DHSI
DIGITAL HUMANITIES SUMMER INSTITUTE

Research Security Practices and Policies

Aaron Mauro

ETCL
ELECTRONIC TEXTUAL CULTURES LAB

Social Sciences and Humanities Research Council of Canada
Conseil de recherches en sciences humaines du Canada

Welcome to DHSI 2023!

Thank you for joining the DHSI community!

In this coursepack, you will find essential workshop materials prefaced by some useful general information about DHSI 2023.

Given our community's focus on things computational, it will be a surprise to no one that we might expect additional information and materials online for some of the workshops—which will be made available to you where applicable—or that the most current version of all DHSI-related information may be found on our website at dhsi.org. Do check in there first if you need any information that's not in this coursepack.

Please also note that materials in DHSI's online workshop folders could be updated at any point. We recommend checking back on any DHSI online workshop folder(s) that have been shared with you in case additional materials are added as DHSI approaches and takes place.

And please don't hesitate to be in touch with us at institut@uvic.ca or via Twitter at @AlyssaA_DHSI or @DHInstitute if we can be of any help.

We hope you enjoy your time with us!

DHSI
DIGITAL HUMANITIES SUMMER INSTITUTE

ETCL
ELECTRONIC TEXTUAL CULTURES LAB

Statement of Ethics & Inclusion

Please review the DHSI Statement of Ethics & Inclusion available here: https://dhsi.org/statement-of-ethics-inclusion/

DHSI is dedicated to offering a safe, respectful, friendly, and collegial environment for the benefit of everyone who attends and for the advancement of the interests that bring us together. There is no place at DHSI for harassment or intimidation of any kind.

By registering for DHSI, you have agreed to comply with these commitments.

Virtual Sessions

Your registration in DHSI 2023 also includes access to the virtual **institute lecture** sessions. Access details for these talks will be shared as DHSI approaches.

Due to the high volume of attendees, please ensure your DHSI registration name or DHSI preferred name and your Zoom name match so that we know to let you into the virtual sessions.

DHSI Materials

DHSI materials (ex. videos, documents, etc.) are intended for registrant use only. By registering, you have agreed that you will not circulate any DHSI content. If someone asks you for the materials, please invite them to complete the registration form to request access or contact us at institut@uvic.ca.

Auditor and participant registration

If you registered to **audit** any workshops, note that auditor involvement is intended to be fully self-directed without active participation in the workshop. The auditor option offers more flexibility regarding pace and time with the workshop content. Your registration as an auditor will include access to some asynchronous workshop materials only and does not include access to live workshop sessions and/or individual/group instruction or consultation. Please direct any questions about DHSI workshop auditing to **institut@uvic.ca**.

If you registered as a **participant** in any workshops, your registration includes access to asynchronous content + active participation in live workshop session(s). The workshop instructor(s) will contact you about the date(s), time(s), and platform(s) of the live workshop session(s).

If you are unsure whether you registered as an auditor or participant, please check your registration confirmation email. Further questions can be directed to **institut@uvic.ca**.

Schedule

The at-a-glance schedule of DHSI 2023 courses, workshops, institute lectures and aligned conferences & events can be found here: **https://dhsi.org/timetable/**

All times are listed in North American **Pacific Time Zone**.

For those who registered as participants in any workshops, live sessions for online workshops are not currently listed on the above-referenced schedule. **Instructors will be in touch with registered participants directly about the exact date(s) and time(s) of their live workshop session(s).**

Acknowledgements

We would like to thank our partners and sponsors (including the Social Sciences and Humanities Research Council), workshop instructors, aligned conference & event organizers, institute lecturers, local facilitators, and beyond for making this possible.

Further information

General DHSI 2023 information: **https://dhsi.org/program/**

Full course listings (in-person): **https://dhsi.org/on-campus-courses/**

Full workshop listings (online): **https://dhsi.org/online-workshops/**

Aligned conferences & events (in-person): **https://dhsi.org/on-campus-aligned-conferences-events/**

Aligned conferences & events (online): **https://dhsi.org/online-aligned-conferences-events/**

Institute lectures: **https://dhsi.org/institute-lectures/**

Frequently asked questions: **https://dhsi.org/faq/**

Any questions not addressed in the above pages? Please email us at **institut@uvic.ca**!

De–identification Guidelines for Structured Data

June 2016

Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Acknowledgments

We would like to thank Dr. Khaled El Emam for reviewing an earlier version of these guidelines and providing helpful comments.

CONTENTS

INTRODUCTION

As the demand for government-held data increases, institutions require effective processes and techniques for removing personal information. An important tool in this regard is de-identification.

“De-identification” is the general term for the process of removing personal information from a record or data set. De-identification protects the privacy of individuals because once de-identified, a data set is considered to no longer contain personal information. If a data set does not contain personal information, its use or disclosure cannot violate the privacy of individuals.[1] Accordingly, the privacy protection provisions of the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) would not apply to de-identified information.

It is important to note that de-identification does not reduce the risk of re-identification of a data set to zero. Rather, the process produces data sets for which the risk of re-identification is very small.

These guidelines will introduce institutions to the basic concepts and techniques of de-identification. They outline the key issues to consider when de-identifying personal information in the form of structured data and they provide a step-by-step process that institutions can follow when removing personal information from data sets.

De-identification can be a complex and technically challenging process. These guidelines take a conservative approach to risk in order to simplify the calculations involved in measuring it. However, some degree of complexity in the process is unavoidable.

When dealing with issues that may arise in de-identification, it is important that you seek advice from technical staff, or other experts in the field (such as your freedom of information and privacy coordinator, or legal counsel). The information contained in these guidelines can serve as a starting point for discussions with those individuals.

Some of the complexity and challenges of de-identification can be addressed through the use of automated tools. While it is possible (and may be appropriate in certain circumstances) to de-identify data sets manually, there are many software tools available that can automate some aspects of the process. When seeking to de-identify a data set, you may wish to consider using de-identification software.

[1] Note, however, that the same cannot be said with respect to the rights of groups of individuals. For a discussion of how to protect against harms relating to groups of individuals when de-identifying data sets, see the section on “De-identification Governance” below.

TERMINOLOGY

Some of the technical terms used in these guidelines are defined below.

adversary: individual or entity attempting to re-identify one or more individuals in the data set

brute force attack: trial-and-error attack that involves attempting all possible combinations to decode an encrypted value

masking: the process of removing a variable or replacing it with pseudonymous or encrypted information

one-way hash function: cryptographic mapping function that is practically impossible to reverse, that is, to recreate the input data from its encrypted value

re-identification: any process that re-establishes the link between identifiable information and an individual

release model: manner in which recipients of a data set are provided access to it

structured data (data set): collection of data in tabular form where every column represents a variable and every row represents a member or individual

target individual: individual targeted by an adversary for re-identification

variable: column of values in a data set representing a set of attributes

SCOPE OF GUIDELINES

Approaches to de-identification range from simple "cookie cutter" lists of variables to be removed or modified, to general loosely defined techniques such as the "cell size of five" rule,[2] to systematic risk-based methodologies. While it may be possible to de-identify data sets in different ways, these guidelines offer direction on taking a *risk-based approach* to de-identification.[3]

Risk-based de-identification involves calculating an acceptable level of re-identification risk for a given data release. The calculation requires the consideration of a number of factors, including whether an adversary can know if a target individual is in the data set. If an adversary knows that a target individual is in the data set, this is called "prosecutor risk." For example, if a teenager's parents know that their child has participated in a survey and the results are to be released in de-identified form, the risk of the parents attempting to re-identify their child's responses would qualify as prosecutor risk. If an adversary does not, or cannot, know if a target

[2] The cell size of five rule is the practice of releasing aggregate data about individuals only if the number of individuals counted for each cell of the table is greater than or equal to five.

[3] The approach to de-identification presented in these guidelines is based largely on the risk-based de-identification methodology developed by Dr. Khaled El Emam. For a select list of books and articles written and co-authored by Dr. El Emam on the topic of de-identification, see Appendix A: Resources.

individual is in the data set, this is called "journalist risk."[4] For example, if only a sample of de-identified rows from an original data set is released, this would qualify as journalist risk.

While some de-identification methodologies support both of the above types of risk—that is, prosecutor and journalist risk—these guidelines support prosecutor risk only—that is, they assume an adversary knows or can know whether a target individual is in the data set. Because prosecutor risk is always equal to or greater than journalist risk,[5] a consequence of this approach is that these guidelines err on the conservative side when it comes to calculating levels of re-identification risk.[6]

De-identification also involves a range of techniques, such as sub-sampling, randomization or swapping. While a number of techniques may be used to remove personal information from data sets, for simplicity these guidelines only discuss the application of the most commonly used techniques, namely *masking, generalization* and *suppression.* Therefore, when using these guidelines to de-identify data sets with a large number of variables, or "high-dimensional" data, the utility of the data sets may be lower than if other techniques were used.

OVERVIEW OF DE-IDENTIFICATION

As noted above, de-identification is the process of removing personal information from a record or data set. "Personal information" is defined in *FIPPA* and *MFIPPA* as "recorded information about an identifiable individual." The Office of the Information and Privacy Commissioner of Ontario (IPC) and the courts have elaborated on this definition, specifically on the meaning of "identifiable," in various orders and reviews.[7] Based on these, de-identification may be defined more precisely as the process of removing any information that (i) identifies an individual, or (ii) for which there is a reasonable expectation that the information could be used, either alone or with other information, to identify an individual.

Throughout these guidelines, the term "de-identification" will be used to convey different aspects of this definition. The term may be used when referring to the *process* of de-identification, which involves a series of steps, considerations and possible outcomes. The term may also be used when referring to the *removal* of identifiable information. From the context, it should be clear in which sense the term is being used.

Applying a "reasonableness standard" to the definition of personal information means that you must examine the context to de-identify information. When de-identifying a data set, you must navigate and consider a number of issues, including:

- *Different release models.* In de-identification, a data set may be released publicly, semi-publicly (also called "quasi-public") or non-publicly. In a public data release, the

[4] See Khaled El Emam, *Guide to the De-identification of Personal Health Information* (Boca Raton, FL: CRC Press, 2013), 182.

[5] See ibid., 195.

[6] Additional guidance on how to de-identify data sets under journalist risk may be found in El Emam, *Guide to the De-identification of Personal Health Information*.

[7] See the test for whether a record can reveal personal information in the judicial review of Order P-1880 at *Ontario (Attorney General) v. Pascoe,* 2002 CanLII 30891 (ON CA), para. 14–15.

data set is available to anyone for download or use without any conditions. This kind of release provides the greatest availability, but the least amount of protection.

In contrast, a non-public data release limits the availability of the data set to a select number of identified recipients. As a condition of receiving the data, recipients must agree to terms and conditions regarding the privacy and security of the data (typically set out in a data sharing agreement). This kind of release provides the least availability but can provide a higher amount of protection.

A data set may also be released semi-publicly, which involves elements of both the public and non-public options. In a semi-public data release, the data set is available to anyone for download; however, as a condition of receiving the data, the recipient must register with the organization releasing the data set and agree to restrictions regarding the processing and sharing of the data (typically in the form of a terms-of-use agreement).

While additional privacy and security measures may be included in terms-of-use agreements for semi-public data releases, these are difficult to enforce due to the open nature of the release. Accordingly, data sets released in this way are limited in terms of the amount of protection they can provide. Depending on the release model used, the required amount of de-identification may vary.

- *Different types of identifiers.* In de-identification, you need to remove information that directly identifies an individual and information for which there is a "reasonable expectation" that the information could be used, either alone or with other information, to identify the individual. The first type of identifier is known as a "direct identifier," and the second type is called an "indirect-" or "quasi-identifier."
- *Different re-identification attacks.* The amount of de-identification that needs to be applied to a data set is determined by how likely it is that an adversary will attempt to re-identify one or more individuals in the data set. Different types of adversaries need to be considered and different types of re-identification attacks need to be analyzed, depending on the release model used. For example, for public data releases, you should assume that someone will attempt a demonstration attack on the data set. For non-public data releases, you should evaluate the threat posed by insiders and data breaches.
- *Different de-identification techniques.* Once you know the level of re-identification risk and have calculated the required amount of de-identification, a corresponding amount of information must be removed from the data set. This can be done in various ways—through techniques such as masking, generalization and suppression.

- *Different types of disclosures.* De-identification techniques protect against the disclosure of individuals' identities and linking information to them. They do not, however, protect against the disclosure of attributes relating to groups of individuals that may be stigmatizing. While you must protect against the disclosure of individuals' identities when releasing de-identified data sets, as a best practice, you should also consider protecting against attribute disclosures. To do this, you may be required to develop a governance model that includes an ethics review of data sets.

USES OF DE-IDENTIFICATION

The primary objective of de-identification is protecting the privacy of individuals. If a data set contains any amount or kind of personal information, it cannot be considered de-identified.

At the same time, one of the main reasons for releasing de-identified data sets is to provide others with an opportunity to study the values and properties of the raw data for research purposes. De-identification, therefore, should also seek to preserve as much utility in the information as possible, while protecting the privacy of individuals.

This dual purpose of de-identification makes it an important tool to consider for use in a number of contexts, including open data, access to information requests and data sharing within and among institutions.

OPEN DATA

De-identification may be used to enable data sharing in situations where an institution does not have the authority to disclose personal information. An example of such a situation is the growing number of "open data" initiatives in Ontario. Open data initiatives seek to increase government transparency and accountability by proactively releasing data sets and making them freely available to anyone for use and republishing. Given the increased amount and availability of information these initiatives provide, it is important that institutions release their data sets in a way that protects the privacy of individuals.

Open data initiatives also seek to promote research, innovation and the development of new applications and services. The greater the utility of open data sets, the better the chances of success for researchers, start-up companies and entrepreneurs seeking to use public data.

ACCESS TO INFORMATION REQUESTS

De-identification may also be useful in responding to access to information requests for structured data or data sets. Under sections 10(2) of *FIPPA* and 4(2) of *MFIPPA*, institutions are required to "disclose as much of the record as can reasonably be severed" without disclosing any exempt information. By using de-identification, institutions can respond to requests in a privacy-protective manner while preserving the utility of the information. De-identification is an innovative tool that may present institutions with an opportunity to further the transparency purposes of *FIPPA* and *MFIPPA* in ways that were not possible before.

DATA SHARING WITHIN AND AMONG INSTITUTIONS

While access to information requests and open data initiatives provide information to the public, there is also a growing desire in government services for institutions to break down their "silos" and share more information within—and among—themselves. This may happen for a number of reasons. For example:

- information from one institution or program area may be relevant to the planning of a program or service in another institution or area
- one institution may have expertise in data processing or software development that another institution requires, but does not have
- an institution that funded a program or service that was delivered by another institution may want to evaluate the effectiveness of the program or service

Data sets that contain personal information may be shared within and among institutions only if the disclosure is permitted under section 42(1) of *FIPPA* or section 32 of *MFIPPA*. If the disclosure is not permitted and the institutions still wish to share data sets, then (similar to an access to information request or open data release) any personal information must be removed.

