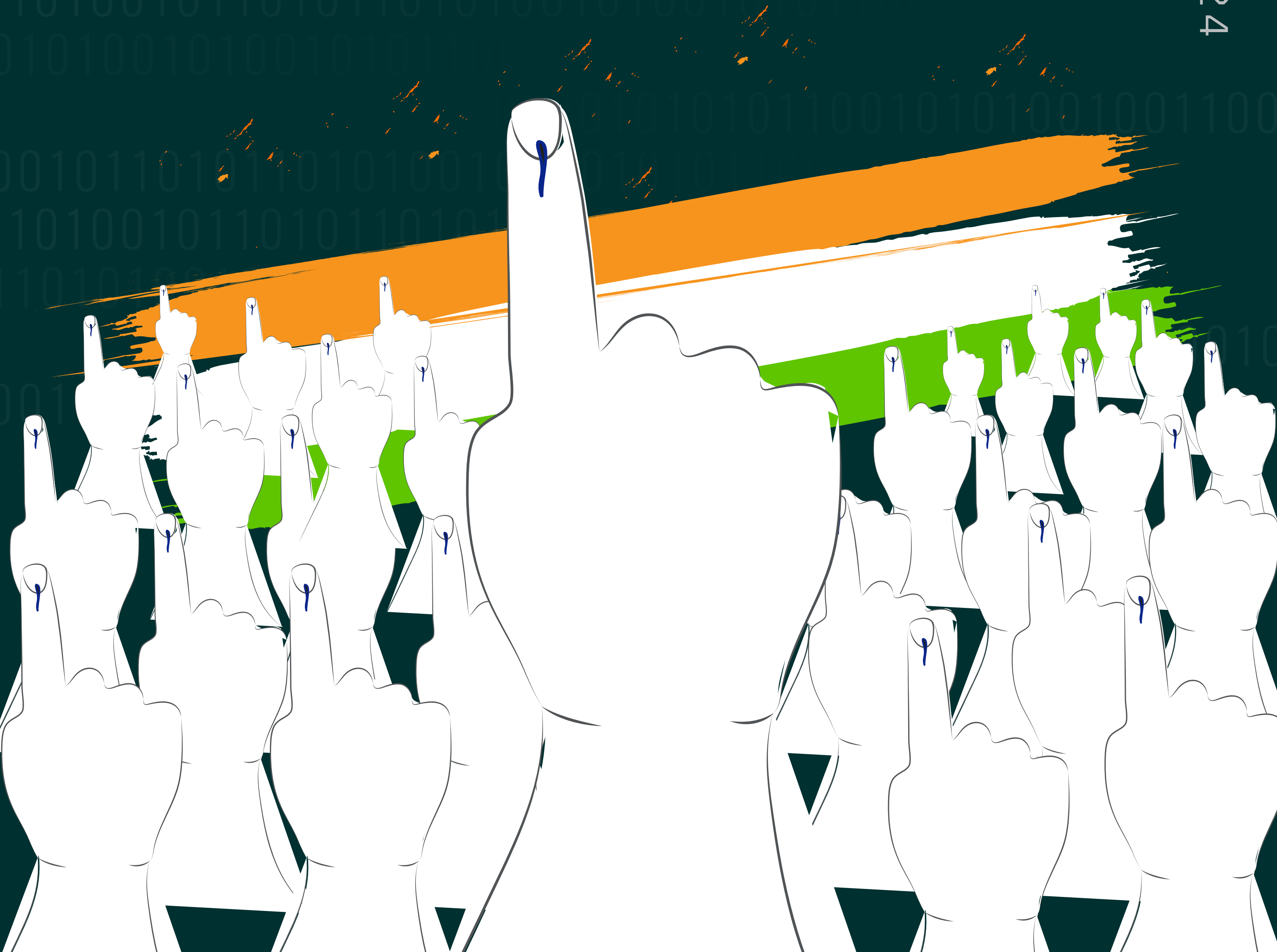
Indian Election 2024

Cyber Security E-Book

for Voters & Candidates

Indian Election 2024

Indian Election 2024

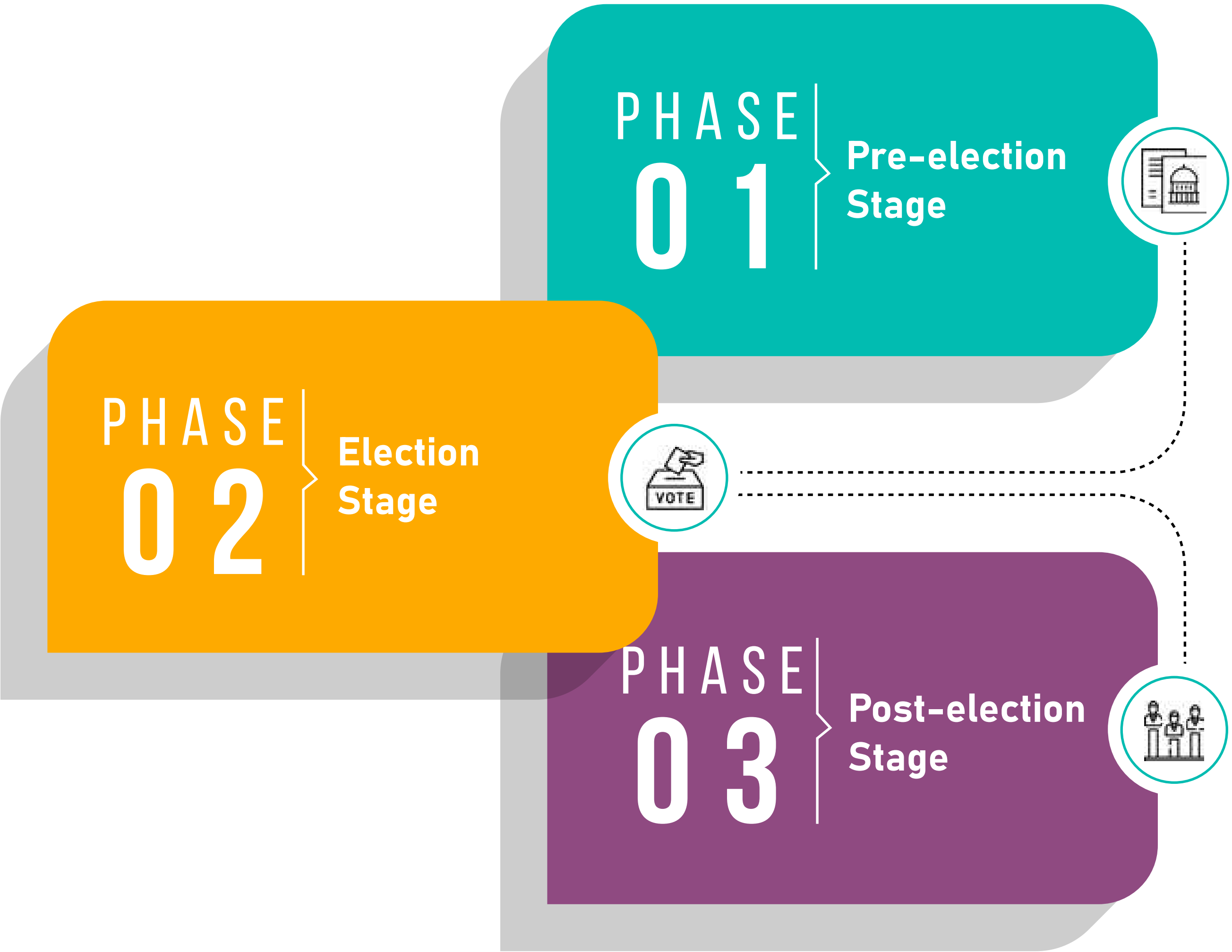


India hosts the world's largest election campaign, with over 800 million eligible voters and a complex electoral landscape in terms of population, geography and cultural diversity.

