CYBERSECURITY

INFORMATIONS ABBREVIATIONS ACRONYMS

Towards a healthy safe & secured childhood
CHILDREN OF INDIA FOUNDATION

Terre des Hommes Netherlands

MESSAGE FROM THE TRUSTEE

Children of India Foundation (CIF) is a women-led organisation established in 2002 in Tamil Nadu, India. Guided by the vision of “A world in which every child attains the right to survive and develop appropriately,” CIF is committed to serving children and their families in the poorest communities in India. CIF is an affiliate of Terre des Hommes - Netherlands (TdH NL), a non-governmental organisation working across 16 countries to prevent child exploitation and promote children’s rights.

In partnership with TdH NL and 8 network partner organisations across 5 states, CIF is implementing the **Stepping Up Fight Against Sexual Exploitation of Children (SUFASEC) project**. This initiative aims to ensure children live free from sexual exploitation, with a specific focus in India on combating **Online Child Sexual Exploitation (OCSE)**—a rapidly growing issue in the digital age.

OCSE is a severe and escalating problem, exposing children to online predators and exploitation through digital platforms. Tackling this issue is complex due to limited awareness, technological barriers, societal stigma, and resource gaps. Protecting children from this threat is a pressing priority.

A cornerstone of the SUFASEC project is the engagement of Youth Ambassadors, who play a vital role by leading peer-to-peer education initiatives on online safety, sensitising parents, caregivers, and service providers, conducting research to support advocacy and action. Their dedication strengthens our mission and ensures meaningful community engagement in addressing OCSE.

Despite challenges, there are significant opportunities, including leveraging technology for child safety, enhancing policy frameworks, engaging communities, and fostering youth-led innovations to create safer digital environments.

This booklet, comprising 197 abbreviations of terms essential for understanding and achieving cybersecurity, underscores our commitment to empowering children, parents, teachers, and community actors with critical knowledge and tools to combat OCSE.

I extend my heartfelt gratitude to the CIF programme, communication, and research teams for their tireless efforts in developing this resource and to the Youth Ambassadors for their selfless contributions to our mission. Together, we can create a safer, exploitation-free future for children.

Thangaperumal Ponpandi
Trustee, Children of India Foundation

ACO (Automated Content Optimization): A process that uses algorithms to automatically adjust content for better visibility and performance.

Address Bar Spoofing: This technique makes a malicious URL appear like a legitimate one on the address bar. It is padded with special characters to show only a portion of the complete URL or the legitimate web address.

ADS (Automated Detection System): A system that automatically detects potential threats and alerts security teams.

Advanced Persistent Threat - APT is concerted and stealthy attacks against specific organisations. APT groups are generally government based and they make use of highly sophisticated malware to breach an organisation's security defences.

AES (Advanced Encryption Standard): A widely-used encryption standard for securing data transmissions.

AI (Artificial Intelligence): A field of computer science that enables machines to learn and make decisions autonomously.

AIOps - Artificial Intelligence for IT Operations: The application of artificial intelligence to automate IT operations.

AIT (Artificial Immune Technology): A cybersecurity defence strategy mimicking biological immune systems to detect and eliminate threats.

API (Application Programming Interface): A set of tools and protocols used to build and integrate software applications.

APT - Advanced Persistent Threat: A prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period.

BEC (Business Email Compromise): A scam in which cybercriminals impersonate executives to steal sensitive data or funds.

BGP - Border Gateway Protocol: A protocol for exchanging routing information across the internet, crucial for internet traffic management.

BIM - Building Information Modelling: A digital representation of physical and functional characteristics of a facility, often used in construction and architecture.

BOTNET: A network of infected devices, connected to the Internet, used to commit coordinated cyber-attacks without their owners' knowledge.

C2S - Client to Site: A type of connection in network communications, often referring to a VPN connection.

Cache Cramming: It is a technique to trick a browser into running malicious Java code from the local disk, instead of the Internet. The execution of local code (which runs with less permissions) enables online criminals to access the target computer.

CASB (Cloud Access Security Broker): Security software that enforces cloud data policies for access and usage.

CDR (Content Disarm and Reconstruction): A cybersecurity technology that removes potentially malicious content from files while preserving usability.

CERT (Computer Emergency Response Team): A group of experts who respond to cybersecurity incidents and emergencies.

CKC (Cyber Kill Chain): A framework that breaks down the stages of a cyberattack to understand and mitigate threats.