However, even if disclosure is permitted under *FIPPA* or *MFIPPA*, there may still be important privacy issues to consider. While information sharing among institutions can play an important role in providing better, more efficient services, the practice may also have the unintended consequence of undermining the privacy of individuals by diminishing the amount of control individuals have over their personal information. Therefore, as a best practice, institutions should always consider de-identifying data sets before sharing them.

PROCESS FOR DE-IDENTIFYING STRUCTURED DATA

To protect the privacy of individuals while preserving as much utility in the information as possible, the amount and types of de-identification need to be determined through a systematic analysis of the level and kinds of re-identification risk involved in the release of a data set. When attempting to de-identify a data set, you should consider the following process:

1. determine the release model
2. classify variables
3. determine an acceptable re-identification risk threshold

4. measure the data risk
5. measure the context risk
6. calculate the overall risk
7. de-identify the data
8. assess data utility
9. document the process

STEP 1: DETERMINE THE RELEASE MODEL

As noted above, a de-identified data set may be released publicly, semi-publicly or non-publicly. Each release model allows for different levels of availability and protection of information. Depending on the purposes and/or legislative requirements of the data release, the suitability of each model may vary.

The release model plays an important role in the de-identification process because the amount of de-identification required may vary, depending on the model. For example, because public data releases provide the greatest availability, but the least amount of protection, you may require a significant amount of de-identification to protect individual privacy. Non-public data releases provide the least availability but can provide a higher amount of protection, requiring a smaller amount of de-identification.

Access requests should be handled as though they are public data releases because *FIPPA* and *MFIPPA* do not require the person requesting information to agree to terms or conditions regarding the processing, privacy or security of the information.

Similarly, when publishing open data, it is common practice to place as few restrictions as possible on the information, including who can access it and how. Requirements for individuals to register and identify themselves to the organization publishing the data are considered barriers to access, use and the ability of individuals to find the information. As such, when individuals who download the data set cannot be identified, these disclosures should be handled as public data releases.

However, there may be instances where registration of individuals and verification of their identities is required. For example, a government- or university-sponsored programming competition, or “hackathon,” may involve the release of a de-identified data set to the public or student body, but restrict participants from using the data set in certain ways (including re-identifying any individuals in it and disclosing the information to third parties, through a terms-of-use agreement). If the terms-of-use agreement does not require participants to have in place additional privacy and security measures or such measures are not enforceable, these kinds of disclosures should be handled as semi-public data releases.

Finally, when sharing information among institutions, because access to the data set is limited to the receiving program area or institution, requirements regarding the privacy and security of the information can be set and enforced through a data sharing agreement. In these cases, such disclosures may be handled as non-public data releases.

For a data release to be treated as non-public, there must be a data sharing agreement in place between the parties. The data sharing agreement is an important part of the risk mitigation strategy in these releases.

STEP 2: CLASSIFY VARIABLES

If a data set is about individuals, then each row in the file represents an individual, and each column represents a variable of information collected about the individuals. Depending on the type of information, some variables may be used to identify individuals, either directly or indirectly, while others may not. De-identification is only concerned with variables that may be used to identify individuals. As noted above, there are two kinds of such variables: direct identifiers and indirect or quasi-identifiers.

DIRECT IDENTIFIERS

Direct identifiers consist of one or more variables that can be used to identify a single individual, either by themselves or in combination with other readily available sources of information.[8] Examples include name, address, email address, telephone number, fax number, credit card number, license plate number, vehicle identification number, social insurance number, health card number, medical record number, device identifier, biometric identifiers, internet protocol (IP) address number and web universal resource locator (URL).

Typically, direct identifiers are not useful for the purposes of data analysis. For example, the email addresses of individuals will likely not be relevant to a study of work commutes. However, if the values of a direct identifier are relevant, then you should classify it as a quasi-identifier and allow the variable to be de-identified. However, if a variable is not useful for data analysis it should be classified as a direct identifier and flagged for removal or replacement with a pseudonym regardless of its characteristics (see step 7).

QUASI–IDENTIFIERS

Quasi-identifiers are variables with two important characteristics: (1) an adversary is assumed to have background knowledge of them, and (2) they can be used, either individually or in combination, to re-identify an individual in the data set.[9] A variable can be a quasi-identifier only if an adversary has background knowledge of it. A challenge with classifying quasi-identifiers

[8] Khaled El Emam and Bradley Malin, "Appendix B: Concepts and Methods for De-identifying Clinical Trial Data," *Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk* (Washington D.C.: National Academies Press, 2015), **http://www.ncbi.nlm.nih.gov/books/NBK285994/**.

[9] See ibid.

is in anticipating the possible sources of background knowledge. An adversary may obtain background knowledge about one or more individuals in the data set in different ways, including:

- information about individuals may be available in public registries (such as voter lists or court records), in the media (e.g., obituaries), from professional organizations (e.g., member lists) or employers (e.g., staff directories or biographies)
- the adversary may know one or more individuals (e.g., neighbour, co-worker or ex-spouse)
- one or more individuals may be a celebrity and there is publicly available information about them
- the adversary may have access to additional sources of information about individuals (e.g., data sets from other research projects)
- individuals may post information about themselves online (e.g., on social networking sites or personal blogs)[10]

Examples of quasi-identifiers include gender, date of birth or age, event dates (e.g., death, admission, procedure, discharge, visit), locations (e.g., postal codes, building names, regions), ethnic origin, country of birth, languages spoken, aboriginal status, visible minority status, profession, marital status, level of education, total years of schooling, criminal history, total income and religious denomination.

The value of a quasi-identifier may also be predicted from one or more variables in the data set that share a correlation with it. For example, an individual's age may be predicted from the date or year of their graduation. Because such variables may reveal the value of a quasi-identifier, you should classify them as quasi-identifiers.

STEP 3: DETERMINE AN ACCEPTABLE RE-IDENTIFICATION RISK THRESHOLD

De-identification protects the privacy of individuals by removing information that identifies an individual or for which there is a reasonable expectation that it could be used, either alone or with other information, to identify an individual. To protect personal privacy, the amount of de-identification that is required to be applied is proportional to the level of re-identification risk involved in the release of the data set. The higher the re-identification risk of a data release, the greater the amount of de-identification required.

To determine an acceptable level of re-identification risk (or threshold) for a data set, you must assess the extent to which the release of the data set would invade an individual's privacy. The result of your assessment should be a qualitative value typically in the range of "low," "medium" or "high."

[10] See "What is a quasi-identifier?" *Electronic Health Information Laboratory,* **http://www.ehealthinformation.ca/faq/quasi-identifier/.**

When assessing the level of potential privacy invasion of individuals, assume that the information in the data set is identifiable and no de-identification has taken place. Under this assumption, the level of invasion of privacy is a function of different factors, including:

- the sensitivity of the information
- the scope and/or level of detail of the information
- the number of individuals
- the potential harms or injuries to individuals in the event of a breach or inappropriate use
- whether the disclosure of the information is permitted under *FIPPA* or *MFIPPA* without the consent of the individuals
- whether the information was unsolicited or given freely by the individuals, with little or no expectation of privacy
- whether the individuals explicitly consented to their information being disclosed in de-identified form for this secondary purpose and/or were properly notified at the time of collection of this data practice[11]

The result of the invasion of privacy assessment is a qualitative value; however, the amount of de-identification that is required to be applied to a data set is quantified numerically. To bridge this divide, once you have assessed the invasion of privacy value, you must translate the result into a numerical value, representing the amount of de-identification proportionate to that level of risk. This "re-identification risk threshold" represents, in general, the minimum amount of de-identification that must be applied to a data set in order for it to be considered de-identified, that is, for it to no longer contain personal information. Accordingly, it forms the baseline against which to compare your calculations concerning de-identification going forward.

When translating between the (qualitative) invasion of privacy value and the (quantitative) re-identification risk threshold, consider a key aspect of de-identification—namely, that de-identification does not produce data sets for which there is *zero probability* of re-identification. Rather, it results in data sets for which the probability of re-identification is *very low*, given the level of re-identification risk involved in the release. The amount of de-identification proportionate to the invasion of privacy value should be equal to a very low probability of re-identification given that level of risk.

The following table may be used as a guideline in determining what may be considered a very low value for the probability of re-identification for data sets with different invasion of privacy values.[12]

[11] See El Emam, *Guide to the De-identification of Personal Health Information*, 283–290. This section of El Emam's book also contains an assessment tool that may help in determining the level of risk to individuals posed by the release of a data set.

[12] See ibid., 228.

Invasion of Privacy	Re-identification Risk Threshold	Cell Size Equivalent
Low	0.1	10
Medium	0.075	15
High	0.05	20

When combined with the calculations involved in step 5, the values listed in the table are consistent with data release precedents across Canada and the United States.[13] The table also includes the cell size equivalent for each probability of re-identification for illustrative purposes only. Cell sizes apply to aggregate count or frequency tables, not individual-level structured data. Nonetheless, the concept can be used to illustrate the general effect of de-identification on such data sets. For example, a data set with a probability of re-identification of 0.1 means that each row in the data set will in general have the same values for quasi-identifiers as nine other rows, that is, have a "cell size" of 10.

STEP 4: MEASURE THE DATA RISK

Once you have determined an acceptable re-identification risk threshold, the next step is to measure the amount of re-identification risk in the data set itself. The data risk is used to determine the level of re-identification risk involved in the release.

Measuring the amount of re-identification risk in a data set is a two-step process. You must (1) calculate the probability of re-identification of each row, and (2) apply the appropriate risk measurement method based on the release model used.

4.1 CALCULATE THE PROBABILITY OF RE-IDENTIFICATION OF EACH ROW

Each row in a data set about individuals contains information about one individual. Accordingly, each row has a probability of re-identification. For a given row, the probability of re-identification is dependent on how many other rows in the data set have the same values for variables that are quasi-identifiers.

All the rows in a data set with the same values for variables that are quasi-identifiers form an "equivalence class." For example, in a data set with variables for gender, age and highest level of education, all the rows corresponding to 35-year-old men with post-secondary degrees would form an equivalence class. The size of an equivalence class is equal to the number of rows with the same values for quasi-identifiers.

For each row, the probability of re-identification is equal to 1 divided by the size of its equivalence class. For example, each row in an equivalence class of size 5 has a probability of re-identification of 0.2.

[13] See ibid., 279–282.

$$\text{Probability of re-identification for a given row} = \frac{1}{\text{Size of equivalence class}}$$

Rows with larger equivalence classes have lower probabilities of re-identification, since more rows and therefore more individuals in the data set have the same values for quasi-identifiers. Rows with smaller equivalence classes have higher probabilities of re-identification, since less rows (less individuals) have the same values for quasi-identifiers.

4.2 APPLY THE APPROPRIATE RISK MEASUREMENT METHOD

While the probability of re-identification of each row is equal to 1 divided by the size of its equivalence class, there are different ways to use these values to measure the amount of re-identification risk in the data set, depending on the release model used.

Public Data Releases: Maximum Risk

For public data releases, you should assume that someone will attempt a demonstration attack for publicity. These kinds of attacks will target the most vulnerable rows in the data set, which are those with the smallest equivalence classes and highest probability of re-identification. Because of this, you should use the maximum probability of re-identification across all rows to measure the amount of re-identification risk.

Non-Public Data Releases: Strict Average Risk

For non-public data releases, because access to the data set is limited to a select number of identified recipients, you should assume that no row is more vulnerable than others to a re-identification attack. Here, you should use the average probability of re-identification across all rows to measure the amount of re-identification risk in the data set. However, to protect against unique rows or equivalence classes with a high risk of re-identification, the average should be a "strict" average where no row may have a probability of re-identification that is greater than a specific value. A cut-off of 0.33 is often proposed, that is, the smallest size of equivalence class in the data set should be 3.[14] In practice, however, a maximum probability of re-identification of 0.5 may also be used, which in the case of strict average ensures that there are no unique rows and that the average risk is acceptably small.

Semi-Public Data Releases: Maximum Risk

Because semi-public data releases are available to anyone for download, you should assume that the most vulnerable rows will be more at risk of attack than others. Because of this, like public data releases, you should use the maximum probability of re-identification across all rows to measure the amount of re-identification risk.

[14] See El Emam and Malin, "Appendix B: Concepts and Methods for De-identifying Clinical Trial Data."

STEP 5: MEASURE THE CONTEXT RISK

While the risk from the data set plays an important role in determining the level of re-identification risk involved in the release of a data set, it is not the only factor to consider. The re-identification risk is also a function of the kinds of re-identification attacks that are possible on the data set given the release model used. Further analyzing the re-identification risk in terms of possible attacks produces the context risk. Together with the data risk, this value is used to calculate the overall risk of re-identification involved in the release of a data set (in step 6).

The context risk is the probability of one or more re-identification attacks being launched against a data set. While re-identification attacks may be launched on any de-identified data set once it has been released, the adversaries and kinds of attacks differ depending on the release model used.

PUBLIC DATA RELEASES

The calculations used to measure the context risk for public data releases are straightforward. Because the data set is made available to anyone for download or use without any conditions, you should assume that someone will attempt a demonstration attack for publicity. The probability of an adversary launching a re-identification attack against the data set is therefore 1.

NON–PUBLIC DATA RELEASES

In contrast, the calculations for measuring the context risk for non-public data releases, in particular the methods and equations used to determine the probabilities of possible re-identification attacks, are more complex and may require specialized knowledge or skills to carry out. As noted in the introduction, if you are not confident in your abilities to carry out these calculations, you may wish to seek advice from technical staff or other experts in the field.

If technical or expert advice is not available, another option is to measure the context risk as though it were for a public data release using the (much simpler) method above. While this may result in a data set with lower utility, the amount of protection against re-identification attacks would be equal to a non-public data release, if not greater.

For non-public data releases, the probabilities of three different re-identification attacks or threats need to be determined:

1. deliberate insider attack
2. inadvertent recognition of an individual in the data set by an acquaintance
3. data breach

You should use the highest of these probabilities when measuring the context risk.

Attack 1: Deliberate Insider Attack

The probability of a recipient of a non-public data release attempting to re-identify one or more individuals in the data set is based on two factors:

1. the extent of the controls set out in the data sharing agreement regarding the privacy and security of the data
2. the motives and capacity of the recipient in regards to performing a re-identification attack

Both of these factors entail qualitative assessments, resulting in values typically in the range of “low,” “medium” or “high.”

