Toolkit:
Youth Guide to (TFGBV)

By Dr. Lela Mirtskhulava
Protection/Technology
Specialist

Tbilisi 2023

MERCY CORPS

What is TFGBV?

TFGBV Definition by UNFPA!

UNFPA has defined TF GBV as “an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person on the basis of their gender.”[1]

When it comes to TFGBV, there are two key facts to remember:

- It is gendered – women and girls are targeted simply because they are women and girls.
- It is broader than online violence, and while it does take place online and in digital spaces, it can also come about through any type of technology – old and new – such as phones, GPS tracking devices, drones or recording devices that are not connected to the Internet.

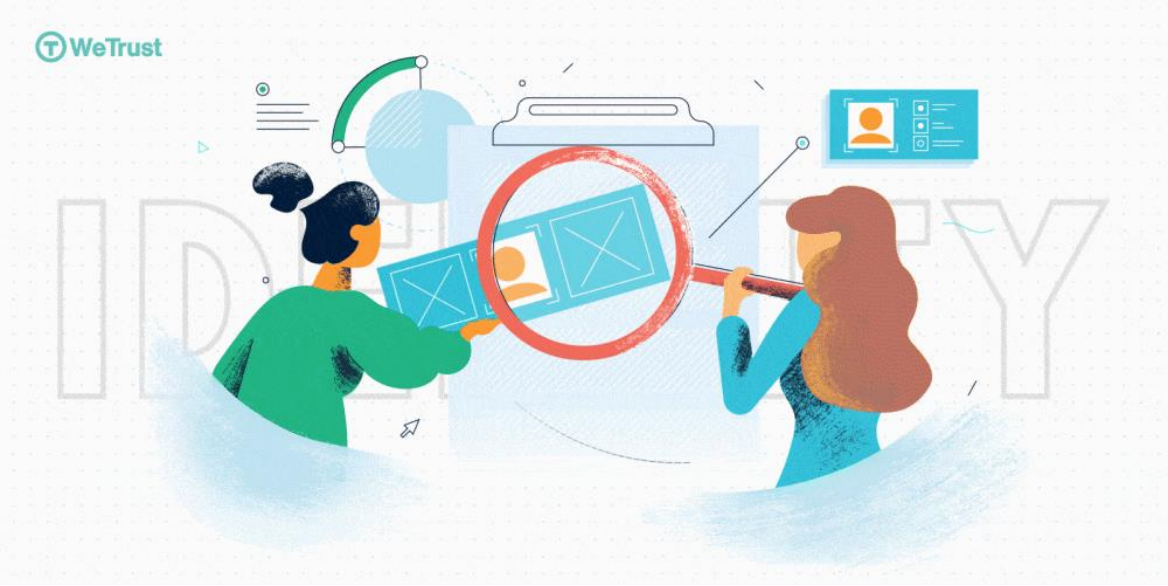
In short: the virtual is real.

MERCY CORPS

Digital Inclusion & Safety

Digital inclusion is not possible without digital safety![1]

That is, benefiting from digital products is not possible without ensuring the safety and security of users. The prevalence of the internet and digital products has presented a tremendous opportunity to create, build, and regulate a more equal future for women and girls.



https://blog.wetrust.io/how-digital-identity-will-power-financial-inclusion-69be0d0a0cb0