Clickjacking: Clickjacking is an attack that fools users into thinking they are clicking on one thing when they are actually clicking on another. It allows cybercriminals to hide malware and other threats under the content of legitimate sites.

CLOUD on the internet: Servers that are accessed over the Internet, and the software and databases that run on those servers, instead of hosted locally.

COOP (Continuity of Operations Plan): A strategy for maintaining business functions during emergencies or disruptions.

CPE (Common Platform Enumeration): A structured naming system for IT products and platforms to standardise their identification.

CPTED - Crime Prevention Through Environmental Design: A strategy used to deter crime, including child exploitation, by modifying the physical environment (Maxwell, 2023).

Creepshots: A secretly taken photograph or short video of a person (usually of a girl or woman) focusing on sexualised areas of the body such as the breasts, groyne, or buttocks.

CSA - Child Sexual Abuse: A term used to describe any sexual activity with a child, including exploitation and abuse, which can have severe psychological effects on victims (Singh et al., 2014).

CSAM - Child Sexual Abuse Material: Any audio or visual material that sexualizes or exploits a child, often used in discussions about online exploitation (Maxwell, 2023).

CSE - Child Sexual Exploitation: A term that encompasses various forms of sexual exploitation of children, including trafficking and online exploitation (Maxwell, 2023).

CSEC - Commercial Sexual Exploitation of Children: A term that refers to the sexual exploitation of children for commercial purposes, including prostitution and pornography (Maxwell, 2023).

CSEM - Child Sexual Exploitation Material: Similar to CSAM, this term refers to materials that depict the sexual exploitation of children, often used in legal and law enforcement contexts (Babchishin et al., 2018).

CSRF (Cross-Site Request Forgery): A security vulnerability that tricks users into performing actions they didn’t intend to.

CTI (Cyber Threat Intelligence): Information collected and analysed about potential or existing cyber threats.

CTO - Chief Technology Officer: The executive responsible for an organisation's technology strategy and infrastructure.

CVE - Common Vulnerabilities and Exposures: A list of publicly disclosed cybersecurity vulnerabilities, providing a reference for security professionals.

Cyber flashing: the act of sending someone unwanted and unsolicited sexual images or videos. This is typically done via social media, dating apps, text messaging, or Bluetooth, such as Apple Airdrop. It can be considered an image-based form of sexual abuse.

DAC (Discretionary Access Control): A method where the owner of the data decides who can access it.

DANE (DNS-based Authentication of Named Entities): A protocol for securing email communications by validating DNS records.

Dark Web: It is a hidden network that requires a special browser to access. Due to its anonymous nature, the dark web is mostly used for illicit and even illegal purposes like the buying and selling of illegal drugs, weapons, passwords, illegal pornography, etc.

DDoS - Distributed Denial of Service: An attack that aims to make a service unavailable by overwhelming it with traffic from multiple sources.

Deepweb: The deep web, also known as the invisible or hidden web, is the part of the internet that is not indexed by search engines like Google, Yahoo, and Bing. The deep web includes pages that are not indexed, private databases, fee-for-service sites, and the dark web.

Digital house arrest: is a cyber scam where criminals use AI-generated audio/video calls to impersonate law enforcement, creating fear and falsely accusing victims of wrongdoing related to their Aadhaar/ phone number often leading victims to transfer money to avoid imminent arrest.

Disinformation: It is false information deliberately spread to deceive people. Disinformation is an orchestrated adversarial activity in which actors employ strategic deceptions and media manipulation tactics to advance political, military, or commercial goals.

DLP - Data Loss Prevention: Strategies and tools designed to prevent data breaches and unauthorised data transfers.

DLP - Data Loss Prevention: Technology that helps ensure that sensitive data is not lost, misused, or accessed by unauthorised users.

DMARC (Domain-based Message Authentication Reporting & Conformance): An email authentication method that prevents email spoofing.

DMZ - Demilitarized Zone: A physical or logical subnetwork that contains and exposes an organisation's external-facing services.

DNS - Domain Name System: The system that translates domain names into IP addresses, enabling users to access websites using human-readable addresses.

DNSSEC (DNS Security Extensions): Adds security to DNS by ensuring the integrity and authenticity of DNS responses.

DoS - Denial of Service: An attack that prevents legitimate users from accessing a service by overwhelming it with requests.

DPO (Data Protection Officer): A role responsible for ensuring that an organisation complies with data protection regulations.

Drive-by Download Attack is an unintentional download (without clicking on anything, pressing download, or opening a malicious email attachment) of malicious code to your computer or mobile device that leaves you vulnerable for cyber-attacks.