Privacy and Security Controls

Depending on the privacy and security controls set out in the data sharing agreement for a non-public data release, the probability of a recipient attempting to launch a re-identification attack may vary. The higher the level of privacy and security controls, the lower the probability of a re-identification attack being launched. While a more complete list of controls is available,[15] some privacy and security controls that may be considered in a data sharing agreement include:

- recipient allows only “authorized” staff to access and use data on a “need-to-know” basis (only when required to perform their duties)
- a non-disclosure or confidentiality agreement (pledge of confidentiality) is in place for all staff, including external collaborators and subcontractors
- data will be disposed of after a specified retention period
- data will not be disclosed or shared with third parties without appropriate controls or prior approval
- privacy and security policies and procedures are in place, monitored and enforced
- mandatory and ongoing privacy, confidentiality and security training is conducted for all individuals and/or team members including those at external collaborating or subcontracting sites
- a breach of privacy protocol is in place, including immediate written notification to the data custodian
- virus-checking and/or anti-malware programs have been implemented
- a detailed monitoring system for audit trails has been instituted to document the person, time and nature of data access
- if electronic transmission of the data is required, an encrypted protocol is used

[15] See the list of privacy and security controls available in Appendix 1 of Khaled El Emam et al., “Evaluating the Risk of Re-identification of Patients from Hospital Prescription Records.” *Canadian Journal of Hospital Pharmacy* 62, no. 4 (Jul-Aug 2009): 307–319, **http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2826964/**.

- computers and files that hold the disclosed information are housed in secure settings in rooms protected by such methods as combination lock doors or smart card door entry, with paper files stored in locked storage cabinets[16]

Motives and Capacity

Additional factors to consider when determining the probability of a recipient attempting to launch a re-identification attack are their motives and capacity. The more motivated and more capable the recipient is with respect to re-identifying one or more individuals in the data set, the higher the probability of a re-identification attack being launched. When assessing motives and capacity, consider:

- whether the recipient has worked with your institution in the past without incident
- whether possible reasons exist, financial or otherwise, for the recipient to attempt to re-identify one or more individuals
- whether the recipient has the technical expertise and/or financial resources to attempt any re-identification
- whether the recipient has access to other private databases or data sets that could be linked to the data to re-identify one or more individuals[17]

Probability of Re-identification Attack

Based on the level of privacy and security controls in the data sharing agreement and the motives and capacity of the recipient, the probability of a deliberate re-identification attack being launched by an insider may be estimated. The following table may be used as a guideline in determining what may be considered an acceptable estimate for the probability of a re-identification attack being launched against non-public data sets.[18]

Privacy and Security Controls	Motives and Capacity	Probability of Re-identification Attack
High	Low	0.05
	Medium	0.1
	High	0.2
Medium	Low	0.2
	Medium	0.3
	High	0.4
Low	Low	0.4
	Medium	0.5
	High	0.6

[16] See El Emam, *Guide to the De-identification of Personal Health Information*, 290–371. This section of El Emam's book also contains an assessment tool that may help in determining the level of privacy and security controls in a data sharing agreement.

[17] See ibid., 373–376. This section of El Emam's book also contains an assessment tool that may help in determining the level of motives and capacity of a recipient.

[18] See ibid., 208.

Attack 2: Inadvertent Recognition of an Individual by an Acquaintance

In addition to deliberately attempting a re-identification attack, the recipient of a non-public data release may also inadvertently re-identify one or more individuals. This could happen if, while analyzing the data, they recognize a friend, colleague, family member or acquaintance. The probability of such an "attack" occurring is equal to the probability of a random recipient knowing someone in the data set. To calculate this, the following equation may be used:

$$1 - (1 - p)^m$$

In this equation, *p* is the percentage of individuals in the population who have the condition or characteristic discussed in the data set and *m* is the number of people, on average, that an individual knows.[19] Take, for example, a data set about individuals who carpool to work. Based on values of *p* and *m*, the equation would give the probability that a random individual knows someone who carpools to work.

The value of *p* should be determined by recent population statistics. On the other hand, the value for *m* may vary depending on the kind of relationship with an individual required to have knowledge about them regarding the condition or characteristic discussed in the data set. For friends, you should in general use a value of *m* between an average of 150, that is, "Dunbar's number,"[20] and 190.[21]

Attack 3: Data Breach

The third attack to consider in the case of a non-public data release is that of a data breach on the part of the recipient. If a data breach occurs at the recipient's facilities, you should assume that an external adversary will attempt a re-identification attack. Therefore, the probability of such an attack occurring is equal to the probability of a breach occurring at the recipient's facilities. To calculate this value, you should use publicly available data on the prevalence of data breaches in the recipient's respective industry.

SEMI–PUBLIC DATA RELEASES

The possible re-identification attacks for semi-public data releases can be considered the same as those for non-public data releases. Accordingly, to measure the context risk for semi-public data releases, you should use the same method and equations as for non-public data releases, with one adjustment. With respect to "Attack 1: Deliberate Insider Threat," you should assume that the recipient has high motives and capacity and, at best, low privacy and security controls. This is because semi-public data releases are available to anyone for download and are limited in terms of the amount of protection they can provide.

[19] See ibid., 211.

[20] See "Dunbar's number," *Oxford Dictionaries,* **http://www.oxforddictionaries.com/definition/english/dunbar's-number**.

[21] See El Emam, *Guide to the De-identification of Personal Health Information*, 213.

When developing the terms-of-use agreement, you should include provisions that, at a minimum, prohibit recipients from:

- attempting to re-identify individuals in the data set
- linking to external data sets or information
- sharing the data set without permission

STEP 6: CALCULATE THE OVERALL RISK

Once the data risk and the context risk have been measured, the overall risk of re-identification can be calculated. The overall risk is equal to the data risk multiplied by the context risk.

Overall risk = data risk x context risk

The overall risk is equivalent to the probability of one or more rows being re-identified if an attack was launched. For example, if a data set has a data risk of 0.2 and a context risk of 0.5, the overall risk for the data set is 0.1.

STEP 7: DE-IDENTIFY THE DATA

For a data set to be considered de-identified, any identifiable information must be removed. The values of a data set may be transformed in various ways to remove any information that identifies an individual or for which there is a reasonable expectation that the information could be used, either alone or with other information, to identify an individual. Depending on the type and nature of the identifiers, different techniques may be applied. To remove any identifiable information, you should:

1. mask direct identifiers
2. modify the size of equivalence classes
3. ensure that the overall risk is less than or equal to the re-identification risk threshold

7.1 MASK DIRECT IDENTIFIERS

Variables classified as direct identifiers are not used for data analysis because, as noted above, they are not normally useful for research purposes. Because of this, the simplest, most privacy-protective way of dealing with them is to suppress their values in the data set by removing the column of the directly identifying variable.

However, depending on the nature of the research, there may be a need to contact the individuals involved and notify them of the results. In such cases, the directly identifying variables should be transformed using a different masking technique, such as:

- replacing the values with pseudonyms and maintaining the linking database in a secure location
- encrypting the values and storing the encryption key in a safe place

Because directly identifying variables can be used, either by themselves or in combination with other readily available sources of information, to identify individuals, the utmost care must be taken when performing such transformations. If a directly identifying variable is transformed improperly or in an insecure manner, an adversary may be able to re-identify a large number of individuals.

For example, a common technique for creating pseudonyms is to transform the value of a directly identifying variable into an irreversible code using a one-way hash function. However, this technique may be vulnerable to brute force attacks if the total number of possible values of the variable is small enough that the adversary can compute the hash values of all the possible values of the variable in a reasonable amount of time and use this to create a reverse lookup table of hashed and original values. To protect against such attacks, you should always add random data to the input of a one-way hash function and maintain this “salt” or “key” along with the linking database in a secure location.

7.2 MODIFY SIZE OF EQUIVALENCE CLASSES

For a data set to be considered de-identified, the overall risk of re-identification must be less than or equal to the re-identification risk threshold. If the overall risk is greater than the re-identification risk threshold, you must modify the size of equivalence classes in the data set in order to reduce the data risk.

Depending on the values of its quasi-identifiers, a data set may have equivalence classes of different sizes. De-identification involves transforming the values of quasi-identifiers in various ways to modify the size of equivalence classes in a data set. Two techniques to do this are generalization and suppression.

Generalization

Generalization is the process of removing precision from a value to produce a more general value. It may be applied in increasing amounts. For example, a full date may be generalized to month and year, which may in turn be generalized to year, which may in turn be generalized to five-year interval, 10-year interval, and so on.

When using generalization, you should apply it to all the rows of a variable. You should also ensure that the set of generalizations used within a variable are uniform and do not overlap. For example, a uniform set of five-year age intervals would be 10–14, 15–19, 20–24, 25–29, 30–34, and so on.

There is one exception to this. For continuous variables, you may introduce a cut-point at the top or bottom range of values to create a “catch all” category for outliers. For example, the age of individuals may be generalized to year, with a catch all category of “90+” for individuals who are 90 or older. This generalization technique is known as top- or bottom-coding, depending on where the cut-point is made.

Suppression

Suppression is the process of removing values from a data set. In contrast to generalization, which applies to all the rows of a quasi-identifier, suppression affects single rows only. Suppression of a value of a quasi-identifier may happen at different levels. For example, it may involve removing the entire row, the set of quasi-identifiers in the row or only the individual cell. While the less information removed from a data set the greater potential for a higher utility data set, when suppressing a value of a quasi-identifier, you may need to remove the entire row or a set of quasi-identifiers in the row to ensure that the equivalence classes are of the appropriate size.

7.3 ENSURE THAT THE OVERALL RISK IS LESS THAN OR EQUAL TO THE RE-IDENTIFICATION RISK THRESHOLD

If the size of any equivalence class in the data set has been modified, you must recalculate the overall risk of re-identification and compare it to the re-identification risk threshold. For a data set to be considered de-identified, the data risk must be sufficiently reduced so that the overall risk is less than or equal to the re-identification risk threshold.

STEP 8: ASSESS DATA UTILITY

There may be a trade-off between the amount of de-identification applied to a data set and the utility of the resulting information. The more the variables that qualify as quasi-identifiers are de-identified using techniques such as generalization and suppression, the higher the potential for a corresponding loss in the utility of the data set.

While generalization and suppression may be applied to a data set to ensure that the overall risk of re-identification is less than or equal to the re-identification risk threshold, these de-identification techniques may be applied in different ways and combinations to achieve this result. For example, one approach may rely more on generalization and reducing the precision of categories to increase the size of equivalence classes. Another approach may rely more on suppression and removing rows or cells of variables with equivalence classes that are too small. Depending on the properties of the data set, different applications and/or combinations of generalization and suppression may preserve more utility in the information while protecting the privacy of individuals.

As a general rule, suppression should be considered before generalization, unless more than five per cent of the rows in the data set already have some form of suppression.[22] Because suppression removes information from single rows, in contrast to generalization, which reduces the precision of all the rows in the data set, you may wish to consider suppression as a starting point for de-identification.

If the utility of the data set is low or could be improved—for example, more than five per cent of the rows have some form of suppression or further generalization could be avoided by suppressing certain rows or values—you may wish to repeat steps 7.2 and 7.3 above. Applying and/or combining the techniques of generalization and suppression in a new way could produce a higher utility data set while ensuring that the overall risk of re-identification remains less than or equal to the risk threshold.

STEP 9: DOCUMENT THE PROCESS

Each attempt at de-identifying a data set containing personal information should follow the same steps and evaluate the same set of issues. However, the variables and values, and the analysis to determine the amount and kinds of de-identification, will differ for each data release. To help guide you through the complexities and challenges involved in de-identifying personal information, you should consider producing a report documenting the process and its results. There are a number of benefits to this best practice, including:

- the ability to demonstrate due diligence and evidence of compliance, which may be important in the event of a privacy breach or complaint to the IPC
- confidence (of individuals, other institutions, partners and your own management) that best practices are being followed.
- increased transparency, awareness, understanding and trust in your organization’s information management practices

DE–IDENTIFICATION GOVERNANCE

Responsibility for releasing a de-identified data set does not end with the completion of the process for removing any identifiable information. Governance is an important aspect of releasing any de-identified data set. A robust de-identification governance process may include activities such as:

- protecting against attribute disclosure[23]
- ongoing and regular re-identification risk assessments

[22] See Khaled El Emam et al., “A Globally Optimal k-Anonymity Method for the De-Identification of Health Data,” *Journal of the American Medical Informatics Association* 16, no. 5 (Sep-Oct 2009): 670–682, **http://dx.doi.org/10.1197/jamia.M3144**.

[23] See El Emam and Malin, “Appendix B: Concepts and Methods for De-identifying Clinical Trial Data.”

- auditing data recipients to ensure that they are complying with the conditions of the data sharing agreement
- examining the disclosures of overlapping data sets to ensure that the re-identification risk is not increasing with new data releases, or that potential collusion among data recipients does not increase the re-identification risk
- maintaining transparency around the de-identification practices of the institution
- assigning responsibility and accountability for de-identification
- maintaining oversight of changes in relevant regulations and legislation as well as court cases
- developing a response process in case there has been a re-identification attack
- ensuring that individuals performing de-identification have adequate and up-to-date training[24]

While all of the above activities are important to consider when developing a de-identification governance process, the first two raise issues that are specific to de-identification.

PROTECTING AGAINST ATTRIBUTE DISCLOSURE

One of the reasons for releasing de-identified data sets is to provide others with an opportunity to study the values and properties of the raw data and draw inferences from them. This is the primary purpose of statistics and data analysis.

While de-identification techniques protect against the disclosure of individuals' identities, they do not protect against the disclosure of attributes relating to groups of individuals that may be stigmatizing to those individuals. Some inferences may be desirable insofar as they may enhance our understanding of a particular issue or topic. Others may subject groups of individuals to unjust or prejudicial treatment or would be considered offensive. For example, a data set showing whether children of parents with a particular religious affiliation are being vaccinated against certain viruses could result in stigmatization.[25]

The privacy protections set out in *FIPPA* and *MFIPPA* relate to the personal information of individuals only and do not include measures to address potential harms affecting groups of individuals. Nonetheless, as a best practice, you should consider whether any group attributes in a de-identified data set are stigmatizing before releasing the data set. An ethics review of the data set may be needed to achieve this.

[24] See Khaled El Emam, "The Twelve Characteristics of a De-identification Methodology," *Risky Business: Sharing Health Data While Protecting Privacy* (Trafford Publishing: 2013), 134–146 at 141.

[25] See El Emam, *Guide to the De-identification of Personal Health Information*, 9–10.

ONGOING AND REGULAR RE–IDENTIFICATION RISK ASSESSMENTS

Another important step in the process of de-identifying a data set is to classify variables, above all, quasi-identifiers. A challenge with classifying quasi-identifiers is in anticipating the possible sources of background knowledge that an adversary may have, especially since new sources of information may become available at any time.