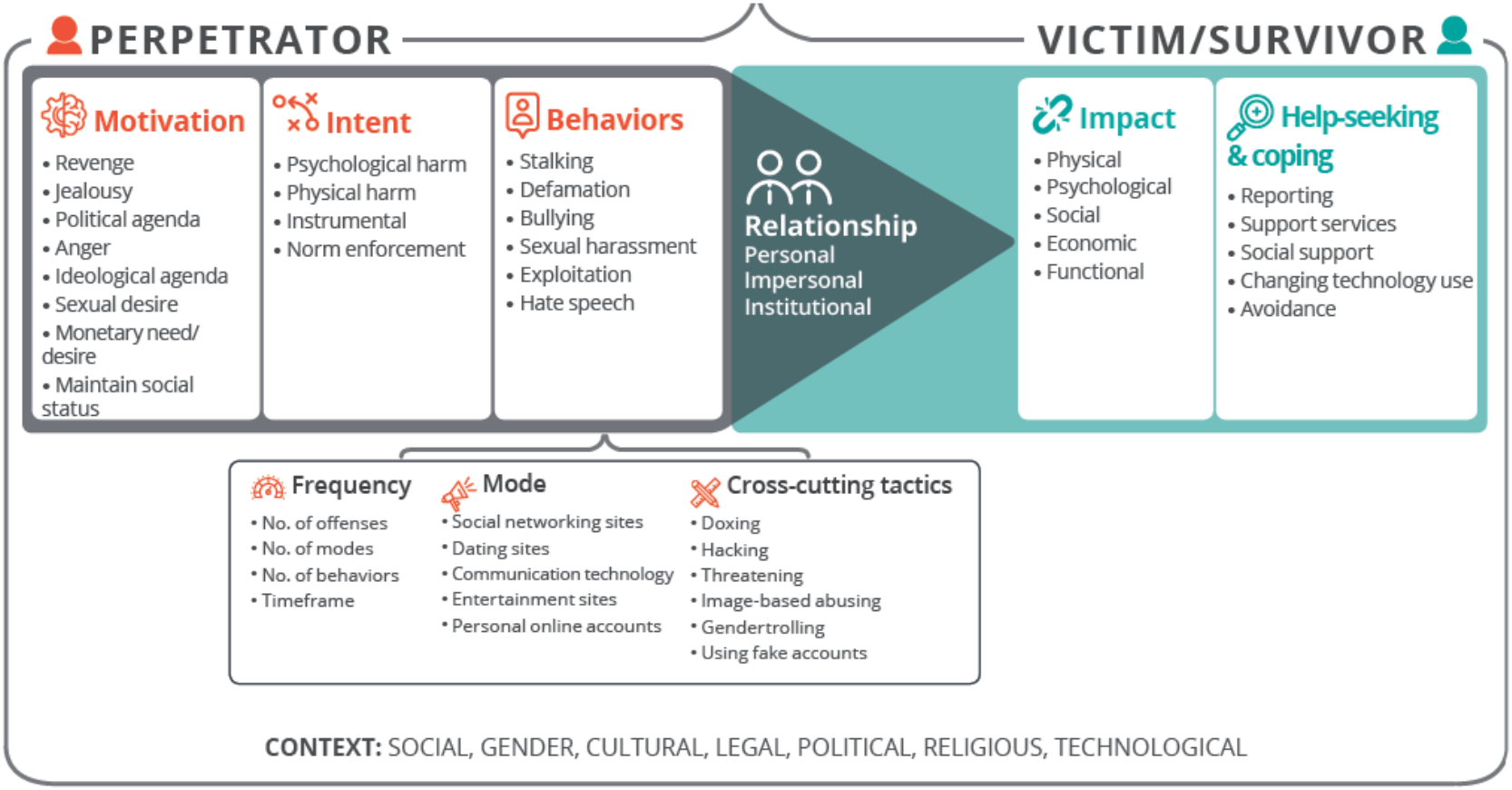
MERCY CORPS

Digital Inclusion & TFGBV

Digital life provides vital spaces for women seeking expression and opportunity including access to basic education and services and yet it is simultaneously a vector for perpetrators and abusers (individuals, groups and collectives) targeting women and adolescent girls because of their gender. Technology-facilitated gender-based violence (TF GBV) comprises a spectrum of behaviors, including stalking, bullying, sexual harassment, defamation, hate speech, exploitation, and is associated with mis and disinformation and violent extremism, which are perpetrated online or using technology.

MERCY CORPS

Technology-facilitated gender-based violence



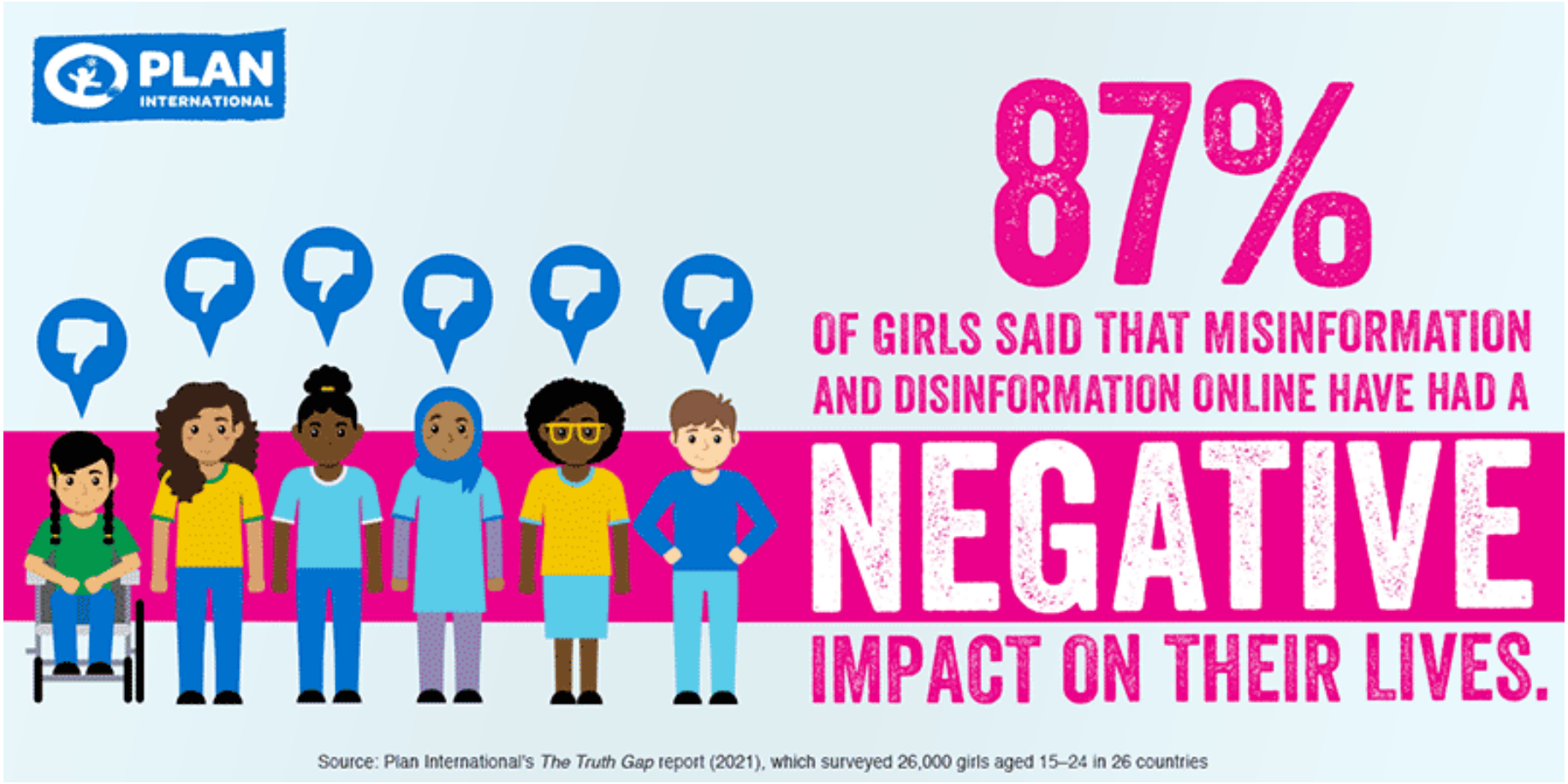
MERCY CORPS

What does TFGBV look like in real life?