Droppers are programs designed to extract other files from their own code. Typically, these programs extract several files into the computer to install a malicious program package. Droppers may have other functions apart from dropping files.

EASM (External Attack Surface Management): Monitoring and managing vulnerabilities outside of an organisation's immediate IT environment.

ECC (Elliptic Curve Cryptography): A public-key encryption method that provides the same level of security as traditional methods with smaller key sizes.

ECSP (External Cyber Security Policy): Guidelines that regulate how an organisation handles cybersecurity threats from external sources.

EDR - Endpoint Detection and Response: Security solutions that monitor and respond to threats on endpoints, providing visibility and control.

ENCRYPTION: Securing digital data using one or more mathematical techniques, along with a password or key used to decrypt the information.

EPP (Endpoint Protection Platform): A system that protects endpoints like laptops and smartphones from malware and cyber threats.

Exploit kit that is used on the internet: Exploit Kit or exploit pack is a type of toolkit cybercriminals use to attack vulnerabilities in systems so they can distribute malware or perform other malicious activities.

FDE (Full Disk Encryption): Encryption that protects all data on a disk by converting it into unreadable code.

FIDO (Fast Identity Online): A set of standards for user authentication that replaces passwords with stronger authentication methods.

FIM - File Integrity Monitoring: A process of verifying the integrity of operating system and application software files.

FISMA - Federal Information Security Management Act: A U.S. law that requires federal agencies to secure their information systems and data.

GDPR - General Data Protection Regulation: A regulation in EU law on data protection and privacy, establishing guidelines for the collection and processing of personal information.

GRC (Governance, Risk, and Compliance): A framework that helps organisations manage risk and comply with regulations.

Hash Value: Hash values can be thought of as fingerprints for files. During digital forensic investigations, hash values play a major role in both file identification and deduplication.

HIDS - Host Intrusion Detection System: Monitors a single host for suspicious activity, providing alerts for potential security breaches.

HIPAA - Health Insurance Portability and Accountability Act: U.S. legislation that provides data privacy and security provisions for safeguarding medical information.

HITRUST - Health Information Trust Alliance: An organisation that helps the healthcare industry address security and privacy challenges.

HMAC (Hashed Message Authentication Code): A code generated by combining a cryptographic hash function with a secret key to ensure data integrity.

HSM (Hardware Security Module): A physical device that safeguards and manages digital keys for strong authentication and encryption.

IaaS (Infrastructure as a Service): Cloud computing service that provides virtualized computing resources over the internet.

IAM - Identity and Access Management: Framework for managing digital identities and access permissions within an organisation.

ICAC - Internet Crimes Against Children: A task force program initiated by the U.S. Department of Justice to combat child exploitation and abuse online (Maxwell, 2023).

ICS (Industrial Control Systems): Systems used to control industrial processes such as manufacturing, production, and utilities.

IDPS - Intrusion Detection and Prevention System: A device or software application that monitors a network or system for malicious activity.

IDS (Intrusion Detection System): A tool that monitors network traffic for suspicious activity and issues alerts.

IIoT (Industrial Internet of Things): The use of IoT devices in industrial settings for monitoring and control.

Info Stealer: Info Stealer is a Trojan that is designed to gather information from a system (generally login info, like usernames and passwords) which it sends to another system either via email or over a network.

IoC - Indicator of Compromise: Digital artefacts that suggest an attack has taken place or is in progress.

IOC (Indicators of Compromise): Clues or evidence that a system has been compromised by a cyber-attack.

IoT (Internet of Things): The interconnection of devices via the internet to exchange data and communicate with each other.

IPS - Intrusion Prevention System: Monitors network traffic and takes action against detected threats, blocking malicious activity.

IPsec (Internet Protocol Security): A protocol suite for securing internet protocol communications through authentication and encryption.

ISMS (Information Security Management System): A systematic approach to managing sensitive company information so that it remains secure.

ITSM - IT Service Management: A set of practices for delivering IT services that meet the needs of an organisation.

JBOC (Joint Business Operations Center): A centralised hub where multiple organisations collaborate on business operations, often in crisis situations.

JSON - JavaScript Object Notation: A lightweight data-interchange format easy for machines to parse.

LDAP - Lightweight Directory Access Protocol: An open, vendor-neutral application protocol for accessing and maintaining distributed directory information services.

LFI (Local File Inclusion): A vulnerability that allows attackers to include files from a server or device into the web application.