At every step of the election process, from filing candidate nominations to registering for voter IDs, the election campaign involves electronic devices and software. We are aware of the threats posed to the election process by physical foes, but the malicious intent to damage the election process through virtual means is a new menace. Apart from the traditional method of election campaigns, election campaigns are now also being conducted via social media platforms. It is noteworthy that clear information remains a critical consideration for the 2024 Elections. As per the World Economic Forum's 2024 Global Risk Report, India ranks highest amongst countries most vulnerable to the risk of misinformation and disinformation. Misinformation in India has emerged as a significant societal challenge, wielding a potent influence on public perception, political discourse, and social dynamics.

Sources of Misinformation During Elections

Misinformation and disinformation during elections is viewed under three phases;



Phase I, Pre-election stage: At the outset, the likelihood of an electoral process falling prey to misinformation and disinformation is highest during the pre-election stages: this includes information pertaining to lists and rolls, parties and candidates, voting mechanisms, campaign rules, funding, etc. Participating parties and candidates often misrepresent and falsify information in their electoral manifestos, directly impacting the voting public's decision-making process.

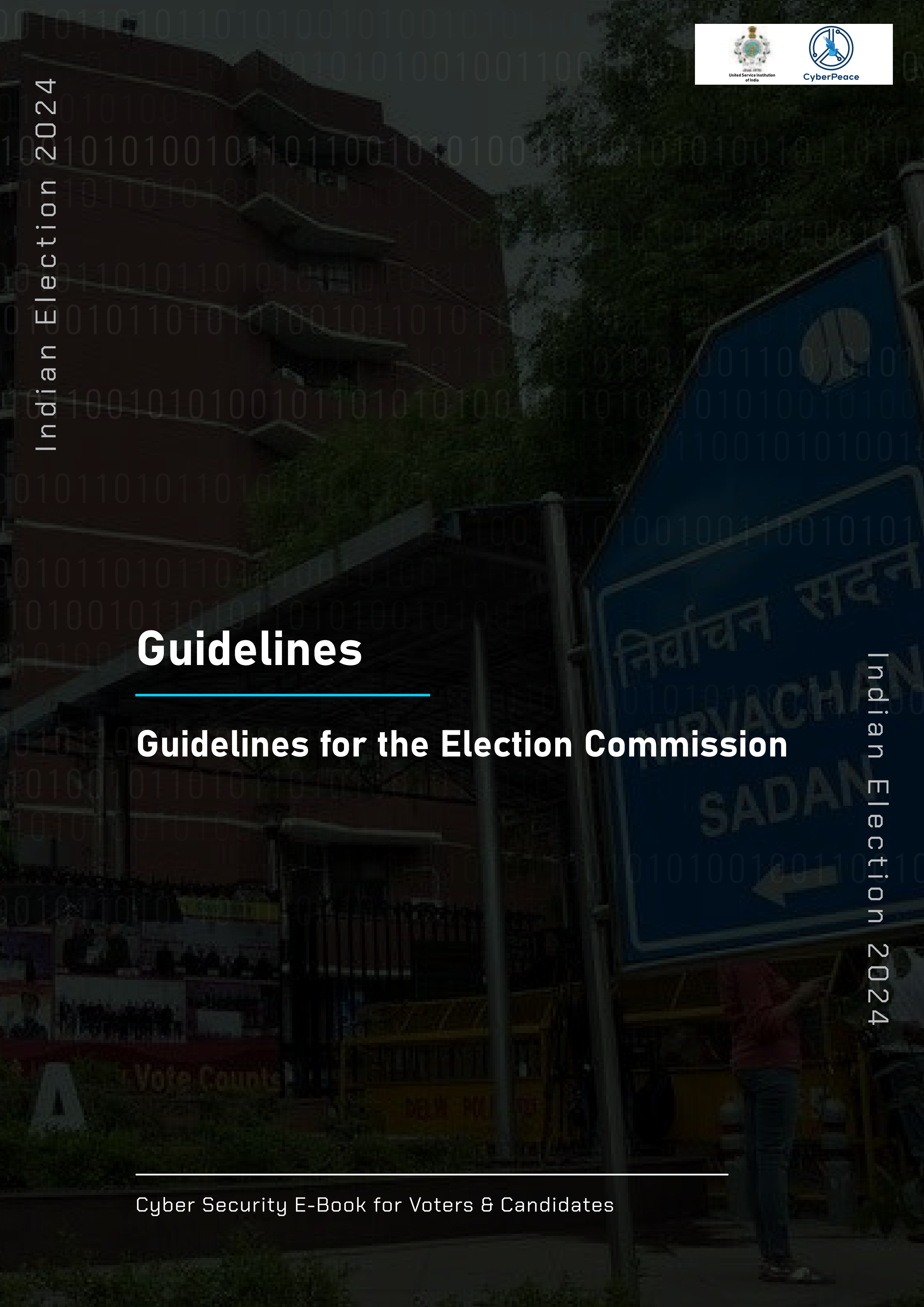
Phase II, Election stage: This includes logistics and election materials, party monitoring efforts, electoral experience, onsite vote counting, Selective Reporting Bias, etc.