TFGBV can be perpetrated using new technologies, or by using old technologies in new ways. Violence against women evolves constantly, and we must remain vigilant. There are many forms of TFGBV, including:

- ✓ Online gender and sexual harassment;
- ✓ Cyberstalking;
- ✓ Image-based abuse, including non-consensual sharing of intimate images, deep fakes or sending unsolicited images of genitals to another person;
- ✓ Technology-facilitated sexual abuse, such as sextortion (blackmail by threatening to publish sexual information, photos or videos), online grooming for sexual assault, etc.;
- ✓ Doxing (publishing private personal information);
- ✓ Hacking;
- ✓ Impersonation;
- ✓ Searching for targets and using technology to locate survivors in order to perpetrate violence;
- ✓ Hate speech;
- ✓ Defamation;
- ✓ Limiting or controlling survivors' use of technology.

MERCY CORPS


PLAN INTERNATIONAL
87%
OF GIRLS SAID THAT MISINFORMATION AND DISINFORMATION ONLINE HAVE HAD A
NEGATIVE
IMPACT ON THEIR LIVES.
Source: Plan International's *The Truth Gap* report (2021), which surveyed 26,000 girls aged 15–24 in 26 countries

MERCY CORPS

What are the impacts of TFGBV?

Digital life is real life.

TFGBV is often perceived as less severe or less harmful than offline forms of violence, but research shows it has serious consequences on the health, lives and futures of women and girls. TFGBV also often leads to offline violence, posing a very dangerous threat to women and girls' safety and physical integrity.

MERCY CORPS

What are the impacts of TFGBV?

The impacts of TFGBV on mental health are severe:

- ❑ Stress;
- ❑ anxiety;
- ❑ Depression;
- ❑ post-traumatic stress disorder;
- ❑ suicidal ideation;

Suicide attempts have been reported by survivors!!!

What are the impacts of TFGBV?

In addition, TFGBV silences women online and reduces their participation in public and political life, in democratic processes and in leadership roles.

As a result, TFGBV reinforces patriarchal roles, norms and structures, and is a major barrier to gender equality and the achievement of the Sustainable Development Goals.

MERCY CORPS

Online Gender-Based violence vs Online Violence

Online Gender-Based violence

also referred to as technology-facilitated gender-based violence (TFGBV),6 is any form of violence that is enabled by or perpetrated by using technology or a digital interface - specifically the internet or smart devices. It can target one's gender, sex, or sexual orientation.

Online Violence

commonly referred to as cyber violence or technology-facilitated violence is the use of computer systems to cause, facilitate, or threaten violence against individuals, that results in (or is likely to result in) physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstance, characteristics or vulnerabilities. 5

MERCY CORPS

TFGBV as Cyber Violence

TFGBV – often referred to as cyber violence or online abuse – is an emerging global public health and human rights issue that affects the safety and well-being of individuals and negatively impacts communities.

TFGBV includes behaviors such as stalking, bullying, sexual harassment, defamation, hate speech, exploitation and gender trolling, which are carried out utilizing computer and mobile technology. Technology-facilitated GBV is violence that is motivated by the sexual or gender identity of the target or by underlying gender norms.

MERCY CORPS

Cyber violence against women and girls (CVAWG)

Digital platforms have often been celebrated for allowing equal opportunities for public self-expression, regardless of one's identity and status. Yet, not everyone is welcome in the cyberspace. The digital arena has become a breeding ground for a range of exclusionary and violent discourses and beliefs, expressed and disseminated in a context of anonymity and impunity.

Both women and men can be victims of cyber violence. However, evidence shows that women and girls are highly exposed to it. Not only are they more likely to be targeted by cyber violence, but they can suffer from serious consequences, resulting in physical, sexual, psychological, or economic harm and suffering.

Cyber violence against women and girls (CVAWG) is often dismissed as an insignificant and virtual phenomenon. However, CVAWG does not exist in a vacuum: it is an act of gender-based violence that is perpetrated through new technologies, but is deeply rooted in the inequality between women and men that still persists in our societies.

EIGE
European Institute for Gender Equality

MERCY CORPS

How is cyber violence gendered?

CVAWG is part of the **continuum of violence against women and girls** and represents yet another form of abuse and silencing embedded within existing gendered power structures. The violent acts taking place through technology are an integral part of the same violence that women and girls experience in the physical world, for reasons related to their gender[4].

Also, there are many forms of cyber violence that target women and girls almost exclusively. These include forms of non-consensual intimate image abuse, like **cyber flashing** and **sextortion** as well as **virtual rape.**

An EIGE study on Gender Equality and Digitalisation in the European Union highlighted the new gendered challenges of digitalisation, including women being potential targets of CVAWG from a very young age6. Often resulting in an abandonment of digital spaces, CVAWG has a devastating impact on women's confidence when it comes to technology, further contributing to worsening gender equality issues like **STEM/ICT gender segregation** and **gender pay gap**.