LSO (Local Shared Objects): Data stored on a user's machine, often by websites or applications, for various purposes including tracking.

Malvertisement: Malvertisements are infected online ads hosted on malicious / legitimate sites. If a user clicks on a malvertisement, the user's system becomes infected with a malware. The use of infected ads allows cybercriminals to spread malware easily.

MDM - Mobile Device Management: A type of security software used to monitor, manage, and secure employees' mobile devices.

MFA (Multi-Factor Authentication): A security system that requires two or more methods of authentication from independent categories of credentials.

Misinformation: A wrong information which is given to someone, (intentional or unintentional to harm anyone) in a deliberate attempt to make them believe something which is not true.

ML (Machine Learning): A branch of artificial intelligence focused on the development of algorithms that enable computers to learn from and make decisions based on data.

MSSP (Managed Security Services Provider): A third-party company that manages and monitors security services on behalf of businesses.

MTC: CM3 - Multiphasic Typology of Child Molesters: A classification system used to categorise different types of child sexual offenders based on their behaviours and motivations

NAC (Network Access Control): Security policies that restrict unauthorised devices from accessing a corporate network.

NAT (Network Address Translation): A method of mapping multiple private IP addresses to a single public IP address.

NDR (Network Detection and Response): A security technology that detects and responds to suspicious network activity.

NGAV - Next-Generation Antivirus: Antivirus software that uses machine learning and behavioural analysis to detect malware.

NGFW (Next-Generation Firewall): A firewall that offers advanced features such as application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

NIDS (Network Intrusion Detection System): A system that detects malicious activity within a network by monitoring network traffic.

NOC (Network Operations Center): A centralised location where IT professionals monitor and manage networks, servers, and other IT infrastructure.

OAuth (Open Authorization): An open standard for access delegation used by many major tech platforms for secure authorization.

OODA (Observe, Orient, Decide, Act): A decision-making framework often applied in cybersecurity to detect, analyse, and respond to threats.

OSCP (Offensive Security Certified Professional): A certification for ethical hackers and penetration testers.

OTP (One-Time Password): A password that is only valid for a single session or transaction to enhance security.

PaaS (Platform as a Service): A cloud service model that delivers applications over the internet.

PAM (Privileged Access Management): A security strategy focused on controlling and auditing access to critical systems by privileged users.

PATCHING on the internet: Applying updates to firmware or software to improve security and/or enhance functionality

PFS (Perfect Forward Secrecy): A cryptographic technique that ensures session keys cannot be compromised even if long-term keys are.

PIV - Personal Identity Verification: A standard for secure and reliable identification of federal employees and contractors in the U.S.

PKI (Public Key Infrastructure): A framework for creating, managing, distributing, and using digital certificates and public-key encryption.

PoLP (Principle of Least Privilege): A security concept that restricts users' access rights to the minimum necessary to perform their jobs.

Polymorphic Viruses: These are complex file infectors that can create modified versions of themselves (by encrypting their codes and using different encryption keys every time) to avoid detection yet retain the same basic routines after every infection.

RAID - Redundant Array of Independent Disks: A data storage virtualization technology that combines multiple physical disk drive components.

RANSOMWARE: A software that makes data or systems unusable until the victim makes a payment.

RAT - Remote Access Trojan: Malware that allows unauthorised remote access to a user's computer, often used for data theft.

RCE (Remote Code Execution): An attack that allows hackers to execute code on a remote device or server.

RDP - Remote Desktop Protocol: A protocol that allows remote access to a computer's desktop, enabling users to connect to their systems from different locations.

RFI - Remote File Inclusion: A vulnerability that allows attackers to include external files in a server-side script.

Rootkit: It is a program that installs and executes code on a system without end user consent or knowledge and maintains undetectable presence. Once installed, an attacker can perform virtually any function on the system.

RPO - Recovery Point Objective: The maximum acceptable amount of data loss measured in time, indicating how often data backups should occur.

RTO - Recovery Time Objective: The maximum acceptable amount of time to restore a system after a disaster, guiding disaster recovery planning.

SAC - Sexual Assault Counsellor: A trained professional who provides support and counselling to victims of sexual assault, including child victims (Maxwell, 2023).

SAML - Security Assertion Markup Language: An open standard for exchanging authentication and authorization data between parties, often used in single sign-on implementations.

SANE - Sexual Assault Nurse Examiner: A registered nurse who has received specialized training to provide care for sexual assault victims, including children (Maxwell, 2023).