Phase III, Post-election stage: Misinformation related to final results, fabricated footage of candidates or election-related events, etc.

United Service Institution of India

CyberPeace

Indian Election 2024



Guidelines

Guidelines for the Election Commission

Indian Election 2024

Cyber Security E-Book for Voters & Candidates

Guidelines for the Election Commission

01 Voters should be aware of the complete flow of the election process in India. This includes information on how the electoral rolls are made, how candidates are monitored, a complete database of candidates and party manifestos, candidate background, etc. For informed decision-making, active reading and information seeking is imperative. Given the low rate of literacy in India, a significant volume of the citizenry needs to be educated and this responsibility rests on the Election Commission and electoral bodies. Educational information as issued by the Election Commission may be improved in the following manner;

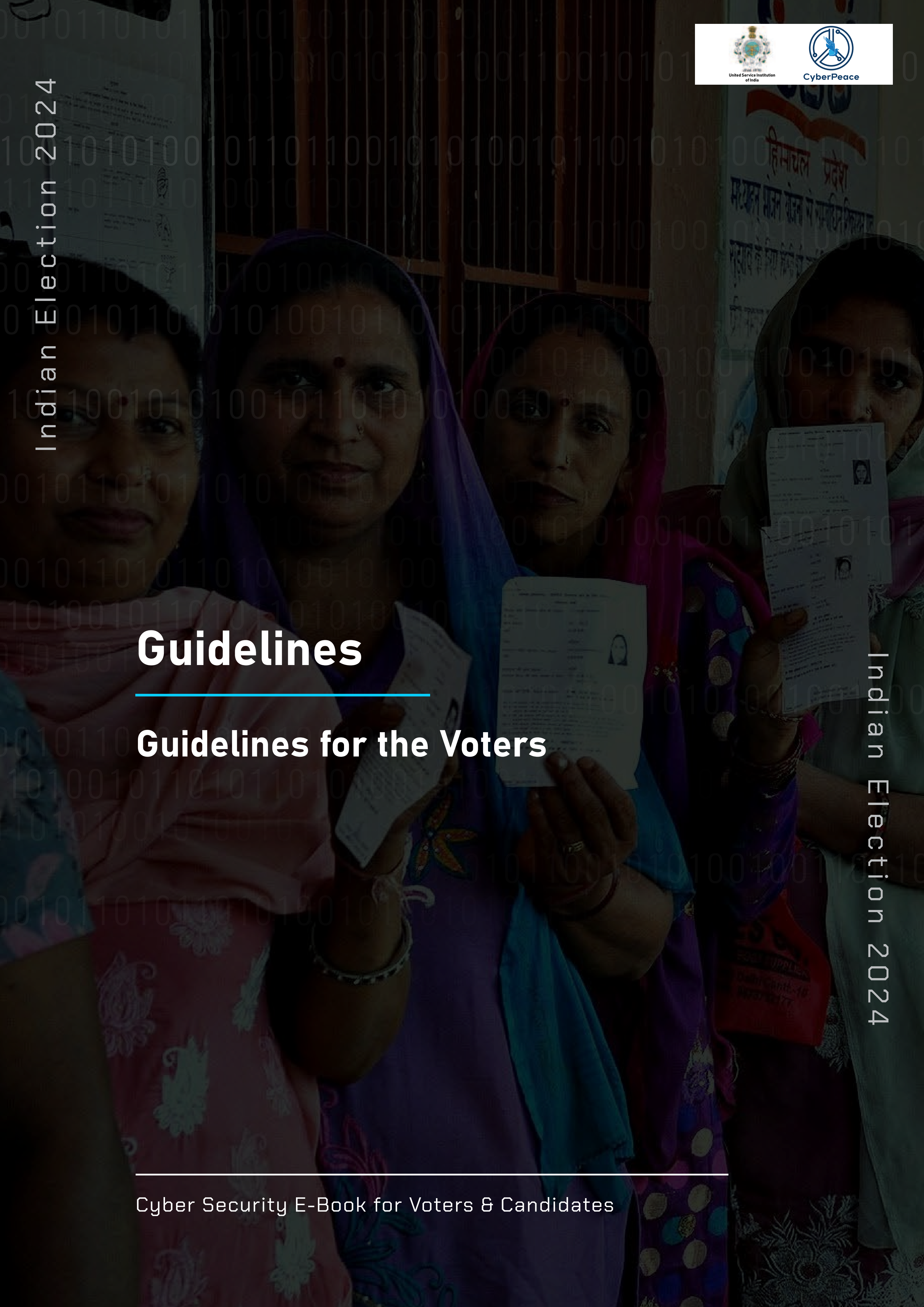
- Sources for electoral lists/rolls and candidature may be cited;
- Timelines for each pre-step in the electoral process (such as a timeline for validation of electoral rolls, removing ineligible voters from rolls, etc.) may be published;
- Publishing a list of officials and personnel who are appointed to oversee the voting stations and polling booths;
- Publishing the security protocols and Points of Contact for polling booths during election days;
- Publishing key information on the rights of voters and the roles and powers of public officials during election campaign periods and election day;
- Ensure that privacy measures are implemented during the election process to ensure data security.