MERCY CORPS

Cyber violence against women and girls

Cyber violence against women and girls includes a range of different forms of violence perpetrated by ICT (Information Communication Technologies) means on the grounds of gender or a combination of gender and other factors (e.g. race, age, disability, sexuality, profession, or personal beliefs).

All acts of CVAWG can:

- start **online** and continue **offline** such as in the workplace, at school or at home;
- start **offline** and continue **online** across different platforms such as social media, emails or instant messaging apps;
- be perpetrated by a person or group of people who are anonymous and/or unknown to the victim;
- be perpetrated by a person or group of people who are **known** to the victim such as an (ex) intimate partner, a schoolmate or a co-worker.

MERCY CORPS

Cyber stalking against women and girls

Cyber stalking against women and girls involves intentional repeated acts against women and/or girls because of their gender, or because of a combination of gender and other factors (e.g. race, age, disability, sexuality, profession or beliefs).

It is committed through the use of ICT means, to harass, intimidate, persecute, spy or establish unwanted communication or contact, engaging in harmful behaviours that make the victim feel threatened, distressed or unsafe in any way.

- Cyber stalking is a key tactic of coercive control used in intimate partner violence (IPV). 7 in 10 women who have experienced cyber stalking have also experienced at least one form of physical and/or sexual violence from an intimate partner[10].
- Several studies highlight the links between stalking and cyber stalking[11]: a UK study found that over half (54 %) of cyber stalking cases involved a first encounter in the physical world[12]. Also, obtaining personal information through cyber stalking can lead to further violent actions both online and offline[13].
- The negative impact of cyber stalking on the victims' well-being appears similar to that of stalking[14]. Cyber stalking victims report increased suicidal ideation, fear, anger, depression, and post-traumatic stress disorder symptomology[15].

MERCY CORPS

Cyber harassment against women and girls

Cyber harassment against women and girls involves one or more acts against victims because of their gender, or because of a combination of gender and other factors (e.g. race, age, disability, profession, personal beliefs or sexual orientation).

It is committed through the use of ICT means to harass, impose or intercept communication, with the purpose or effect of creating an intimidating, hostile, degrading, humiliating or offensive environment for the victim.

- According to a 2019 FRA survey, 13 % of women across the EU, the UK and North Macedonia had experienced cyber harassment during the previous 5 years. Victims are more commonly younger respondents (20 % of young women aged 18 to 29), members of the LGBTIQ+ community and people with disabilities[16].
- Cyber harassment tends to reflect a broader pattern of victimization on the offline-online continuum of violence. 77 % of women who have experienced cyber harassment have also experienced at least one form of sexual and/or physical violence perpetrated by an intimate partner[17].
- 41 % of responding women who experienced cyber harassment felt that their physical safety was threatened. One in two women have experienced reduced self-esteem or loss of self-confidence, stress, anxiety, or panic attacks because of cyber harassment[18].

MERCY CORPS

Cyber bullying against girls

Cyber bullying against girls means any form of pressure, aggression, harassment, blackmail, insult, denigration, defamation, identity theft or illicit acquisition, treatment or dissemination of personal data, carried out repeatedly by ICT means on the grounds of gender or a combination of gender and other factors (e.g. race, disability or sexual orientation), whose purpose is to isolate, attack or mock a minor or group of minors.

- There is a strong connection between cyber bullying and bullying: most students who are victims of cyber bullying have been bullied in school first, and a large percentage of victims of bullying have been bullied both online and offline, often by the same perpetrator(s)[19].
- Across the OECD countries with available data, about 12 % of girls aged 15 report having been cyber bullied, compared with 8 % of boys[20]. The Cyberbullying Research Center found that adolescent girls are more likely than boys (50.9% vs. 37.8%) to have experienced cyber bullying in their lifetimes[21].
- Certain minority groups are more exposed to cyber bullying, such as LGBTIQ+ individuals and students with special needs[22]. Also, there are clear links between cyber bullying and mental health problems[23].

MERCY CORPS

Online gender-based hate speech

Online gender-based hate speech is defined as content posted and shared through ICT means that:
a)is hateful towards women and/or girls because of their gender, or because of a combination of gender and other factors (e.g. race, age, disability, sexuality, ethnicity, nationality, religion or profession); and/or
b)spreads, incites, promotes or justifies hatred based on gender, or because of a combination of gender and other factors (e.g. race, age, disability, sexuality, ethnicity, nationality, religion or profession).
It can also involve posting and sharing, through ICT means, violent content that consists of portraying women and girls as sexual objects or targets of violence.
This content can be sent privately or publicly and is often targeted at women in public-facing roles.

- Victims may decide to post less often, tone down their language to mitigate provocation or even deactivate their accounts. According to Amnesty International, this self-censorship has a 'silencing effect' and results in women and girls not openly participating to debates and meaningful exchanges online[24].
- As victims are often prominent female figures like politicians, journalists or sportswomen, online gender-based hate speech directly impacts on the presence and activities of potential role models for girls who may want to pursue careers in traditionally male-dominated industries.
- ICT means can contribute to make online forms of gender-based hate speech more harmful, because it is significantly more difficult to permanently remove abusive or triggering content from the Internet, which often results in re-victimisation[25].

MERCY CORPS

Non-consensual intimate image abuse

Non-consensual intimate image (NCII) abuse against women and girls involves the distribution through ICT means or the threat of distribution through ICT means of intimate, private and/or manipulated images/videos of a woman or girl without the consent of the subject.

Images/videos can be obtained non-consensually, manipulated non-consensually, or obtained consensually but distributed non-consensually. Common motivations include sexualizing the victim, inflicting harm on the victim, or negatively affecting the life of the victim.