SART - Sexual Assault Response Team: A coordinated team of professionals who respond to sexual assault cases, ensuring that victims receive appropriate care and support (Maxwell, 2023).

SASE - Secure Access Service Edge: A security framework that combines network security functions with WAN capabilities to provide secure access to applications.

SAT - Security Awareness Training: Training programs to educate employees about cybersecurity best practices and awareness of potential threats.

SAV - Sexual Assault Victim: A term used to describe individuals, including children, who have experienced sexual assault or abuse (Maxwell, 2023).

SCP - Secure Copy Protocol: A protocol used to securely transfer files between local and remote hosts.

SDLC - Software Development Life Cycle: A process used by software developers to design, develop, and test high-quality software.

SDN - Software-Defined Networking: A networking architecture that enables the network to be intelligently and centrally controlled.

SDP - Software-Defined Perimeter: A security approach that controls access to resources based on user identity rather than IP address.

SDR - Software-Defined Radio: A radio communication system where components are implemented by means of software.

SD-WAN - Software-Defined Wide Area Network: A virtual WAN architecture that allows enterprises to leverage any combination of transport services.

SIEM - Security Information and Event Management: A solution that provides real-time analysis of security alerts.

SIM - Subscriber Identity Module: A small card in a mobile device that holds subscriber information and encrypts communication.

SIM cloning, also known as SIM swapping, is a technique used by cybercriminals for cloning a phone's SIM to duplicate a SIM card. This can lead to unauthorised access to sensitive data, financial transactions, and even leading to sexual exploitation.

SIP - Session Initiation Protocol: A protocol used to initiate, maintain, and terminate real-time sessions for voice, video, and messaging applications.

SMB - Server Message Block: A protocol for sharing files, printers, and other network resources over a network.

SMTP - Simple Mail Transfer Protocol: An internet standard for email transmission.

SOAR - Security Orchestration, Automation, and Response: A technology that helps coordinate, automate, and respond to security alerts.

SOC - Security Operations Center: A centralised unit that deals with security issues on an organisational and technical level, monitoring and analysing security events.

SOCIAL ENGINEERING: Manipulating people into carrying out specific actions, or divulging information, that's of use to a cybercriminal.

SOP - Standard Operating Procedure: Established procedures to be followed in carrying out operations, particularly in response to security incidents.

SPEAR PHISHING: A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

SPF - Sender Policy Framework: An email validation system designed to prevent spam by verifying sender IP addresses.

SQLi - SQL Injection: A code injection technique that might destroy your database and exploit SQL vulnerabilities.

SSH - Secure Shell: A protocol for securely accessing and managing network services over an unsecured network.

SSL - Secure Sockets Layer: A protocol for establishing a secure connection over the internet, ensuring data privacy between applications.

SSO - Single Sign-On: An authentication process that allows a user to access multiple applications with one set of login credentials, enhancing user convenience.

Stalkerware: Stalkerware is a type of spyware or monitoring software that allows someone to secretly spy on another person's device and private life. It is used for cyberstalking by abusers.

STIX - Structured Threat Information Expression: A standard for sharing cyber threat intelligence.

STP - Spanning Tree Protocol: A network protocol that ensures a loop-free topology for Ethernet networks.

TDP - Threat Detection and Prevention: A process that uses security tools to identify and respond to potential cyber threats.

The Onion Router: The Onion Router is a technology stack that hides your web activity by routing and obscuring it through multiple nodes, like the layers of an onion. It is essentially a network that masks online traffic.

TIC - Trauma-Informed Care: An approach to treatment that recognizes the impact of trauma on individuals, particularly relevant for survivors of child sexual abuse.

TKIP - Temporal Key Integrity Protocol: A security protocol used in WPA to secure wireless networks.

TLS - Transport Layer Security: A protocol that ensures privacy and data integrity between communicating applications over a network.

Trace evidence: It occurs when objects make contact, and material is transferred. This type of evidence is usually not visible to the naked eye and requires specific tools and techniques to locate by the cyber specialists while investigating cyber crimes.

Trojan: A Trojan, or Trojan horse, is a type of malware that disguises itself as a legitimate file or program to gain access to a device. The term comes from the Greek myth of the Trojan Horse, where Greek warriors hid inside a wooden horse and tricked Trojans into bringing it inside their city walls.

TTP - Tactics, Techniques, and Procedures: The behaviour or modus operandi of cyber adversaries, used for threat intelligence.