The potential for individuals to be re-identified by combining new sources of information with otherwise de-identified data is an important privacy concern to consider. Unanticipated sources of information that were not available at the time of de-identification may become available and be used to re-identify individuals.

Once you have released a de-identified data set, you should consider monitoring whether any new sources of information have become available and whether such sources may be used to re-identify individuals in the data set. If so, you should re-assess the classification of variables. Depending on the re-assessment, you may need to mask or de-identify additional variables to ensure that the overall probability of re-identification is less than or equal to the re-identification risk threshold.

In addition, you may also wish to commission a staged re-identification attack on a data set to determine how difficult (or easy) it would be for an attacker to re-identify one or more individuals. This would provide an empirical measurement of the risk of re-identification. While more expensive than statistical evaluations, commissioned attacks should be performed on particularly high-risk data sets, or every few years on other data sets, to understand the attack landscape.[26]

CONCLUSION

De-identification is the process of removing information that identifies an individual or for which there is a reasonable expectation that the information could be used, either alone or with other information, to identify an individual.

De-identification can be a complex and technically challenging process. The risk-based approach developed in these guidelines outlines a step-by-step process for de-identifying data sets in accordance with *FIPPA* and *MFIPPA.*

When attempting to de-identify structured data or data sets, institutions may wish to seek advice from technical staff or other experts in the field, their freedom of information and privacy coordinator or legal counsel. Institutions may also wish to consider automated tools or de-identification software to facilitate the process.

De-identification results in data sets for which the probability of re-identification is very low, given the level of re-identification risk involved in the release. While de-identification techniques protect against the disclosure of individuals' identities, they do not protect against other risks, including the disclosure of stigmatizing group attributes. Institutions should consider instituting a robust de-identification governance process to address additional risks and concerns.

[26] See the "motivated intruder" test in the U.K. Information Commissioner's Office, *Anonymisation Code of Practice,* **https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf**.

APPENDIX A: RESOURCES

Emam, Khaled El. *Guide to the De-identification of Personal Health Information*. Boca Raton, FL: CRC Press, 2013.

Emam, Khaled El. "The Twelve Characteristics of a De-identification Methodology." *Risky Business: Sharing Health Data While Protecting Privacy*. Trafford Publishing: 2013.

Emam, Khaled El and Luk Arbuckle. *Anonymizing Health Data.* Sebastopol, CA: O'Reilly, 2014.

Emam, Khaled El, Fida K Dankar, Régis Vaillancourt, Tyson Roffey and Mary Lysyk. "Evaluating the Risk of Re-identification of Patients from Hospital Prescription Records." *Canadian Journal of Hospital Pharmacy* 62, no. 4 (Jul-Aug 2009): 307–319*,* **http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2826964/**.

Emam, Khaled El, Fida Kamal Dankar, Romeo Issa, Elizabeth Jonker, Daniel Amyot, Elise Cogo, Jean-Pierre Corriveau, Mark Walker, Sadrul Chowdhury, Regis Vaillancourt, Tyson Roffey and Jim Bottomley. "A Globally Optimal k-Anonymity Method for the De-Identification of Health Data." *Journal of the American Medical Informatics Association* 16, no. 5 (Sep-Oct 2009): 670–682, **http://dx.doi.org/10.1197/jamia.M3144**.

Emam, Khaled El and Bradley Malin. "Appendix B: Concepts and Methods for De-identifying Clinical Trial Data." *Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk.* Institute of Medicine of the National Academies. Washington DC: The National Academies Press, 2015. **http://www.ncbi.nlm.nih.gov/books/NBK285994/**.

The Expert Panel on Timely Access to Health and Social Data for Health Research and Health System Innovation, *Accessing Health and Health-Related Data in Canada.* Ottawa: Council of Canadian Academies, 2015. **http://www.scienceadvice.ca/uploads/eng/assessments%20and%20publications%20and%20news%20releases/Health-data/HealthDataFullReportEn.pdf**.

Health Information Trust Alliance, *HITRUST De-identification Framework*, 2015. **https://hitrustalliance.net/de-identification/**.

National Institute of Standards and Technology, *NIST Internal Report 8053. De-identification of Personal Information*, 2015*.* **http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf**.

Office for Civil Rights (OCR), *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, 2012. **http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html**.

PhUSE De-identification Working Group, *De-identification Standard for CDISC SDTM 3.2*, 2015. **http://www.phuse.eu/Data_Transparency.aspx**.

U.K. Information Commissioner's Office, *Anonymisation Code of Practice*, 2012. **https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf**.

"What is a quasi-identifier?" *Electronic Health Information Laboratory.* **http://www.ehealthinformation.ca/faq/quasi-identifier/**.

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The role of the Information and Privacy Commissioner of Ontario is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under the three Acts, the Commissioner:

- Resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction,
- Investigates complaints with respect to personal information held by government or health care practitioners and organizations,
- Conducts research into access and privacy issues,
- Comments on proposed government legislation and programs and
- Educates the public about Ontario's access and privacy laws.

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Website: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

June 2016

APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS

WOMEN'S INTERNATIONAL LEAGUE FOR
PEACE & FREEDOM

This page can't be displayed
• Make sure the web address http://internetshutdown.org is correct
• Look for the page with your search engine
• Refresh the page in a few minutes
Fix connection problems

Why Gender Matters in International Cyber Security

April 2020

Why Gender Matters in International Cyber Security

First edition
28 pp.

Authors: Deborah Brown and Allison Pytlak
Cover illustration: Cathy Chen
Design: Nadia Joubert

www.wilpf.org
www.reachingcriticalwill.org
www.apc.org

Canada

This research was made possible in part by a financial contribution by Global Affairs Canada.

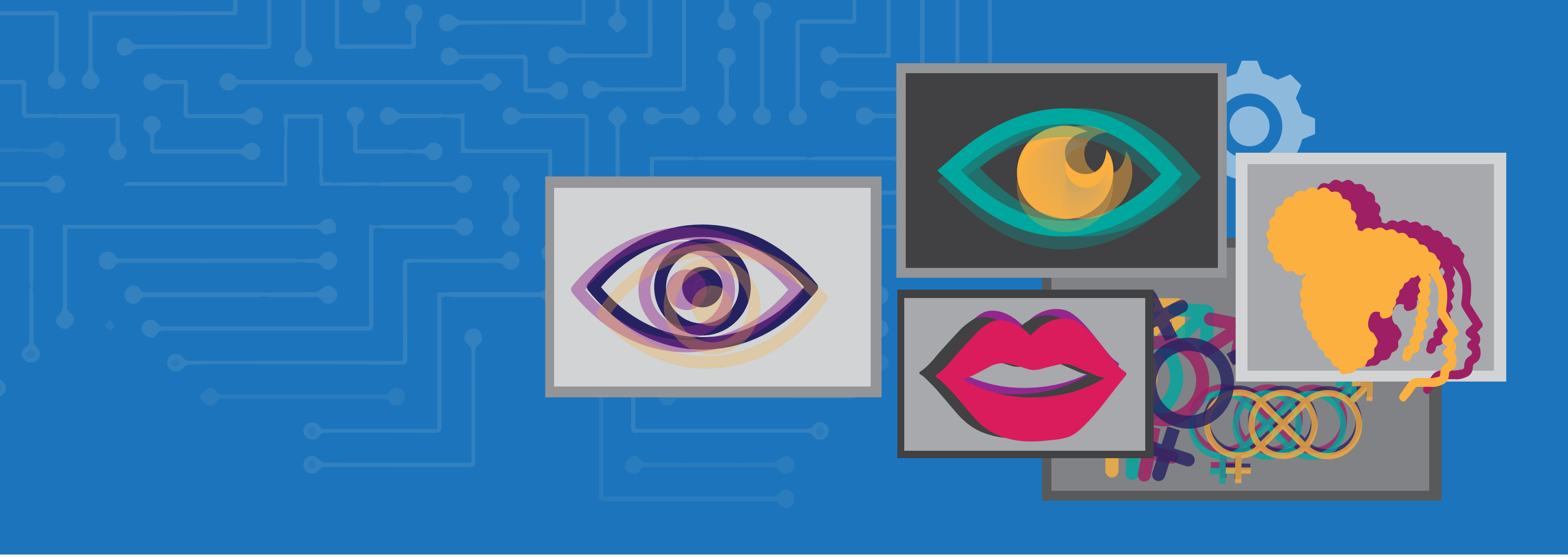


Table of Contents

Section I: Introduction

Gender matters in international cyber security. It shapes and influences our online behaviour; determines access and power; and is a factor in vulnerability, whether real or perceived. As a result, malicious cyber operations can differently impact people based on their gender identity or expression. Online gender dynamics have been shown to reinforce or even amplify the social, economic, cultural and political structures of the offline world. As gender affects the way people and societies view weapons, war, and militarism, a gender analysis of international cyber security can generate more nuanced understandings of the dynamics which shape policy and practice in this area.

Yet, much of what is known about gender and cyber security comes from studies of online gender-based violence (GBV) and gender inequality within the information and communications technology (ICT) sector. There is growing recognition that online GBV is rooted in historical and structural inequalities in power relations between genders, which needs to be addressed as part of broader efforts to realize women's human rights. At the international level, human rights and ‘international security’ are sometimes kept separate, meaning that while human rights should be a consideration when discussing international cyber security[1], the reality is that this has rarely been the case. As a result, less is known about how malicious international cyber operations between states affect people differently on the basis of gender or other characteristics that may put them in positions of vulnerability. While great strides have been made in recognizing the applicability of the human rights framework to threats and abuses against women's digital contexts, including though resolutions and recommendations from authoritative human rights bodies, the gender dimensions of international cyber security remain nearly unexplored.

This report aims to fill that gap. It will have relevance for those working in or studying international cyber security policy, diplomacy, or research as well those interested in the nexus of gender and security. This report, commissioned by Global Affairs Canada, should help to inform recommendations for how multilateral cyber security processes, in particular the United Nations’ (UN) Open-ended working group (OEWG) on ‘Developments in the field of information and telecommunications in the context of international cyber security’ and participating member states can incorporate a gender perspective into future work. It opens by presenting key gender-relevant terms and concepts, alongside relevant frameworks in order to establish a common baseline of knowledge among readers. The subsequent sections use both desk and original research in the form of interviews to consider what are the potential impact of international cyber operations, in particular internet shutdowns, data breaches, and disinformation campaigns. The third section explores gender diversity and women’s participation within cyber policy and diplomacy.

There are some limitations to highlight for readers at the outset. While the subsequent section will unpack terms and concepts that relate to gender, the original research found in later sections of the report focus exclusively on the experiences of women (except where otherwise noted). The researchers fully acknowledge and support the importance of approaching this topic with the wider lens, but because of time and other constraints were unable to examine the broader spectrum of people who may be impacted in relation to their gender identities and expressions. More research in this area should be encouraged. For similar reasons, the research does not include girls in its consideration of gender. The section on participation focuses mainly on the policy and diplomatic sectors within cyber security, and less on technical roles. Finally, the report assumes that readers have more familiarity with cyber security than gender. The researchers relied on desk research and interviews, conducted over a two-month period. Our methodology is detailed at the start of sections III and IV.

[1] Deborah Brown and Anriette Esterhuysen, “Why cybersecurity is a human rights issue, and it is time to start treating it like one”, Association for Progressive Communications, 28 November 2019, https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one

Section II: Framing

Gender perspectives are being more readily accounted for and discussed in multilateral peace and security forums that have traditionally addressed security from a state-centric and militaristic lens. This is a positive step forward but in order to be impactful, it's important to have clarity and common understanding of key terminology and concepts, in order to avoid their conflation or misuse.

To begin, gender is not interchangeable with biological sex (i.e. male, female, intersex). Gender refers to the roles, behaviours, activities, attributes and opportunities that any society considers appropriate for girls and boys, and women and men. Gender interacts with, but is different from, the binary categories of biological sex.[2] Significantly, gender constructs determine who holds power, whether in families, societies, and even in global affairs.[3]

As such, a gender analysis, sometimes described as applying a gender perspective, can illuminate important patterns within armed violence and conflict, and how it is differently experienced as based on gender. This in turn can help inform policies and programs that specifically address these challenges. A gender analysis asks questions about how an experience is different for someone on the basis of their gender identity, and also examines relationships between genders, including what that means for power, access, and limitations.

To use an offline example: it is well-established that there is a strong correlation between gun cultures and perceptions of manliness. In fact in the United States (US) a statistical correlation between domestic violence and mass shootings has also been documented.[4] Cultural norms of masculinity have long denoted men as protectors and as warriors in ways that encourage violence and often, the use of guns, whether as soldiers or in the context of urban gang violence.[5] Acknowledging this enables policy and programmatic responses that focus on addressing violent masculinity as a root cause of violence and gun cultures, in addition to reducing access to and availability of weapons.

In the digital space, gender analysis can reveal the power dynamics which influence, for example, why there is a preponderance of men working in cyber security fields, and how offline inequalities are exacerbated through growing gender digital divides.[6] There is also a gender dimension present in data collection and surveillance[7], as activities that are inherently about labeling and categorising individuals through methods are often predicated on existing binary gender norms. Systems developed by such data can be exploited in ways that either perpetuate such norms—for example, by contributing to unrealistic expectations of female beauty or binary definitions of gender—or to limit access and discriminate against those who do not conform.

Violence that is perpetrated against a person on the basis of gender is known as gender-based violence (GBV). Acts of GBV violate a number of human rights principles enshrined in international instruments and can constitute violations of international humanitarian law (IHL) if perpetrated during armed conflict.[8] There are four generally recognized forms of GBV: physical, sexual, psychological/emotional, and economic, although others are increasingly being recognized as well.

[2] World Health Organization, https://www.who.int/health-topics/gender

[3] UN Women, https://www.un.org/womenwatch/osagi/conceptsandefinitions.htm

[4] Jane Mayer, "The Link Between Domestic Violence and Mass Shootings", *The New Yorker,* https://www.newyorker.com/news/news-desk/the-link-between-domestic-violence-and-mass-shootings-james-hodgkinson-steve-scalise

[5] Henri Myrttinen, "Disarming Masculinities", *Disarmament Forum: Women, Men, Peace and Security,* UN Institute for Disarmament Research, Vol. 4, pp. 37–46.