- The spread of such images can destroy victims' educational and employment opportunities as well as their intimate relationships. Victims are often threatened with sexual assault, stalked, harassed, fired from jobs, and forced to change schools. Some have committed suicide[26].
- NCII abuse is closely linked to intimate partner violence (IPV). The perpetrator can be an ex-partner who aims to publicly shame and humiliate the victim, often in retaliation for ending the relationship. For this reason, media-generated terms like *non-consensual pornography* or *revenge porn* are often used. However, these terms are legally incorrect and create false impressions around the circumstances of the offense.
- Technological advances are enabling more and more realistic manipulation of images. This can be done using software such as Photoshop or AI tools to create synthetic media like deepfakes[27].

MERCY CORPS

OGBV causes real harm!

OGBV has grave consequences, not only for women and girls, but it affects society as a whole. An analysis of documented cases in the Philippines showed that survivors of OGBV experienced emotional harm (83 per cent), sexual assault (63 per cent) and physical harm (45 per cent).

In Pakistan, online harassment has resulted in femicide, suicide, physical violence, emotional distress, women losing their jobs and silencing themselves in online spaces.[3]

OGBV is deeply rooted in discriminatory social norms, gender inequality and often connected to offline violence. It is actively a barrier against women's and girls' freedom of speech and their involvement in the public agenda.

MERCY CORPS

OGBV is a barrier against girls' and women's freedom of expression and their involvement in education, the labour force and political and public discussion. It undeniably widens existing gender inequalities that work against peaceful, prosperous and sustainable societies.

MERCY CORPS

Online Safety is not a dream!

TFGBV or OGBV is as preventable as any other form of GBV. Research shows that tailored prevention efforts aimed at all levels, including governments, the private sector, tech companies, communities, and individuals; along with adequate response services to survivors can lead the way to ending OGBV.

Involving more girls and women in STEM (Science, Technology, Mathematics, Engineering) fields; supporting women-led tech companies, and mainstreaming gender in our current tech ecosystem including AI (Artificial Intelligence), would further help to deconstruct gender-blind and gender-biased tech ecosystems, and ultimately help to build a gender-transformative ecosystem.

MERCY CORPS

How to Reduce Technology-Facilitated Gender-Based Violence

TFGBV is not only online but is also facilitated through the use of digital products and devices. The rising use of and demand for interconnected devices or Internet of Things (IOT) devices offers benefits that greatly improve quality of life and increase efficiency of certain tasks.

However, there is little concerted decision-making and policymaking to address the amount of personal data collected and stored by these devices and how these devices and the data they generate may be coopted for malicious purposes.

Smart chips are becoming common: smart TVs, wearables, voice assistants, computerized personal assistants, and even ordinary household devices like washing machines, toasters and refrigerators can now be connected to the internet. The setup and installation of these gadgets often require more than necessary personal data from users. IOT devices might c ollect and retain mass amounts of data and metadata on women and girls and share with a variety of parties, who may be able to extract data on where these women and girls are, what they are doing or saying, and perhaps even capture imagery and videos of them.

MERCY CORPS

Recommendations:

- Strengthen systems to support data security, including confidential information collected and managed by State actors and data collected through location-based applications and platforms.

- International agreements and a common right-based legislative framework to address cross-border TFGBV.

- Reduce privacy risks to women and girls by disconnecting the data subject from the data collected. Methods such as differential privacy, synthetic data or homomorphic encryption, could aid as part of a solution to ensure data collected cannot be traced back to the particular user.

MERCY CORPS

Recommendations: Safety by Design: Ensuring survivor-centered product financing, ideation, development and Deployment

The Global Digital Compact should work with Government and private technology companies to ensure solutions, products and platforms are designed with gender equity in mind, including design pedagogies that center (1) the voices of those who are directly impacted by design process outcomes, (2) the impact on communities over designer intentions and (3) everyday people as experts on end user experiences who collaborate with designers and developers.24 This mandates the participation of women and marginalized populations in the financing/funding of tech development and includes ideation, conceptualization, development, testing and scaling of products that have accessible safety features and complaint mechanisms in their solutions and platforms. Governments and businesses must ensure women's active role in internal staffing across roles and levels of responsibility and in decision-making processes.

MERCY CORPS

Recommendations: Privacy by Default and Design: Ensuring robust data privacy and security to proactively mitigate use of data for TF GBV