02 Additionally, the Election Commission must deploy technology that bolsters electoral sanctity. These include using the following;

(a.) The Election Commission may consider deploying blockchain technology to ensure fair and systematic voting procedures. The risks posed by technology-based voting (such as risks of data breaches, legitimacy, manipulation of data, etc.) are addressed by blockchain technology since it offers decentralised, distributed, immutable and advanced security protection. Not only will it eliminate paper ballots, it will also promote transparency by bringing the voting process under public monitoring and eliminating electoral malpractice and corruption.

(b.) Additionally, the Election Commission may consider using algorithms that detect voter fraud, such as the one developed by a team of political scientists at CalTech. It consists of a two-tier mechanism: one detects dynamic changes in the voting records and the other monitors irregularities and anomalies in the changes. This background is used to track changes in voters' addresses and other details while scrutinising to ascertain if there are any inconsistencies in such changes. A third algorithm also scans data to isolate double votes.

03 The Election Commission must also sensitise voters on emerging cybersecurity threats and the impact they can have on the electoral procedure. These include issuing and publishing periodic advisory notifications in all schedule IX languages and ensuring comprehension through simple, easy-to-understand content.



United Service Institution of India

CyberPeace

Indian Election 2024

Guidelines

Guidelines for the Voters

Indian Election 2024

Cyber Security E-Book for Voters & Candidates

Guidelines for Voters

Use Multiple Sources

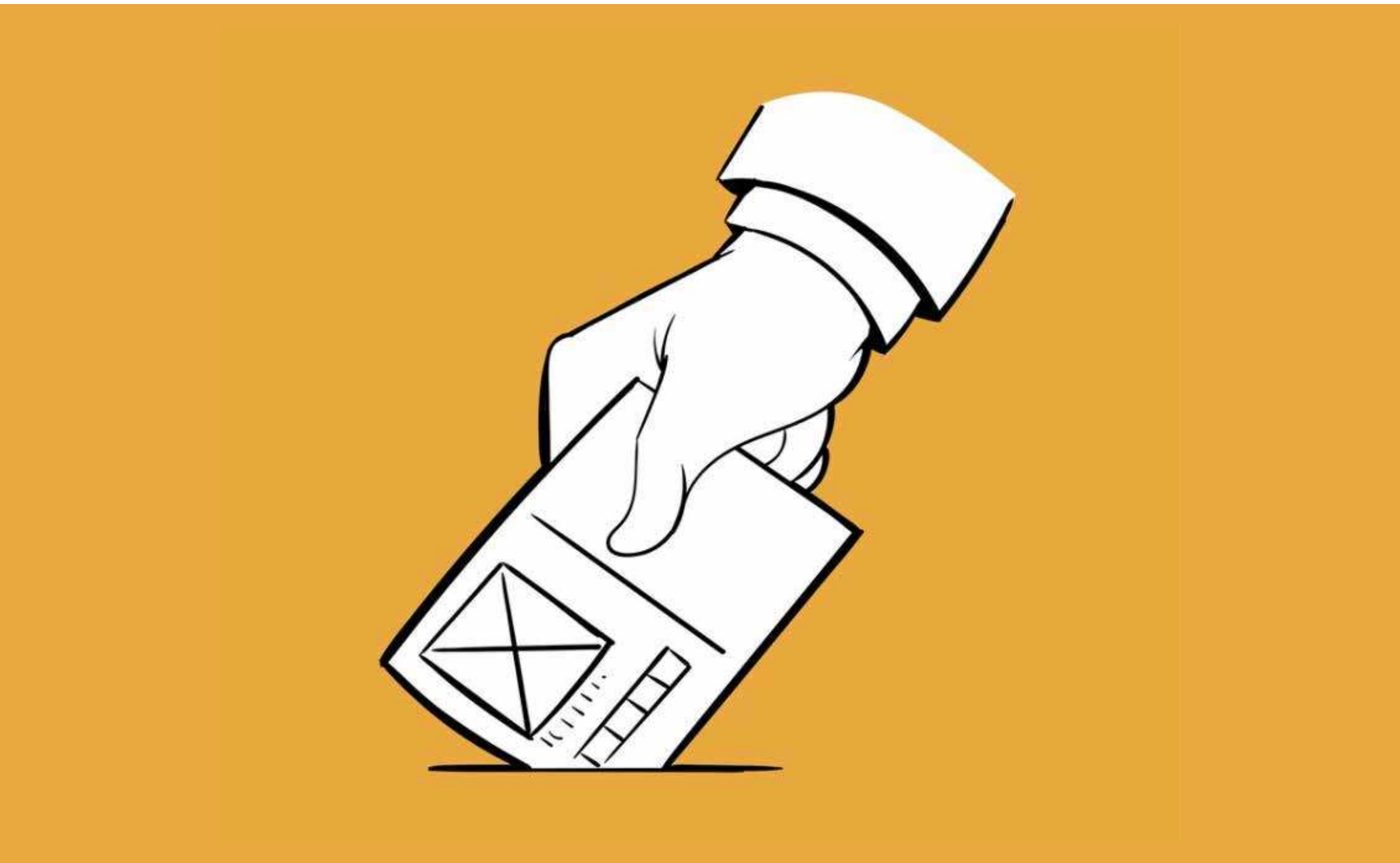
Voters must seek information from multiple sources. These include reading manifestos, parliamentary questions on public portals such as the Digital Sansad portal, advisory notifications from the Election Commission, etc.