UAC - User Account Control: A security feature in Windows that helps prevent unauthorised changes to the operating system.

UAV - Unmanned Aerial Vehicle: A drone used for various applications, including surveillance and data collection.

UEFI - Unified Extensible Firmware Interface: A specification that defines a software interface between an operating system and platform firmware.

UEM - Unified Endpoint Management: Solutions that integrate the management of multiple endpoint devices for security and efficiency.

UPS - Uninterruptible Power Supply: A device that provides backup power in the event of a power failure.

URL - Uniform Resource Locator: The address used to access a particular resource on the internet.

UTM - Unified Threat Management: An approach to security that provides multiple security functions within a single device or platform.

VA - Vulnerability Assessment: The process of identifying, quantifying, and prioritising vulnerabilities in systems and networks.

VAPT - Vulnerability Assessment and Penetration Testing: A combination of services to detect and address vulnerabilities.

VCISO - Virtual Chief Information Security Officer: A remote CISO service that provides expert guidance on security strategies.

VDI - Virtual Desktop Infrastructure: A technology that hosts desktop environments on a central server.

VLAN - Virtual Local Area Network: A logical grouping of devices on a network that allows for segmentation and improved security.

VPC - Virtual Private Cloud: A private cloud hosted within a public cloud that isolates an organisation's cloud resources.

VPN - Virtual Private Network: A service that encrypts your internet connection to enhance security.

VSS - Volume Shadow Copy Service: A technology in Microsoft Windows that allows for backup copies or snapshots of computer files.

WAF - Web Application Firewall: A security system that monitors and filters HTTP traffic to and from a web application to protect against attacks.

WAN - Wide Area Network: A telecommunications network that extends over a large geographical area

WEP - Wired Equivalent Privacy: A security algorithm for wireless networks, now largely replaced by WPA.

WHALING: Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

WHITELISTING: Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications.

Whitespace Padding: It is an action inserting spaces before a filename extension to disguise the real extension of the file. Malware authors do this so that, in a fixed-width column, the extension is no longer seen and a false extension is seen instead by the user.

WIFI - Wireless Fidelity: A technology that allows electronic devices to connect to a wireless local area network (WLAN).

VSS - Volume Shadow Copy Service: A technology in Microsoft Windows that allows for backup copies or snapshots of computer files.

WLAN - Wireless Local Area Network: A local area network that uses wireless data connections.

WPA - Wi-Fi Protected Access: A security protocol and security certification for securing wireless networks.

XDR - Extended Detection and Response: A unified security solution that detects and responds to threats across multiple layers.

XSS - Cross-Site Scripting: A security vulnerability that allows attackers to inject malicious scripts into web pages viewed by users.

YARA - Yet Another Recursive Acronym: A tool aimed at helping malware researchers identify and classify malware.

ZKP - Zero Knowledge Proof: A cryptographic method that allows one party to prove to another that a statement is true without revealing the information.

ZTA - Zero Trust Architecture: A security model that assumes that threats could be both external and internal, requiring verification for every access request.

About DtZ SUFASEC

Sexual exploitation of children (SEC) is a grave violation of children's rights and affects millions of children and youth annually, regardless of gender. No region, country or child is immune. However, girls, boys and children with other gender identities face differing levels of risk to different manifestations of SEC depending on their intersectional vulnerability factors. It impacts heavily and long-lasting on their physical, emotional and mental well-being. It deprives children and youth of establishing healthy (sexual) relationships and from developing to the best of their potential. The DtZ SUFASEC programme is designed to combat SEC. It will work in 12 countries in Latin America and Southeast Asia: Bangladesh, Bolivia, Brazil, Colombia, Dominican Republic, Guatemala, India, Indonesia, Laos, Nepal, Philippines and Thailand.

About Children of India Foundation

Children of India Foundation, an affiliate of Terre des Hommes Netherlands in India, is a non-profit organisation which empowers children and families from socio-economically vulnerable communities. We address child labour, child marriage and child sexual exploitation, ensuring access to education, health care, livelihood and child protection.

About Terre des Hommes Netherlands

Terre des Hommes Netherlands (TdH NL) is an international child protection organisation working to tackle exploitation of children at the roots. In India, TdH NL works to address child labour, empowers victims of child marriage, addresses exploitation of children in the Devadasi system and advocates against child marriage and child trafficking.

Towards a healthy safe & secured childhood
CHILDREN OF INDIA
FOUNDATION

Terre des
Hommes
Netherlands