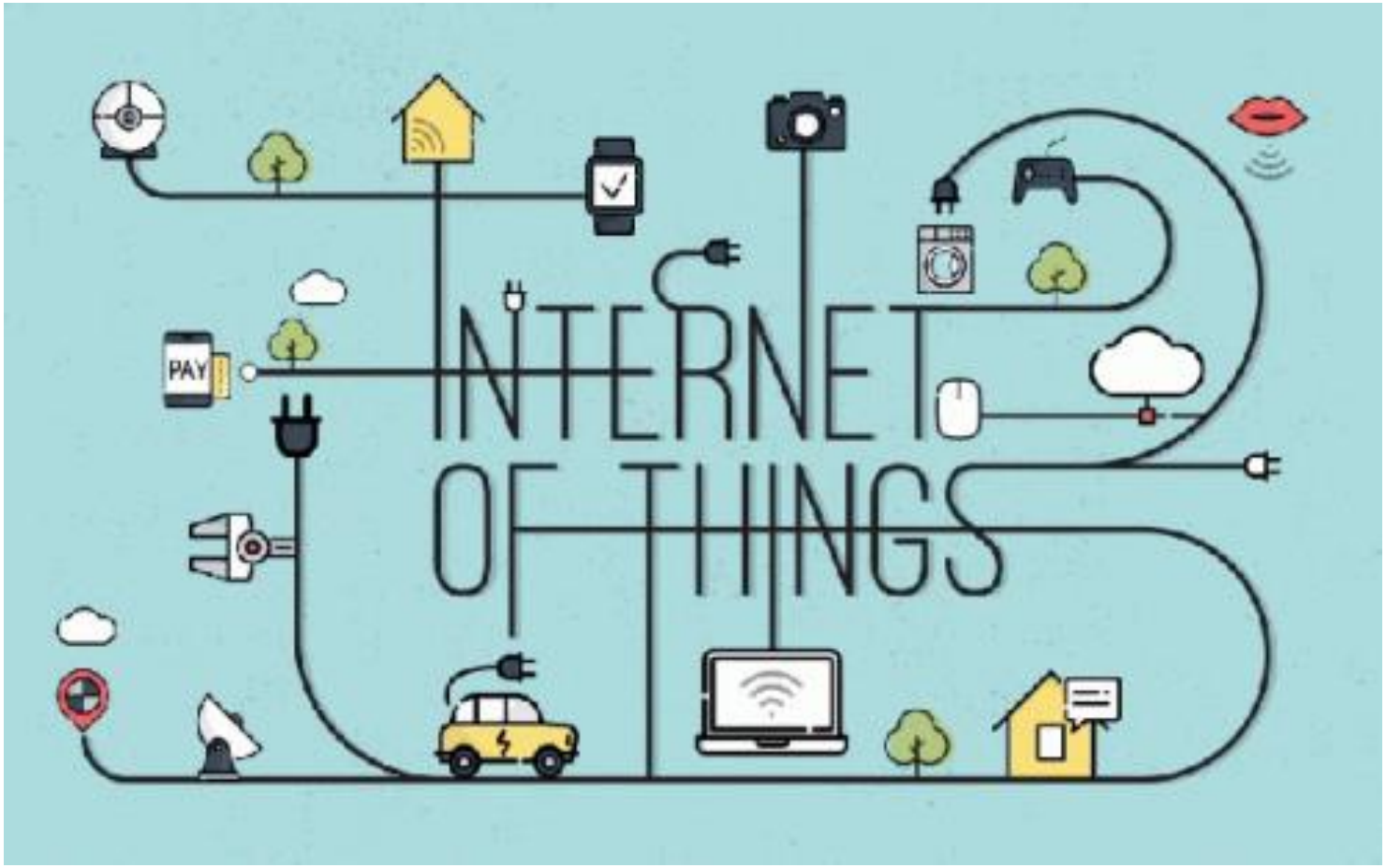
The Global Digital Compact should work with Governments and business and technology to advance, regulate, and standardize data collection practices, privacy, and security.

Data collected and stored can be weaponised to commit and amplify TF GBV including intimate partner violence, cyberstalking, sharing of intimate images without consent, doxxing and impersonation. While data is highly valuable and essential to the business model of companies, collection of personal data should be only for certain cases when consent has been provided and there is a primary functional user driven reason.

The economic value of data incentivises technology companies to collect data, often unknown or poorly understood by end users, resulting in a loss of data privacy, data security, and a sense of control over how one's information is being used by others.

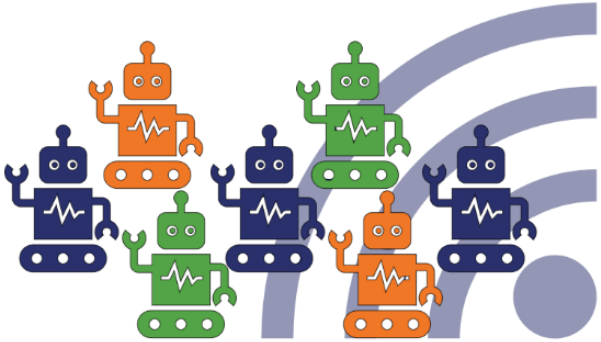
MERCY CORPS

IoT (Internet of Things) used by TFGBV



MERCY CORPS

Bad Bots



What are Bad Bots?

Malicious (bad) bots are software applications designed to execute automated tasks with harmful intentions, including criminal activities such as fraud and theft. These bots are often used by fraudsters, attackers, unethical competitors, and other bad actors with various motives to conduct a range of malicious activities and attacks on websites, mobile apps, and APIs.

MERCY CORPS

Types of Bad Bots …

- **Web Scrapers** - the process of extracting data from websites using automated software or bots. **For example**, web scraping can be used to copy content, create fake -commerce sites, deliver malware, or perform ad fraud.

- **Credential Stuffing Bots** - is a cyberattack where hackers exploit stolen usernames and passwords from one site to gain access to user accounts on other sites. It can have a negative impact on businesses, as it can lead to:

Fraud:
Hackers can use compromised accounts to order expensive products or services for personal use or resale, leading to chargebacks, fines, and revenue loss for businesses.

Account takeover:
Hackers can access user accounts and personal data such as credit card numbers, addresses, loyalty points, and gift cards for fraudulent purchases, sell access to other hackers, or impersonate users for phishing and identity theft.

Espionage and theft:
Hackers can use credential stuffing to access employee or administrator accounts, obtaining sensitive business information, customer data, and financial records.

Reputational damage:
Credential stuffing attacks can damage customer trust and loyalty, harm brand reputation, and lead to customer loss, lawsuits, and regulatory penalties for businesses.