[6] International Telecommunication Union, "Bridging the gender divide", https://www.iatu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx

[7] Privacy International, *From Oppression to Liberation: Reclaiming the Right to Privacy,* November 2018, https://www.privacyinternational.org/report/2457/report-oppression-liberation-reclaiming-right-privacy. https://www.apc.org/sites/default/files/APC_submission_Gender_Perspectives_on_Privacy_Oct_2018.pdf

[8] Ray Acheson, *Gender-Based Violence and the Arms Trade Treaty,* 2015, p.6, http://www.reachingcriticalwill.org/resources/publications-and-research/publications/10112-gender-based-violence-and-the-arms-trade-treaty

GBV tends to have a disproportionate impact on women and girls, due to their subordinate status in society and vulnerability to violence, but this does not mean that all victims of gender-based violence are women. Men and boys, trans or intersex people, may also be victims of GBV, and it can also be conducted against individuals on the basis of sexual orientation and gender identity; in fact, men and boys tend to be targeted for GBV when their sexual orientation or gender identity diverges from gender norms Therefore, violence against women (VAW) fits within and constitutes GBV but is a narrower and more limited term.

Online GBV is an act of GBV that is committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as mobile phones, the internet, social media platforms, and email. Online GBV tends to mirror and exacerbate gender norms and inequalities of the offline world.[9] It is often directed at those who break from—or are perceived as breaking from—traditional gender norms in any range of ways, whether it be sexual orientation or gender identity, choice of profession, physical appearance, lifestyle, athletic or intellectual ability, or political views, as just some examples. Non-conforming behaviour frequently becomes the focus of abuse; a lot of trolling, for example, uses language and insults that are highly gendered—misogynist or anti-gay rhetoric, threats of rape, etc. With the emergence of social media in particular, sexual and intimate partner violence have taken on new dimensions that include bullying, defamation, impersonation, surveillance, tracking, and harassment as well as non-consensual sharing of photos or messages.

Finally, there are also important distinctions to be made between gender diversity, equality, equity, parity, and women's participation. Sometimes these terms are used interchangeably within UN settings or are selected for use deliberately because of their respective and perceived political viability, in that some may be considered as more 'ambitious' than others, or touch on cultural sensitivities. Diversity would encourage just that—space for the views and inputs of individuals on the basis of diverse identifying features or attributes; in this case gender but which could include other intersecting characteristics. Parity has often been used to advocate for a 50/50 participation ratio between two sexes in a given setting. Somewhat similarly, equality emphasizes that all genders receive the same resources or rights; whereas equity means fairness of treatment for all genders according to their respective needs. Women's participation lifts up the involvement of women alone and is necessary for women's equity, in that participation means that women themselves can identify their unique needs, but also contribute experiences and perspectives so that any policy (or other) output works for the women it impacts. Participation is one of four 'pillars' of the Women, Peace and Security (WPS) Agenda established by UN Security Council Resolution 1325, outlined in Annex I, yet is sometimes overshadowed by other of the pillars, notably the 'protection pillar'.

Understanding the Normative Landscape

There are relevant instruments, agendas, and frameworks that policymakers in global cyber security can draw from when seeking to advance a gender perspective within multilateral cyber security, either as a source of information or to establish policy coherence with states' existing commitments to gender equality.

This includes the WPS Agenda, as established by UN Security Council resolution 1325 and WPS National Action Plans; the Beijing Declaration and Platform for Action; the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW Convention); the 2030 Agenda; UN Human Rights Council (HRC) Resolution 38/5; outcome documents of the World Summit on the Information Society; International Telecommunication Union (ITU) Resolution 70; and the Feminist Principles of the Internet, developed by the Association for Progressive Communications (APC). These are all outlined in Annex I.

[9] *Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences,* November 2017, https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf

In Focus: A gender analysis of the 2015 UN cyber norms

The 2015 UN Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace in the context of international security issued a consensus report, which[10] *outlines eleven recommendations for voluntary, non-binding norms and principles for responsible state behavior in cyberspace. These were endorsed by the UNGA and now form a baseline for discussion in the UN OEWG.*

As already explained, a gender analysis asks questions to reveal underlying gender and power dynamics and differentials in any given situation. Common questions would include: Where are the women, girls, men, boys in this context? What are they doing? Which women, girls, men, boys? What are their respective needs, interests, and vulnerabilities? What are structural power relations between and among them?

A gender analysis of the eleven norms and principles reveals the following guidance for a more gender-sensitive approach to their implementation:

- *Define "critical infrastructure" in ways that are human-centric and holistic. Recognize that a breakdown or loss of different critical infrastructures would be experienced differently on the basis of gender. (Norms f, g, and h)*
- *Build understanding of the gender components of the Human Rights Council and General Assembly resolutions referenced in norm e, as well as of newer iterations of those resolutions*[11] *and who they link to the mandates of the OEWG and GGE. These resolutions, as well as the 2018 HRC resolution, "Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts" (38/5) outline existing state commtments to promoting and protecting women's human rights, which have linkages to the differential harms women face in the context of international cyber incidents (as explored in this report).*
- *In applying measures to increase security and stability of ICT practices (norm a), states should acknowledge that threat models and what is deemed harmful is informed by gender.*
- *When considering all relevant information in the case of an ICT attack (norm b), states include research into possible gendered impacts, and work inclusively with all stakeholders to understand the larger context of an ICT incident, including its impact on the enjoyment of women's rights.*
- *Capacity-building or other measures to build a global culture of cyber security to protect critical infrastructure (norm g) should be developed inclusively with full participation by a diverse set of women and LGBTIQ individuals and seek to illuminate the gender dimensions of cyber security operations.*

[10] UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* Resolution A/70/174, 22 July 2015, https://undocs.org/A/70/174

[11] The 2016 and 2018 versions of the HRC resolution on the *Promotion, protection and enjoyment of human rights on the internet* (32/13 and 38/7) condemn online gender-based attacks and include calls to bridge the gender digital divide. The 2018 UNGA resolution on *Privacy in the digital age* (73/179) included calls on states to consider developing, reviewing, implementing, and strengthening gender-responsive policies that promote and protect the right of all individuals to privacy in the digital age.

Section III: Differentiated Impact of Cyber Incidents on the Basis of Gender

It is well established that women are uniquely and disproportionately affected by conflict and other threats to international peace and security. While men are often the main combatants, women are impacted in less visible ways or are targeted for being women.[12] There is, however, little data on how this differentiated impact can be better understood and addressed within the field of ICTs in the context of international security. This section aims to address this question. Before addressing the specific needs and threats faced by women in potential conflicts in cyberspace, it is necessary to contextualize women's differential experiences in their use of ICTs.

First, women do not enjoy equal access to ICTs. According to the ITU, in 2019, the proportion of women using the internet globally was 48 percent, compared to 58 percent of men.[13] While in some regions, such as the Americas, the gender gap is nearly zero, and in others, such as the former Soviet countries and Europe, it is shrinking, in many parts of the world—in particular the Arab States, Asia, the Pacific, and Africa—the gender gap has actually grown between 2013 and 2019. Women's ability to gain meaningful internet access[14] is influenced by factors including location, economic power, age, gender, racial or ethnic origin, social and cultural norms, and education, amongst other things.[15] Disparity and discrimination in these areas translate into specific gender-based challenges and barriers to meaningful access.

For example, in India it is critical to look at the context and how access to the internet is gendered. Ninety percent of people access the internet through a mobile device, with families typically having one device, access to which is controlled by a man. There are time limitations on when women can use the device and content limitations on what women can access. Some uses of mobile connectivity that are gendered include relying on devices to reach out to family, ordering a ride sharing service when feeling unsafe, and for educational purposes.[16] Multiple interviews conducted for this section of the research stressed the importance of situating the differential way women experience threats in cyberspace in the underlying and more fundamental gender divides that are located within economic, social, political, and cultural contexts that recognize existing inequalities, which among other things, includes unequal access to the internet. Taking an intersectional approach was also emphasized, given that gender is one of many critical factors that impacts how people experience threats in cyberspace. Location (urban vs. rural) socioeconomic levels, and political stability/instability are also key.

Second, threats women face in cyberspace cannot easily or neatly be separated from their offline lived realities. Online GBV is experienced on a continuum, as is demonstrated by the fact that the online doxxing of women can result in-person rape and death threats and even bomb scares.[17] Even when there is a data breach or intentional disclosure of personally identifiable information that is not targeted at women, women can experience differential impacts because of underlying inequality and discrimination.

[12] See, for example, *Women, Peace and Security: Study of the UN Secretary-General pursuant to UN Security Council Resolution 1325*, 2002 and UN Office for the Coordination of Humanitarian Affairs, *Global Humanitarian Overview* 2019, p. 17.

[13] ITU Backgrounder, "Bridging the gender divide", https://www.itu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx

[14] "Meaningful internet access" should be construed as pervasive, affordable connectivity (of sufficient quality and speed) to the internet in a manner that enables the user to benefit from internet use, including to participate in the public sphere, exercise human rights, access and create relevant content, engage with people and information for development and well-being, etc.; irrespective of the means of such access (i.e. whether via a mobile or other device; whether through private ownership of a device or using a public access facility like a library). See https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3406/437

[15] A. Milek, C. Stork and A. Gillwald, "Engendering communication: A perspective on ICT access and usage in Africa", *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media,* 13(3), 2011, pp. 125-141.

[16] Interview with Mishi Choudhary, Legal Director, Software Freedom Law Center, February 6, 2020.

[17] N. Wingfield, "Feminist Critics of Video Games Facing Threats in 'GamerGate' Campaign", 15 October 2014, https://www.nytimes.com/2014/10/16/technology/gamergate-women-video-game-threats-anita-sarkeesian.html?_r=

Take, for example, the 2017 publishing by WikiLeaks of massive databases containing sensitive and private information of millions of ordinary Turkish citizens, which included a special database of almost all adult women in Turkey.[18] WikiLeaks did not appear to have an agenda to put women at risk in publishing this information. But as Turkish sociologist Zeynep Tufekci put it, “We are talking about millions of women whose private, personal information has been dumped into the world, with nary an outcry. Their addresses are out there for every stalker, ex-partner, disapproving relative or random crazy to peruse as they wish. And let’s remember that, every year in Turkey, hundreds of women are murdered, most often by current or ex-husbands or boyfriends, and thousands of women leave their homes or go into hiding, seeking safety.” In considering the specific needs of women related to cyber security threats and potential conflicts in cyberspace, it is critical to understand that while the threats may be perpetrated or exacerbated through technology, they must be situated in underlying power dynamics and inequalities.

Finally, it is important to note that in many contexts, use of the internet is gendered, and in some cases when they have access, women may be more reliant on the internet. For example, women may be particularly reliant on the internet for earning income or pursuing an education (if for example their responsibilities in the home prevent them from doing so offline), for expressing themselves (especially when it comes to expression or content that is taboo, such as sexual expression or defying gender stereotypes), for accessing information relating to their sexual and reproductive health and rights (which may not be accessible offline),19 for seeking out services that enhance their physical safety (for example ride hailing and domestic violence services), and for exploring their sexual orientation of gender identity (which may be criminalized or stigmatized if done openly offline). Therefore, threats in cyberspace can have a compounding effect on women because of the empowering effect the internet can have for them.

> ***In Focus – LGBT people’s use of the internet***
>
> *The internet, in part because of the degree of anonymity it can provide, enables individuals and minority groups to associate on sensitive matters, including sexual orientation.*[20] *It creates enabling environments for people to share and seek sensitive information and engage in online associations based on identities which can be illegal in some countries, such as sexual orientations or gender identities. Marginalised or persecuted sexual minorities find spaces for exercising their freedom of expression and association more privately in online spaces as compared to offline spaces. For example, dating apps tailored to LGBT people can provide a unique space to communicate within a safe community without the persecution or stigma that may be experienced in other dating methods. It is therefore crucial that LGBT people have access to tools that enable them to protect the confidentiality of digital communications to ensure their enjoyment of human rights. A global survey conducted by APC as part of the EROTICS (Exploratory Research on Sexuality and the Internet) project*[21] *revealed that “the internet is considered an ‘important’ or ‘very important’ medium of sexual expression by 66 percent of the sample (among them, 39% consider it ‘very important’).”*[22] *However, while the internet*

[18] Z. Tufekci, “WikiLeaks Put Women in Turkey in Danger, for No Reason (UPDATE)” 25 July 2016 (Updated 6 December 2017) https://www.huffpost.com/entry/wikileaks-erdogan-emails_b_11158792

[19] Example from Bachchao project research: The reference material a researcher needed for her dissertation on women’s studies was not available at the local public library, university or other avenues, which prompted her to search for it on Archive.org. The researcher also gave the example of using YouTube to get videos, which are helpful for adolescent girls, on topics like menstrual hygiene. One respondent in her early twenties said that she watches videos on YouTube to expand her knowledge of handmade embroidery and to learn to use new machines. Both examples illustrate that young women actively use the Internet for gaining knowledge, nurturing their ambitions and learning the skills that contribute to their livelihood. See: Chinmayi S K and Rohini Lakshané, *Of Sieges and Shutdowns: How unreliable mobile networks and intentional Internet shutdowns affect the lives of women in Manipur,* The Bachchao Project, 2018 http://thebachchaoproject.org/wp-content/uploads/Of_Sieges_and_Shutdowns_The_Bachchao_Project_2018_12_22.pdf

[20] APC, *The right to freedom of expression and the use of encryption and anonymity in digital communications: Submission to the United Nations Special Rapporteur on the right to freedom of opinion and expression,* 2015, https://www.apc.org/sites/default/files/APC%20submission%20to%20SR%20FOEX_20150211_0.pdf

[21] EROTICS is a network of activists and researchers working at the intersections of sexuality and the internet. More information at: https://erotics.apc.org/about-erotics

[22] H. Vale, “Body as data: EROTICS exploratory research on sexuality, rights and the internet”, https://slides.com/hvale/body-as-data-dataveillance-the-informatisation-of-the-body-and-citizenship#/1

> *is an essential tool to communicate and spread critical information regarding LGBTIQ activism, these activists also face significant threats online: "the most frequent is harassment (75%), followed by intimidating online comments (63%) and blocked websites or filtering software that prevented the user from accessing information (54%)."* [23]
>
> *An interview conducted for this research with a person from Iran, who wishes to remain anonymous, demonstrates just how critical the internet can be for LGBTQ people in an environment in which their very identity is criminalized. In this person's words, "After coming to terms with my identity and orientation I did what I knew best: I established a network through which we tried to provide support to LGBTQ people. Our work included translation and online distribution of pamphlets, along with offering some support to those who were facing problems at home. You certainly know how things are in Iran. Parents usually get oppressive and violent when their kids come out. Even if they don't, the coming out process is complicated. Both parents and their kids need guidance which was (and is) nonexistent in Iran. Most people do not have access to queer-friendly sources of information. This gets worse especially when people come from less well-off backgrounds. They haven't got proper English training and Persian sources were, and I think still are, scarce. We also used to provide some help to transgender people. At the time we used Yahoo Messenger for communicating. Using the service we were able to prevent a few self-harm incidents by simply listening to the people."* [24]

Internet Shutdowns

While internet shutdowns are primarily used as a tool by governments against people under their jurisdiction, they have also been used as a tactic during conflict against other populations, such as Russia's 2016 shutdown of the internet in Crimea[25] and by cybercriminals, who have launched cyberattacks across borders, such as the attack that took Liberia offline in 2016.[26] Because internet shutdowns conducted by a government domestically are much more common and better documented, the researchers were able to study the gender dimensions of this phenomenon, from which it is possible to extrapolate the gendered impact of internet shutdowns when carried out in the context of international cyber conflict.