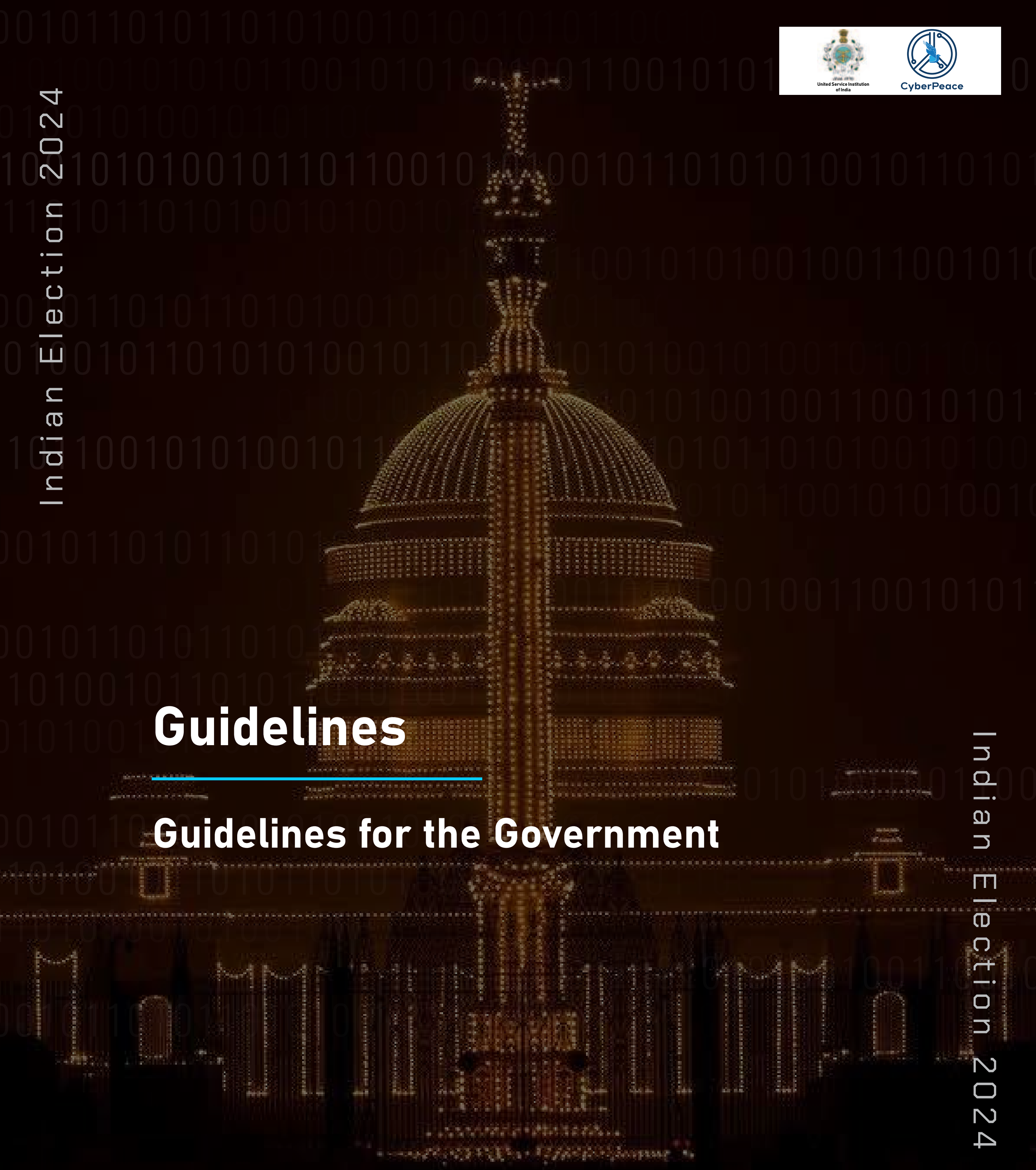
Consume News Responsibly

Voters must acquaint themselves with dependable news channels and various fact-checking organisations that ensure the integrity of news content.

The Voters Fact-Checking Resources

Reliable and trustworthy fact-checking tools are crucial to gauge the reliability of information sources in the digital space. Voters must be encouraged to use these tools to cross-check information from numerous sources and add a layer of verification on their own. This practice is essential to nurture a culture of critical thinking. This habit plays a critical role in empowering citizens against deceptive deepfakes and malicious misinformation, creating a more sound and resilient electorate.