MERCY CORPS

Types of Bad Bots …

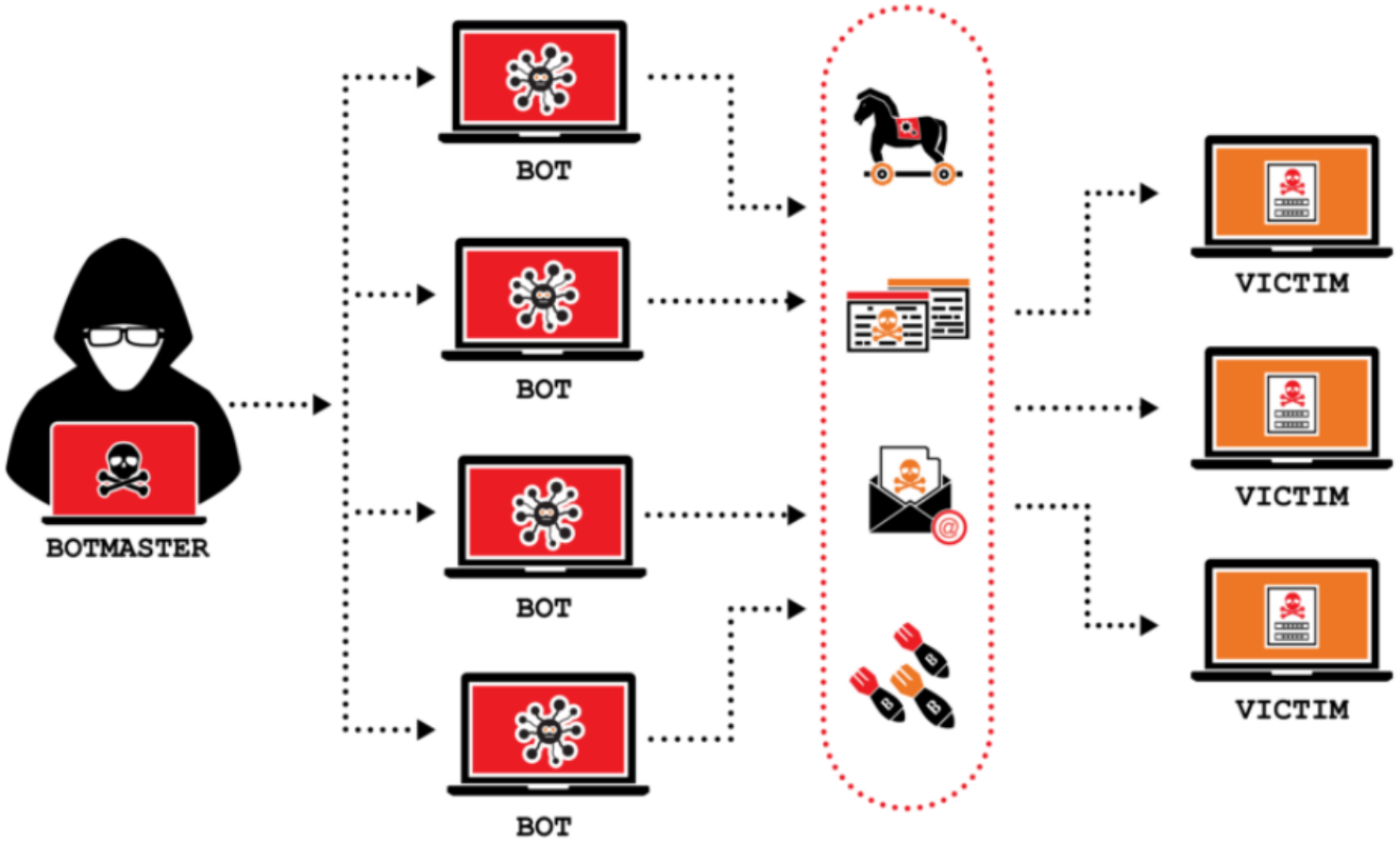
- **DDoS Bots -** DDoS bots execute Distributed Denial of Service (DDoS) attacks, which disrupt the normal traffic of targeted servers, services, or networks by overwhelming them with internet traffic. These attacks can cause significant business impacts, such as financial losses from offline websites or online shops, and reputational damage. Hackers may also combine DDoS attacks with other cyberattacks, leading to data loss.

DDoS attacks are increasing in size and complexity. Gcore reports that in 2022, the number and volume of DDoS attacks doubled compared to 2021, with average attack power rising from 150–300 Gbps to 500–700 Gbps. Both ordinary users and businesses across various industries, including fintech, gaming, and e-commerce, are being targeted.

- **Spam Bots** - Spam bots are automated programs that mimic real user behavior to spread content. While some are beneficial, many are malicious, spreading harmful or false information. These bots can damage a company's reputation by impersonating it or its employees, lead to financial loss and data breaches, and incur significant costs in time, effort, and money to combat.