The methodology for this section relied on a combination of desk research and interviews, with a heavy reliance on the latter given there is very little published on the gender dimensions of internet shutdowns, despite the practice being widespread. The researchers compiled a list of all the internet shutdowns documented in 2018 and endeavored to interview people who either experienced those shutdowns or conduct research or advocacy around those shutdowns. Time constraints meant that it was not possible to interview people from each country that experienced shutdowns, so the researchers aimed to reach countries from different regions and political contexts. Interviewees were a mix of people who experienced shutdowns firsthand, and those who work on the issue (as journalists, researchers or advocates) in or from the countries in question. All interviewees were women, with the exception of a queer person from Iran, who spoke on the condition of anonymity. Countries covered by the interviews were: Cameroon, Democratic Republic of Congo (DRC), Ethiopia,[27] India (2), Iran (2), Pakistan, and Venezuela. One interviewee covered the issue globally, as she led a global campaign to counter internet shutdowns. The shutdowns covered in this research are not representative or in any way comprehensive but shed light into the different ways that internet shutdowns can affect women.

[23] APC, *EROTICS Global Survey 2017: Sexuality, rights and internet regulations,* https://www.apc.org/sites/default/files/Erotics_2_FIND-2.pdf.

[24] Anonymous interview, February 20, 2020.

[25] Hayes Brown, "Russia Cuts Off the Internet in Crimea," 11 August 2016, https://www.buzzfeednews.com/article/hayesbrown/russia-cut-off-the-internet-in-crimea

[26] Dominic Casciani, "Briton who knocked Liberia offline with cyber attack jailed", 11 January 2019, https://www.bbc.com/news/uk-46840461

[27] The interviewee from Ethiopia has expertise on internet shutdowns globally as the lead of the KeepItOn campaign, so her contribution to this research extended beyond Ethiopia.

Internet shutdowns can be defined as “an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.”[28] The UN Human Rights Council (HRC) has unequivocally condemned “measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law” and called on all States to “refrain from and cease such measures.”[29] The shutdowns covered in this research include years-long shutdowns as well as shorter ones, bans on popular social media and communications platforms and total communication blackouts, and shutdowns occurring in times of conflict and other forms of political turmoil.

For the most part, internet shutdowns are blunt tools that hit entire communities. However, because of power differentials in society and the specific ways that women use the internet, research conducted found that there were gendered impacts of internet shutdowns studied. A comment from an interviewee from Venezuela captured this well:

> *“I feel that due to certain gender roles, women are affected differently, particularly in Venezuela. We are left with a lot of the caregiving responsibilities – take care of the food, paying the bills – and in these situations [shutdowns] our ability to solve certain problems is restricted. Having access to certain information is key – during a blackout, my sister won’t know if she should take her daughter to school or not, and my friend won’t have a way of checking in with her boss since she telecommutes, thus facing the possibility of being fired and not being able to provide for her children since she’s a single mom.”* [30]

A few themes emerged concerning the ways in which gender impacted women’s experiences of internet shutdowns: personal safety, professional/economic impact, emotional wellbeing, education, and connectivity.

Personal safety

A common theme from interviewees and existing literature is that mobile phones increase the perceived levels of security among women outside their homes and in public places. The study “Of Sieges and Shutdowns: How unreliable mobile networks and intentional Internet shutdowns affect the lives of women in Manipur'' interviewed women in northeast India and found “[h]aving a phone is a way of feeling secure. When in 2006, there were not many mobile phones in Manipur, we were doing focus group discussions with women on the status of security of women. One of the outcomes was [that] women would feel safe if they had a mobile phone. But we did not think that it would turn [into] a reality in 2016 where every woman has a phone. Today it’s a better situation because women can inform their family members if they are going to be late or if they go out.” [31]

Physical violence against women in publicis a common phenomenon in many parts of the world. An interviewee gave the example of a contact in Tehran who is a single woman in her 30s, who lives near an area that was quite violent during the protests in late 2019, where women were getting arrested and assaulted. When the government shut down the internet during the protests, it left the woman without the ability to be in contact if anything happened to her.The respondent was worried about her contact’s safety. The woman in Tehran reported feeling isolated and afraid to go out.[32] In Pakistan’s Federally Administered Tribal Area, or FATA, which has experienced an internet shutdown since 2016, people could go to internet cafes before fixed broadband was cut, but men make it difficult for women to go to internet cafes by creating a very hostile environment.[33]

[28] Berhan Taye, *Targeted, Cut-Off and Left in the Dark: Report of Global Shutdowns,* Access Now, 2019. https://www.accessnow.org/keepiton/#problem

[29] Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet,* Resolution A/HRC/RES/32/13, 18 July 2016, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13

[30] Interview with Marianne Diaz, Analista de Políticas Públicas Derechos Digitales, 17 February 2020.

[31] S K Chinmayi and Rohini Lakshané, *Of Sieges and Shutdowns: How unreliable mobile networks and intentional Internet shutdowns affect the lives of women in Manipur,* The Bachchao Project, 2018 http://thebachchaoproject.org/wp-content/uploads/Of_Sieges_and_Shutdowns_The_Bachchao_Project_2018_12_22.pdf

[32] Interview with Mahsa Alimardani, Internet researcher that specialises in Iran and the Middle East, 29 January, 2020.

[33] Interview with Hija Kamran and Amel Ghani, Program Managers at Media Matters for Democracy, Pakistan, 3 February 2020.

An interviewee from India noted:

> *"The intersectional impact of a shutdown impacts women differently, especially in Delhi which continuously reports high number of cases of violence against women and sexual harassment. Most of the time, as a woman I share my live location during late night travel or when visiting an area less traveled. Further, since I personally visit social protests to report on them, keeping in contact with my colleagues and family becomes important. With the internet being suspended, reaching out for help becomes difficult. Further, during protests, minorities depend hugely upon community support, which is usually achieved through online messaging platforms. Not being able to use that is hugely restraining."* [34]

During partial internet shutdowns, people may be able to find ways to access the internet, but may not have access to the full range of communication channels that they rely on. For people who rely on secure communications channels because of their sexual orientation or gender identity, for example, being cut off from encrypted communications can be a threat to their safety. “When you are doing what I am doing, you need to constantly be cautious about your communications. Every personal contact can be used against you. In a country where gay relationships are criminalized, not having access to encrypted communication services is scary and life-threatening.” [35]

Professional/economic impact

There are a number of efforts to measure the economic costs of shutdowns, much of which is guesswork in part because so much of the informal sector is typically not included in such measurements. A number of interviews identified women’s use of e-commerce as having a negative impact on their financial well-being when the internet is shut down. For example, in Iran women sell and distribute handcrafts and homemade food through online platforms for industry/e-commerce (Facebook and Telegram)[36]. Internet shutdowns disrupted this. In Cameroon and Ethiopia, women specifically use Whatsapp/Telegram groups to sell household items (such as hair products and spices), outside of the mainstream/formal sector. During shutdowns, they are unable to sell their products.[37] A respondent from DRC similarly noted that women in the informal economy rely heavily on mobile communications to send and receive money.[38]

For women working in the formal economy, especially in sectors dominated by men, they expressed feeling their work and professional achievement was compromised because of internet shutdowns. In fact, both women who expressed this in interviews ultimately decided to leave where they were living, in part because of the impact of the disruptions on their professional life.

An independent woman journalist in Manipur, India who relies heavily on the internet for her work lamented that internet shutdowns affect her work. She explained that as a woman one is already at a disadvantage, and that in a competitive environment where opportunities for women are scarce, internet shutdowns additionally hamper one’s work which has long term effects. In her words, “You miss opportunities… when your connectivity is hampered, your sense of independence is also affected. One may say it affects all… but as [a] woman you feel additionally frustrated, as your sense of empowerment or freedom is being affected…[the] internet gives me a sense of empowerment or say, opportunity to access information, opportunity to network, [I] send my stories across many places and get information from many places. Now, when you don't have access, when the net shuts down you feel disconnected, feel helpless, disempowered. [The] Internet give[s me an] advantage, the edge, and when that is curtailed one feels frustrated and disempowered, all the more as a woman.” [39]

[34] See: Software Freedom Law Centre’s Internet Shutdown Tracker: https://internetshutdowns.in.

[35] Anonymous interview, 20 February 20 2020.

[36] Interview with Mahsa Alimardani, Internet researcher that specializes in Iran and the Middle East, 29 January 2020.

[37] Interview with Berhan Taye, Senior Policy Analyst, Access Now, 10 February 2020.

[38] Interview with Annie Matundu-Mbambi, Chairwoman, WILPF DRC, 24 January 2020.

[39] Interview with Ninglun Hanghal, independent journalist, 18 February 2020.

A civil society activist from Venezuela shared similar frustrations and concerns:

> *"[T]hese constant issues with accessing the internet freely were the main reason why I had to leave Venezuela. I was already working as a researcher for Derechos Digitales and it had become impossible to hold a conference call, to research a paper or to stay on top of emails with less than four hours of reliable internet access a day. I had to face the choice of leaving my work or leaving the country, which was possibly the hardest choice I've had to make in my life."* [40]

Emotional well-being

Harm to emotional well-being is a commonly expressed response to internet shutdowns, both by people experiencing the shutdown and by people in the diaspora.

A woman who experienced an internet shutdown in 2016 in Manpur, India said, "For 15-20 days we could not communicate [with anyone]. No emergency cases happened. But it was scary because we could not communicate with people even when they go to [the] bazaar or if they were late from a travel. There was insecurity and fear."[41]

As an article on the prolonged shutdown in FATA in Pakistan put it, "Women, already deeply vulnerable in Pakistani society at large, are even more oppressed in the tribal areas. Their mobility is very restricted—and now the roads to information have been shut to them. Moreover, many men from FATA move to Gulf states to work as manual laborers on construction sites. Before the shutdown, local entrepreneurs started internet cafes that people could use to talk to their family members abroad. Now that those cafes don't exist anymore, people are forced to go months without talking to family members."[42]

Interview respondents who live outside their country (Iran and Venezuela) reported emotional distress at not being able to be in touch with their relatives, especially their female relatives during times of social/political unrest. "I am the provider/caregiver for my family back in Venezuela, so this means that when they are incommunicado this affects me severely, not only in a logistical manner, but also affects my mental health in a severe way."[43]

A queer person in Iran echoed this sentiment: "If I were to describe the experience in one word I would say, suffocating…young queer Iranians have been able to establish a support network using social media platforms. There are several Iranian news outlets and activists that are publishing LGBT-friendly information as well. The internet shutdown cut off the minority from a source of information and moral support. Everyone was affected by the blackout but queer people were more panicked. They were feeling a sense of isolation. Even amid natural disasters, people find time for love. Without the internet, the chances of meeting another queer person and hitting it off with them is close to zero in oppressive countries like Iran. Furthermore, online services like Telegram and WhatsApp provide people with a secure line of communication. During the shutdown, we were back to old-school telephony services and text messages which are monitored by state authorities. The encrypted messaging apps provide people with a sense of privacy the blackout put an end to that as well."[44]

Impact on education

Beyond impacts on safety, work, and emotional well-being, the research found that there was a gendered dimension to education during shutdowns. For example an interviewee in FATA noted that the shutdown affected people similarly, but because of patriarchy and cultural issues, there are/were differential effects. For example, women don't have much access to education throughout Pakistan, and in the tribal regions in particular. The internet helped women access education, and now that it's off, men still have access to schools, but women do not. Women had to drop out of schools/colleges.[45]

[40] Interview with Marianne Diaz, Analista de Políticas Públicas Derechos Digitales, 17 February, 2020.

[41] Bachchao Project.

[42] Hija Kamran, "A Year Without the Internet", 21 August 2017, ahttps://slate.com/technology/2017/08/the-internet-has-been-shut-down-in-pakistans-fata-for-more-than-a-year.html

[43] Interview with Marianne Diaz, Analista de Políticas Públicas Derechos Digitales, 17 February, 2020.

[44] Anonymous interview, February 20, 2020.

[45] Interview with Hija Kamran and Amel Ghani, Program Managers at Media Matters for Democracy, Pakistan, 3 February 2020.

Finding connectivity during a shutdown

Finally, in cases where the shutdown is partial, for example only covering mobile data, people go to public spaces, universities, and hotels and pay in order to use those services. Women in some contexts may be less likely to have cash to be able to pay for a coffee in a cafe that also offers access, or it may not be safe for them to carry it. In some contexts, due to cultural or security factors, going to a public space, particularly alone, might not be so possible for women. In Ethiopia there was a famous photo that captured this well. It was of people leaning against a university wall checking their mobile phones for an internet connection during a shutdown—all men.[46]

Data Breaches

Data breaches have become commonplace and can occur for a number of reasons, as a result of cybercriminals looking to make a profit, cyberespionage to gather intelligence, or cyber-blackmail to coerce desired behavior. Data breaches can also result from hacking by foreign powers which can be seen as an intentionally wrongful act in cyberspace. While attribution of such attacks is difficult, China's hacking of a United States' Navy contractor in which "massive amounts of highly sensitive data related to undersea warfare" were stolen, is one example.[47] Data collection never takes place in a gender-neutral setting, so when data breaches occur, even if they are not targeting people specifically on the basis of gender, they can have a more severe impact on women and LGBTIQ people because of historical and structural inequalities in power relations based on gender and sexuality. This subsection explores data breaches that did not take place in the context of international conflict in cyberspace due to a lack of available information on those that have, but nonetheless illustrate how data breaches can have a gendered impact.

For example, in July 2016, the municipality of São Paulo experienced a data breach exposing the personal data of an estimated 650,000 patients from the Brazilian public health system. This massive data breach included names, addresses, and medical information such as information about pregnancy and abortion care.[48] According to the media, the personal data was from 2001 to 2007 and referred – in almost all of the cases – to women at some point of their pregnancy. Among those affected were 15,926 mothers who had given birth before seven months of gestation, 4,237 abortions and 181 recent stillbirths. It is worth noting that abortion is illegal in Brazil, so this data breach not only violated the right to privacy of the women affected around a socially sensitive issue, but also exposed them and their doctors to potential criminal charges.