Indian Election 2024

Indian Election 2024

Guidelines

Guidelines for the Government

Cyber Security E-Book for Voters & Candidates

Guidelines for the Government

Official Information Channels

There's a need to eliminate intermediary media corrupting the electoral information plaguing the election campaigns. Voters must have direct access to official statements and announcements to ensure authentic information is reached by voters. Cost-effective and easily accessible subscription models should be deployed by official government sources and reliable media, especially during elections, to minimise the spread of misleading content, protect the integrity of reliable election-related confirmation, and safeguard against electoral deepfakes.

Digital Literacy Clubs

To educate and empower the general public against the malice of electoral deepfakes and fake media, it is essential to establish an unshakeable foundation at the ground level. Free digital literacy clubs can be established in every locality to impart education on fake media, deepfakes and cyber resilience. An educated citizenry is an empowered citizenry.

AI Detection Apps

Along with fact-checking tools, specific apps can be developed using AI-based mobile applications to help users scan and check the authenticity of media sources on a real-time basis. These apps can act as the first line of defense against deceptive deepfakes and fake electoral media.

Synthetic Media

The great shift toward digital systems coincides with the proliferation of the synthetic generation of images, videos, and audio. Though cybersecurity experts have been warning about synthetic media and deepfakes, it appears the accessibility of these tools are reaching an inflection point. The difficulty in detecting deepfakes, especially considering cultural and linguistic diversity, highlights the need for advanced and localised detection tools which should be utilised for detection and taking down such content from the Internet.

United Service Institution of India

CyberPeace

Indian Election 2024

Guidelines

Guidelines for the Candidate

Indian Election 2024

Cyber Security E-Book for Voters & Candidates

Guidelines for Candidates

Resilience Certification: The administration should institute certification programs for political campaigns that test for and confirm resilience against deepfake attacks. This effort can be fortified with penetration testing at regular intervals. Certified campaigns via official channels are crucial for fostering a motivated and competitive atmosphere and pushing candidates to achieve AI resilience. All candidates must apply for and earn the certification to fulfill eligibility criteria.

Watermarking: This new technology must be used while creating all digital content to ensure authenticity. Fostering new partnerships with tech-based startups and firms specialising in the field is essential. The implementation of dynamic watermarking on electoral videos and other media can help ensure robust lines of defense against deepfakes and fake media, bolstering public trust in media sources. All candidates and parties must be encouraged to fulfill the responsibility of verifying the content they publish.

Deepfake Defense Drills: Various political campaigns can group together to participate in defense drills against deepfakes, misinformation and false media. These collaborative efforts can simulate authentic scenarios and devise strategies to safeguard electoral campaigns against the malice of AI and deepfakes. These collaborative drills can help in fostering a culture of sharing information and best practices to ensure campaigns are well-prepared against deepfakes and fake media.

AI Review Boards: An ethical review board comprising AI and ethics experts should be established to oversee electoral campaigns. All campaigns should be mandated to submit to a periodic ethical review of AI applications to ensure their alignment with proper AI principles. Annual reports should be published with outcomes and recommendations. This practice guarantees upholding ethical standards in the deployment of AI by electoral campaigns.

References

- https://www.statista.com/statistics/996930/india-lok-sabha-voting-related-information-availability/
- https://thewire.in/media/survey-finds-false-information-risk-highest-in-india
- https://www.statista.com/topics/5846/fake-news-in-india/#topicOverview
- https://www.weforum.org/publications/global-risks-report-2024/digest/
- https://www.caltech.edu/about/news/algorithms-seek-out-voter-fraud
- https://www.geeksforgeeks.org/generative-adversarial-network-gan/
- https://sansad.in/rs/questions/questions-and-answers
- https://www.thehindu.com/news/national/misinformation-harmful-for-society-democracy-norms-against-deepfakes-after-elections-ashwini-vaishnaw/article67928669.ece

USI-CYBERPEACE

CENTER OF EXCELLENCE

Rao Tularam Marg, opposite Signals Enclave,
Anuj Vihar, Vasant Vihar, New Delhi, Delhi 110057