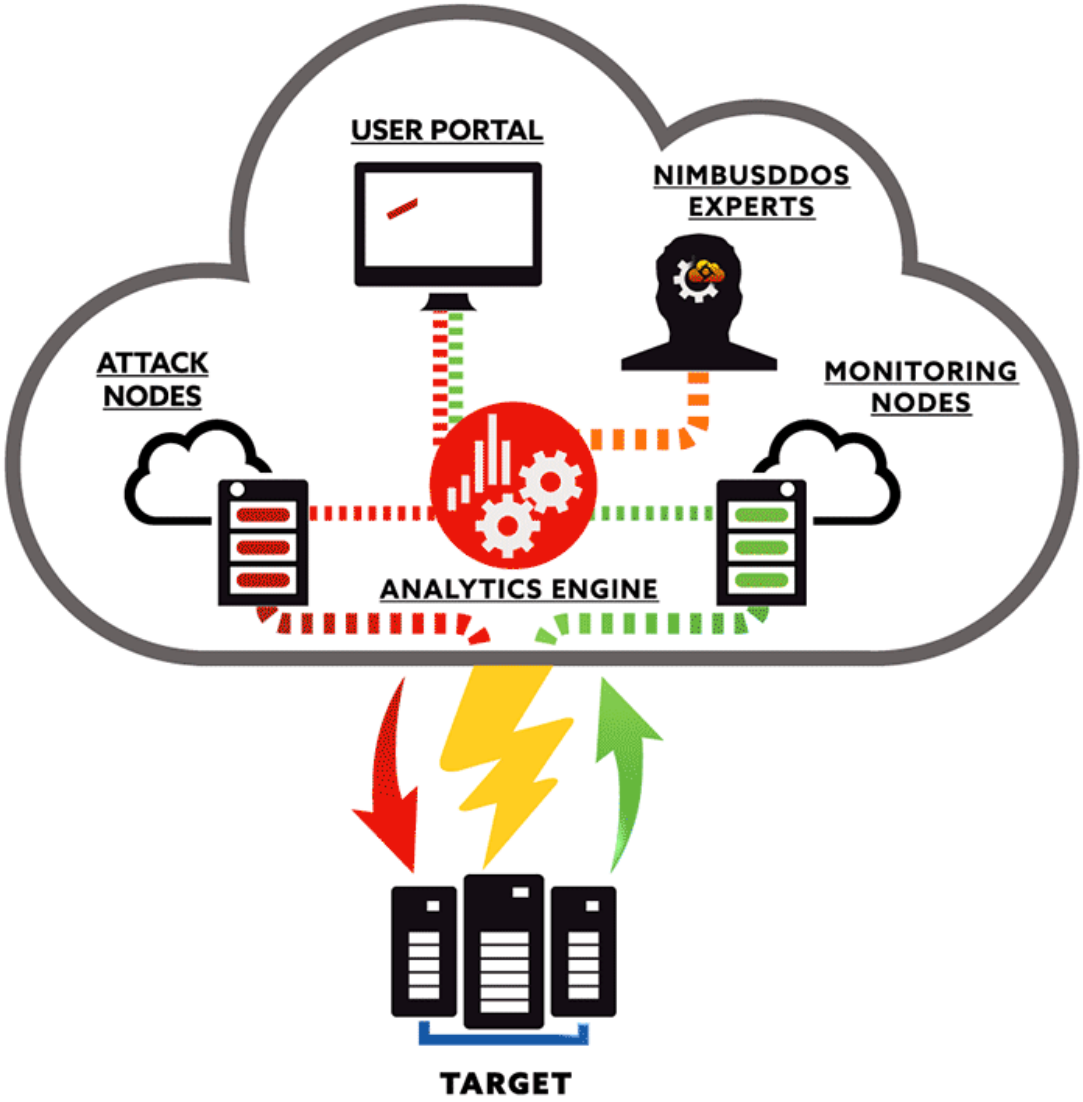
MERCY CORPS

Cyber Attacks



MERCY CORPS

DDOS Attacks



MERCY CORPS

How to Spot Malicious Bots?

Signs of malicious bot activity include:

1. Abnormally high pageviews: Bots may attempt to overwhelm servers.
2. Unusually high bounce rates: Bots often have specific goals.
3. Fake or junk conversions

MERCY CORPS

Here are some methods and tools for identifying malicious bots:

1. Differentiating bots from human users based on communication frequency:

Bots often maintain continuous communication with their targets.

2. Identifying browser-based bots separately.

3.Analyzing the payload of incoming requests.

4. Differentiating between browsers and other types of clients.

5. Analyzing the targets of bot attacks, such as specific URLs and endpoints.

MERCY CORPS

References

1. UNFPA, 2021 “Technology-facilitated Gender-based Violence: Making All Spaces Safe”
2. https://www.ictworks.org/technology-facilitated-gender-based-violence/
3. https://digitalrightsfoundation.pk/wp-content/uploads/2020/06/Covid-19.pdf
4. GREVIO (Council of Europe Group of Experts on Action against Violence against Women and Domestic Violence) (2021), *General Recommendation No1 on the digital dimension of violence against women*, Council of Europe, Strasbourg, 20 October 2021 (https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147).
5. Van der Wilk, A. (2018), Cyber Violence and Hate Speech Online against Women, European Parliament, Policy Department for Citizens’ Rights and Constitutional Affairs, Brussels (https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf).
6. 3 Lomba, N., Navarra, C., and Fernandes, M. (2021), Combating Gender-based Violence: Cyber violence – European added value assessment, European Parliamentary Research Service, Brussels (https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf).
7. https://www.radware.com/cyberpedia/bot-management/bad-bots/

MERCY CORPS

References

7. 4 EIGE (European Institute for Gender Equality) (2020), Gender Equality Index Report, Vilnius https://eige.europa.eu/publications/gender-equality-index-2020-report).
8. 5 GREVIO (Council of Europe Group of Experts on Action against Violence against Women and Domestic Violence) (2021), General Recommendation No1 on the digital dimension of violence against women, Council of Europe, Strasbourg, 20 October 2021 (https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147).
9. 6 EIGE (2018), Gender equality and digitalization in the European Union, Vilnius (https://eige.europa.eu/publications/gender-equality-and-digitalisation-european-union).

MERCY CORPS

MERCY CORPS