The aforementioned example constitutes a clear example that personal data breaches can dramatically affect not only women's privacy but also their sexual and reproductive health rights, their dignity and self-development. When data breaches occur it is crucial to observe with a gender lens which human rights can be affected and analyse it beyond only a consideration of privacy rights; in this case, a hospital is a critical infrastructure (because of the management of sensitive and health data) that should have heavy security measures as part of a cyber security policy respectful of human rights. This highlights a key point, the need for countries to implement cyber security policies with a human rights perspective.

Another massive data breach occurred in Chile in 2016. In this case, a public hospital suffered a cyber security failure and made available to their workers and even to the general public (via their intranet) more than three million health records including the names, ID numbers, and addresses of women and girls who asked for the morning-after pill in a public hospital and people living with HIV.[49] The authorities had been alerted to this flaw in the hospital's computer system 10 months earlier, but neither the authorities nor the company in charge of

[46] Interview with Berhan Taye, Senior Policy Analyst, Access Now, 10 February 2020.

[47] Ellen Nakashima and Paul Sonne, "China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare", *The Washington Post,* 8 June 2018, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html

[48] R. Hernandes, "Gestão Haddad expõe na internet dados de pacientes da rede pública", Folha de Sao Paulo, 6 July 2016, https://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados-de-pacientes-da-rede-publica.shtml

[49] M. Jara and V. Carvajal, "Grave falla en la red del Minsal dejó expuesta información confidencial de pacientes," CIPER, 3 March 2016, https://ciperchile.cl/2016/03/05/grave-falla-en-la-red-del-minsal-dejo-expuesta-informacion-confidencial-de-pacientes

the hospital's cyber security took action to remedy the situation despite being warned of the risks.[50] The people most affected by the data breach were women, girls, and people living with HIV. Women and sexual minorities are more profoundly affected by the consequences of these kinds of data breaches because they may face discrimination or even prosecution as a result. These breaches impact not only their right to privacy but also their sexual and reproductive health and rights.

Disinformation

Disinformation campaigns involve the deliberate sharing and spreading of false information in order to achieve a desired goal or influence a situation. While political propaganda has existed for centuries, modern disinformation campaigns utilise ICTs, especially social media platforms, in any number of ways: the use of 'political bots' to amplify hate speech or tensions; placing manipulated content to sway opinion; exploiting data about users for micro-targeting; or deploying an army of trolls to harass political candidates, leaders, dissidents, journalists, or ordinary people expressing a political opinion online.[51] As the internet and social media have become primary platforms for information sharing, news, and political campaigning in many countries because of the ease with which people can connect through them, that same easy access—and anonymity—can transform those platforms into arenas of abuse, humiliation, and used to discredit, often on the basis of false information. Traditionally seen as a human rights issue, as it pertains to content, disinformation is rapidly becoming a matter for global security when states use disinformation campaigns to influence events in another country or target foreign nationals.

Research shows that there is a strong gender dimension in politically motivated disinformation activities.[52] As gender identity and sexual orientation are identifiers, they can become the basis on which someone is targeted to receive information across platforms. Doing so makes certain gendered assumptions about one's interests and ability to be influenced.

Gender norms also play a large role in direct attacks of false information. Women are already significantly under-represented in global media coverage of political issues[53] and stories of female politicians and candidates often reinforce highly gendered stereotypes and norms by focusing on the way women are dressed, their body image, and their family life, with much less attention paid to their ideas, policies and proposals.[54] Disinformation activities perpetuate these trends and often in more malicious ways. Ahead of parliamentary elections in Georgia in 2016, for example, several female politicians were targeted by fake videos meant to depict them engaging in sexual activities, and in one case, an extramarital affair. The men implicated in the latter example were not impacted because male adultery is socially acceptable—except for one man who was labelled by media as gay, which put him at risk due to strong homophobia in the country.[55]

In 2018, a shadowy video and blurry screenshots of a naked woman straddling a man was published in the Philippines and were claimed to be Leila de Lima, a senator and strong critic of president Duterte. It was never proven to be her in the video but it damaged her reputation and eroded her support base, which may have made a subsequent political move against her easier.[56]

A woman Al-Jazeera reporter in the Philippines was the target of false stories asserting that she had undergone plastic surgery. A meme was circulated that placed her face beside that of another journalist, with the caption,

[50] Ibid.

[51] Samantha Bradshaw and Philip N. Howard, The Global Disinformation Disorder: 2019 *Global Inventory of Organised Social Media Manipulation,* Working Paper 2019, Oxford, UK, Project on Computational Propaganda.

[52] This report is focusing on women more than other vulnerable or marginalised groups but encourages further research into the differentiated impact of disinformation campaigns on the basis of gender more broadly.

[53] See Global Media Monitoring Project, 2015.

[54] Lucina De Meco, *#Shepersisted: Women, Politics & Power In The New Media World,* Fall 2019, p. 10.

[55] Nina Jancowicz, "How Disinformation Became a New Threat to Women," 11 December 2017, https://codastory.com/disinformation/how-disinformation-became-a-new-threat-to-women/

[56] P. Occeñola, "Fake News Real Women: Disinformation gone macho", 15 December 2018, https://www.rappler.com/newsbreak/in-depth/217563-disinformation-gone-machao

"When the looks God gave you simply isn't enough".[57] The head of a non-governmental organization there explains that male journalists are also attacked "...but when it is a female journalist, it centers on their being a woman, on their bodies, like, 'you're so ugly, but I still hope you get raped.'"

A recent Inter-Parliamentary Union (IPU) survey of 55 women legislators worldwide found that 81.8 percent of the respondents had experienced psychological online gender-based violence, including high incidences of humiliating or sexual images having been circulated, where were often fake or doctored.[58] Tracking in the United States shows that female politicians there are often the target of online abuse and this is a particular problem for women of colour.[59]

Women politicians or other leaders are targeted more often than their male counterparts are; for example, Hillary Clinton received twice as many tweets containing insults and offensive comments as Bernie Sanders during their campaigns for the United States' Democratic Party nomination. The same was true of Julia Gillard in comparison to Kevin Rudd between January 2010 and January 2014, in Australia.[60]

Not all of these activities can be strictly considered as "disinformation", although it could be argued that they should not be discounted either: a high incidence of abuse, with or without an information base, can still serve to deter or discredit. Where disinformation campaign activities influence events in another country, or target foreign nationals, it becomes relevant to international cyber security.

These examples are fewer and suffer from the same attribution challenges as any cyber operation but they do exist. A recent Oxford University report on disinformation notes that the release of limited information about "foreign influence operations" from Twitter and Facebook shows that a small but sophisticated group of countries are engaging in disinformation activities.[61] A Bellingcat researcher revealed in 2019 a disinformation campaign in which Saudi Arabia created more than 300 Facebook accounts and pages masquerading as local news organizations in countries throughout the Middle East and North Africa, in the wake of the death of Jamal Khashoggi.[62] The pages, which were eventually removed by Facebook, posted content praising Crown Prince Mohammed bin Salman, the presumed mastermind behind Khashoggi's death, or targeting enemies of Saudi Arabia, including Amnesty International, Al Jazeera, or countries like Iran. While Russian efforts to meddle in the 2016 US elections through disinformation (and other means) is now common knowledge, what is less known is that as far back as 2014, Russian propaganda operations conducted a dry run, impersonating social media accounts of black feminists in the US in order to gain support among their supporters.[63] In fact, black feminists documented fake accounts, misinformation, bot networks, and weaponized trolls using the hashtag #YourSlipIsShowing.[64] In 2018, a New Knowledge report[65] commissioned by the US Senate described how Russian agents specifically "focused on developing black audiences and recruiting black Americans as assets," but never picked up on the gender dimension of the propaganda operation, or credited the black feminists who documented it.

[57] M. Buster, "Busted: Al Jazeera reporter hits Duterte supporter for claiming she had cosmetic surgery, using a different woman's photo", 20 April, 2017, https://memebuster.net/al-jazeera-reporter-hits-duterte-supporter/

[58] Inter-Parliamentary Union, *Sexism, harassment and violence against women parliamentarians,* October 2016, http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf

[59] M. Astor, "For Female Candidates, Harassment and Threats Come Every Day" 24 August 2018, https://www.nytimes.com/2018/08/24/us/politics/women-harassment-elections.html

[60] E. Hunt, N. Evershed and R. Liu, "From Julia Gillard to Hillary Clinton: online abuse of politicians around the world," *The Guardian,* 27 June 2016. www. theguardian.com/technology/datablog/ng-interactive/2016/jun/27/from-juliagillard-to-hillary-clinton-online-abuse-of-politicians-around-the-world

[61] China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela. See Bradshaw and Howard, p. 2.

[62] See "Inside Saudi Arabia's Disinformation Campaign", *NPR,* 10 August 2019, https://www.npr.org/2019/08/10/750086287/inside-saudi-arabias-disinformation-campaign

[63] R. Hampton, "The Black Feminists Who Saw the Alt-Right Threat Coming", 23 April, 2019, https://slate.com/technology/2019/04/black-feminists-alt-right-twitter-gamergate.html

[64] "Your slip is showing" in the Southern black dialect of South Florida refers to something that's meant to be concealed but is, embarrassingly, on full display.

[65] S. Shane and Sheera Frankel, "Russian 2016 Influence Operation Targeted African-Americans on Social Media", *New York Times,* 17 December 2018, https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html

A Finnish journalist who exposed a fake news operation and troll farm in St. Petersburg was later the target of stories from Russian media outlets alleging that she had engaged in drug use and sales.[66] In the run-up to the 2019 Indonesian elections, Grace Natalie, head of the Indonesian Solidarity Party (PSI), was accused by an anonymous Twitter user of having an extra-marital affair with Pak Ahok, the former governor of Jakarta. The accuser claimed to have access to a sex tape, which they threatened to make public. She challenged him to release it and he did not, which vindicated her, but some speculated that had even a fake video been produced it could have influenced the election. The growth of "deep fakes" are becoming a complicating factor and a new tactic, making it more difficult to distinguish between what is real and what is false.[67]

Section IV: Participation

The 'gender digital divide' is real. As already outlined in this report, there is a substantial, and in some cases growing, divide between women and men in their access to and use of the internet.

Beyond issues of access, there is another dimension of this divide that warrants attention—the gender gap in participation within all aspects of the cyber security field. This gap has been well-established within relevant technological and business sectors. For example, while precise estimates vary, most surveys place women's participation levels in all ICT-related professions at between 15-20 percent, and slightly lower for information security.[68] The World Economic Forum's Gender Gap report notes that only 22 percent of artificial intelligence (AI) professionals globally are female, compared to 78 percent who are male.[69] This is not only problematic in the context of gender parity, but also because it means that technology, which always reflects the values and biases of its developers, will further entrench problematic gender norms and stereotyping.[70] Multiple studies and testimonies highlight how entrenched gender biases and stereotypes are steering girls and women away from science and related fields. Even in countries that score higher in gender equality indexes, this remains a problem.

What has been less examined is the participation of women working in cyber security policy and diplomacy, including confidence and capacity-building measures, whether at national, regional, or international levels. This section will seek to identify gender participation gaps in international and regional cyber security fora, the causes and consequences of such gaps, and practical steps to help address them. Due to the constraints outlined in the introduction, this research is focused primarily on women's participation, although the researchers highlight the necessity of diversity and an intersectional approach. Five interviews were done with women in mid-career to senior positions in national governments, or regional and international organizations, where their role focuses on cyber security in a non-technical way. They were selected for their experience and to ensure regional diversity. Researchers reached out to a further four women for interviews but they were unavailable.

[66] Jessikka Aro, "How pro-Russian trolls tried to destroy me", *BBC,* 6 October 2017, https://www.bbc.com/news/blogs-trending-41499789

[67] Oliver Ward, "Sex and deepfakes: Sexualised misinformation will hamper future female democratic participation," *ASEAN Today,* 21 November 2019, https://www.aseantoday.com/2019/11/sex-and-deepfakes-sexualised-misinformation-will-hamper-future-female-democratic-participation/

[68] See J. Reed, Y. Zhong, L. Terwoerds and J. Brocaglia, *The 2017 Global Information Security Workforce Study: Women in Cybersecurity,* https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf and (ISC)2, The 2013 (ISC)2 Global Information Security Workforce Study, https://www.isc2.org/giswsrsa2013/

[69] World Economic Forum, "Assessing Gender Gaps in Artificial Intelligence", *Global Gender Gap Index 2018,* http://reports.weforum.org/global-gender-gap-report-2018/assessing-gender-gaps-in-artificial-intelligence/

[70] Mahita Gajana, "AI Voice Assistants Reinforce Gender Biases, U.N. Report Says," *Time Magazine,* 22 May 2019, https://time.com/5593436/ai-voice-assistants-gender-bias/

But Why Diversity?

The rationale for improved women's participation, and gender diversity more broadly, is rooted in a simple premise: cyber security is an issue that impacts everyone, and women are stakeholders who should have equal opportunities to participate in the decisions, policies, and programs that will affect them. Their inclusion expands the diversity of perspectives and skills available, thereby contributing to overall effectiveness and sustainability. In particular, as the previous section demonstrated, women face different threats in the context of cyber security, and may bring different threat models and priorities to discussions.

Most research on the specific benefits of gender diversity, or of women, in cyber security come from the private sector and often stresses the "soft skills" that women tend to emphasize in their resumes, such as interpersonal and analytical skills, as well as the "business case" for hiring more women.[71] While this analysis reinforces various gender stereotypes of 'womanly characteristics', it does highlight skill sets that are equally critical for cyber security policy or diplomacy work, such as in the area of confidence-building measures, negotiation, or incident response and coordination.

More is known however about the benefits of women's direct participation in peace negotiations for the longevity and success of related agreements. A study investigating 82 peace agreements in 42 armed conflicts between 1989 and 2011 found that peace agreements with women signatories are associated with durable peace.[72]

Research also shows that women's participation in a negotiation process is more likely to lead to the inclusion of gender provisions; an analysis of 98 peace agreements across 55 countries between 2000 and 2016 found that peace agreements are more likely to have gender provisions when women participate in track 1 or 2 peace processes.[73] It can be inferred then that in order for cyber security policy and diplomacy to reach outcomes that account for the experiences and needs of women, their participation is a necessity—as stakeholders, but also as advocates for themselves.

Security—An Old Boy's Club

It is challenging to paint a statistically precise picture of the current status of women's participation in these aspects of the cyber security field for two reasons: first, the fields themselves are indistinct and individuals may play many roles, such as being involved in national implementation of globally agreed norms, to attending multilateral negotiations. The second reason is that there has not been wide-ranging tracking of gender- or sex-disaggregated participation rates.

> ***In Focus – Gender report cards***
>
> *Recognizing the absence of consistent and reliable gender-disaggregated data on participation in internet governance spaces, starting in 2011 theWomen's Rights Programme of the Association for Progressive Communications (APC) began compiling Gender Report Cards to monitor and assess the level of gender parity and inclusion at the UN Internet Governance Forum (IGF).[74] These Gender Report Cards have been instrumental in monitoring the level of gender parity and inclusion at IGF workshop sessions. Efforts by the IGF Dynamic Coalition on Gender made reporting on gender diversity in IGF workshops part of the official reporting process, which transformed this from a civil society initiative into a formal part of the Forum's work . In 2015, the IGF Secretariat published the first overall analysis of gender participation in the IGF, based on gender report cards.[75]*

[71] Fortinet, Exploring the Benefits of Gender Diversity in Cybersecurity", 4 October 2018, https://www.fortinet.com/blog/business-and-technology/exploring-benefits-gender-diversity-cybersecurity.html

[72] Krause, J. Krause, W & Bränfors, P., "Women's Participation in Peace Negotiations and the Durability of Peace", *International Interactions,* 44:6, pp. 985-1016.

[73] Jaqui True and Yolanda Riveros-Morales, "Towards inclusive peace: Analysing gender-sensitive peace agreements 2000-2016", *International Political Science Review,* 27 November 2017.

[74] The report cards and relevant background information can be found at https://www.genderit.org/feminist-talk/igf-gender-report-cards

[75] "Joao Pessoa, "Gender report cards: Analysis and results", November 2015, https://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/takingstock/726-gender-report-card/file

A useful starting point can be official meeting and participation records from relevant meetings or events. An overview of gender diversity and women's participation in United Nations processes on cyber security in the context of international security by the UN Institute for Disarmament Research (UNIDIR)[76] reveals strong and consistent gender imbalance:

- In the six UN GGEs that have been convened in the last 15 years, women have represented on average only 20.2 percent of participants.
- As recently as the fifth GGE, convened in 2016-2017, women represented only 20 percent of participants.
- The current and sixth GGE, being convened in 2020-2021, does have gender parity, which is credited to the UN Secretary-General's commitment to achieving gender parity "in all panels, boards, and expert groups established under his auspices in the field of disarmament" as contained in Action 37 of his 2018 Agenda for Disarmament.[77]
- At the first session of the UN Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security in September 2019, 32 percent of 414 participants were women and 68 percent were men; while only 24 percent of delegations were led by women.
- At the second session of the OEWG in February 2020, there were a total of 148 women (39%) and 233 men (61%). This includes non-member state delegations such as the Holy See, the European Union, and the International Telecommunication Agencies. At the second session, 34 of the 114 delegations included no women and 10 delegations had no men.[78]
- One hundred and nineteen statements, out of 280 total statements delivered during the second substantive OEWG session in February 2020, were delivered by women delegates.[79]

These numbers are consistent with what has been observed in other UN forums that cover matters of disarmament, non-proliferation, or arms control, which is where both of the UN cyber processes have their basis.[80] Interestingly, research shows that the gender gap is greatest in UN bodies on this issue area—the UNGA Third Committee (on social, humanitarian and cultural issues) has the highest proportion of women representatives attending, at 49 per cent in 2017, in contrast to the First Committee on disarmament which has the lowest.[81] This may speak to the perceived dichotomy between the issues covered by those committees, the "feminization" of different disciplines, and how people are encouraged to engage with one or the other onthe basis of their gender.[82]

Looking beyond the UN cyber security forums, the gap exists in other policy bodies. As one example, when INTERPOL countries were requested to provide participation statistics to Monitoring and Assessment missions on cybercrime, none were able to provide gender dis-aggregated statistics.

Recognizing the need to promote gender equality in its own work, the International Telecommunication Union adopted a resolution at its 2018 Plenipotentiary meeting committing member states and sector members (typically private sector entities from the ICT sector) to take a number of actions, including to encourage gender-balanced

[76] "Factsheet—Gender in Cyber Diplomacy", UN Institute for Disarmament Research, https://www.unidir.org/publication/fact-sheet-gender-cyber-diplomacy

[77] Antonio Guterres, *Securing our Common Future: An Agenda for Disarmament,* May 2018, https://www.un.org/disarmament/publications/more/securing-our-common-future/

[78] Analysis of participant data by the Gender Team of the UN Office for Disarmament Affairs. Reasons for noticeable increase in gender diverse participation are explained later in this report.

[79] Allison Pytlak, "A new 'Women In Cyber' fellowship has a big impact on the OEWG", *Cyber Peace & Security Monitor: Volume 01, Number 07*, 18 February 2020 http://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf

[80] Both the GGE and the OEWG were established by resolutions adopted by UN member states at the 2018 session of the UN General Assembly First Committee on Disarmament and International Security.

[81] Renata Hessmann Dalaqua, Kjølv Egeland, Torbjørn Graff Hugo, *Still Behind the Curve,* UNIDIR, p. 19, https://www.unidir.org/publication/still-behind-curve

[82] Ibid., p.33.

representation in delegations to ITU conferences, assemblies and other meetings, as well as in candidatures for leadership roles. It also resolved the ITU itself to compile and process statistical data from countries and draw up indicators that take into account gender equality issues and highlight trends in the sector, disaggregated by socio-economic factors, in particular sex and age and to take affirmative measures when necessary, in ITU as a whole, to ensure capacity building and the appointment of women to senior-level positions, including ITU elected positions.[83]

When looking at participation rates, it's important to look beyond numbers alone. Are women able to contribute in ways that are meaningful? What specific roles do they fill, what leadership and decision-making roles do they hold, and are their skills and inputs valued? The same UNIDIR report shows that in arms control, non-proliferation and disarmament forums, heads of delegations are mostly men and the proportion of women tends to decline as the importance of the position increases, while the proportion of men grows linearly as one moves "from regular diplomatic personnel to United Nations ambassadors, to foreign ministers and, lastly, to heads of State or Government."[84]

Moreover, numbers do not give a sense of the discrimination that women experience, or the social and cultural gender dynamics that persist in their working environments. In the course of preparing this report, all five women interviewed stressed the invisible gender discrimination they have encountered as a result of working in a heavily male-dominated field, or how that has set a tone and dynamics for the environment they work in.

"When you are in a room with many men, the social norms tend to be masculine. The socialization makes the structure," noted one interviewee. Another interviewee described a situation that occurred earlier in her career in the context of having an older male colleague who reported to her. She explained that people regularly assumed that she reported to him, as evidenced that he was invited to principal-level meetings in her place. Another interviewee said that sometimes when she attends meetings with her junior male colleague other people assume the male is the boss.

Three interviewees described how they have had to adapt their behaviour in various ways to better 'succeed' in male dominated spaces, such as through gender assertiveness training. "We have to claim our place," said one interviewee, explaining that she always deliberately raises her hand or national flag in a meeting to ask questions, deliver a response, or similar just to make the point that she is in the room and has a voice. She observed that women often feel that "we need to know things 110 percent before [we feel] are really an expert" whereas men hesitate less to give an opinion; an observation that was supported by another interviewee.

Barriers and Challenges

The reasons underpinning the gender gap in these aspects of cyber security are multiple, and often, context specific.

In many instances however, the gap goes back to unequal access and/or a lack of encouragement to engage in the cyber security field, in any capacity, as already described. As one interviewee highlighted, "In many regions the issue of access in many mainstream professions are systemic, and for digital related fields it can be compounded with the sheer lack of access to online resources."

This is rooted in the prevailing patriarchal and masculine structures on which most societies are based, in which women do not associate themselves with work in a security profession.[85] A complicating factor is that, as this report has already revealed, women are often the targets of online GBV and abuse, which reinforces a sense of being targeted and unwelcome. Yet, if more women were to work within cyber security and in leadership roles, these perceptions could be reversed and solutions and structures that work for women developed.

[83] ITU Plenipotentiary Resolution 70, "Mainstreaming a gender perspective in ITU and promotion of gender equality and the empowerment of women through telecommunications/information and communication technologies", 2018, https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/Resolutions/RESOLUTION%2070%20(REV.%20DUBAI,%202018).pdf. See Annex I for more details on the commitments by states included in ITU Resolution 70

[84] Ibid., p.6.

[85] Donna Peacock and Alastair Irons, "Gender Inequalities in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression," *International Journal of Gender, Science and Technology,* Vol.9, No.1, 2018, p. 26.

The women interviewed all indicated that they personally did not face many formal obstacles or barriers to working in their field and receiving relevant training and education. Their combined backgrounds include legal, political science, and molecular biology degrees alongside experience in compliance, global trade, and knowledge of coding and computer science. Yet most described situations where either they, or another female colleague, were not taken seriously despite relevant expertise or being in a leadership role. While it was hard for them to specify that this was on account of their being a woman, they felt that it did relate to assumptions and gender norms. One described that she has sometimes deliberately asked a male colleague to reiterate her points in a negotiation or meeting room, after feeling that she was not being heard.

Two interviewees also highlighted that negative gender dynamics can become something that cause women to leave the profession. This points to another important consideration: how women's participation in other professions is being impacted by disinformation campaigns and online GBV, as described in Section II.. "All it takes is a fake story and smear campaign fabricated by a journalist to ruin years of hard work," says Joyce Banda, the former president of Malawi in a new report on women and media. "This makes women nervous to run for office, because not only can it harm her political aspirations, but also bring shame to her family."[86] Other women surveyed for the same report expressed similar concerns; most reported being "extremely concerned about the pervasiveness of gender-based abuse (ranging from insults to death threats) in the digital space as a real barrier for women who want to engage in politics."[87]

Gender norms in relation to parenting and family life can also be a factor, although this is probably true of most professions and not unique to cyber security. One interview said that this may be more of a barrier in diplomacy than "cyber", in which all of the women she knows in her Ministry are divorced and single, and those who are not have partners willing to follow them as they move to new postings. She further described stigmatization against women with families, with single people being perceived as being able to work more, and therefore able to become more successful.

How to Support Women's Participation in Cybersecurity Diplomacy

The key to involving more women in cyber security in ways that drive change and influence policy outcomes towards greater peace and stability is to look beyond "adding women" in a tokenistic way and to make it meaningful. This requires addressing the underlying gender norms that act as barriers and disincentives, as well as investing in knowledge-sharing and network-building. As one interviewee stated, "The big mistake that we make often is to think that the numbers are the only thing that matters." Another added, "I think tackling [access] at the granular level to resolve the access issue will build a cadre of women who are more knowledgeable and can take part in more meaningful discussion."

At the national level, resources allocated to address gender equality are consistently low, sometimes less than one percent of national budgets.[88] But more positively, there are multiple initiatives underway within international bodies, supplemented by guidelines, agreements, and crucially, resourcing.

In the context of the UN's OEWG on cyber security, for example, five governments have initiated a fellowship program for around 25 women working within cyber security in their national governments, from the regions of Africa, Asia, Latin America and the Caribbean, and the Pacific. The program includes knowledge-building opportunities on thematic topics as well as negotiating skills, after which they participate in the OEWG substantive session with their national delegation. Participation of the fellows went a long way toward closing the gender gap during the OEWG's second session in February 2020 and also increased the level of technical expertise in the room.

The momentum within these bodies is possibly buoyed along by a broader swell of support for inclusion of gender perspectives within disarmament and arms control. Many treaties or instruments are being re-interpreted in "gender-sensitive ways" such as through a new emphasis on improving gender- and sex-disaggregated information, gender-based violence preventing in relation to armed violence, and increasing gender diversity. During the 2019 UNGA First Committee session, an unprecedented 28 per cent of all adopted 2019 resolutions include gender aspects.[89] There could be lessons and examples here for the cyber security community.

[86] De Meca, p. 11.

[87] Ibid., 30.

[88] OAS (2017). Third Hemispheric Report on the Implementation of the Belém do Pará Convention.

[89] Katrin Geyer, "Gender", *First Committee Monitor,* November, 2019, http://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/FCM19/FCM-2019-No6.pdf

The Organization of American States (OAS) has started implementing initiatives to raise awareness about the importance of cyber security policies that are gender sensitive. It encourages member states to nominate a more gender-balanced delegation to its activities and provide incentives to facilitate women's participation whenever possible. At the same time, it also works to encourage its member states to include provisions to promote equal access to science and technology education and professions for women in order.[90] Many OAS states run a "CyberWomen Challenge" in partnership with tech company TrendMicro and partnership with countries like Canada and the United Kingdom, which is focused on developing cyber security skills in women in the ICT industry throughout Latin America to help bridge the diversity and skills gap. In 2018, more than 650 women participated in the trainings.[91] It is part of a collaboration agreement between organizations to promote initiatives that contribute to a more secure and inclusive insurance in the field of cyber security.[92] Additionally, OAS states are bound by the Inter-American Program on Women's Human Rights and Gender Equity and Equality (IAP), adopted in 2000, which one interviewee pointed to as acting as a baseline for improving participation in cyber security.[93]

There are a growing number of tools and guidelines to draw on, such as the frameworks and agendas outlined in Annex I. Additional resources include: the Government of Canada's *Playbook for Gender Equality in the Digital Age;*[94] *Securing our Common Future: An Agenda for Disarmament;*[95] and the UN's Guidelines for Gender Inclusive Language.[96]

Finally, most interviewees spoke to the importance of mentorship and support networks in their own experience.

In any initiative, it will be important to avoid gender essentialisms, and understand that women's participation is rooted in a broader need for diversity. It is important that participation not be co-opted to support other agendas or the further militarization of cyberspace, and that efforts to build capacity are not, even unintentionally, presented in ways that can be viewed as patronizing or undermining of the experiences and knowledges that any woman already brings to the table. The problem of gender diversity is not a "cyber" problem, but a broader societal one which manifests as gender inequality in cyber security spaces. To address this, broader changes in the overall culture is vital.

[90] Email correspondence with Government of Canada, Anti-Crime Capacity Building Program, February 2020.

[91] Ibid.

[92] Ibid.

[93] Ibid.

[94] Digital Inclusion Lab, *Playbook for Gender Equality in the Digital Age,* Government of Canada, 2018, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/playbook-manuel_instructions.aspx?lang=eng

[95] Antonio Guterres, Securing our Common Future: An Agenda for Disarmament, May 2018, thttps://www.un.org/disarmament/publications/more/securing-our-common-future/

[96] United Nations, Guidelines for Gender Inclusive Language, https://www.un.org/en/gender-inclusive-language/guidelines.shtml

Section V: Recommendations

Based on the information presented in this report, the researchers put forward the following recommendations:

Normative and structural recommendations:

- States should integrate their obligations to protect, promote and uphold women's human rights as part of their cyber security strategies;
- States should utilize WPS National Action Plans or opportunities provided by other frameworks to advance women's participation within international cyber security, alongside their protection; and
- States should conduct a gender audit of national or regional cyber security policies to identify areas for improvement.

Recommendations relating to impact and cyber security operations:

- States and companies should adopt data minimization as a key principle of data protection, to minimize the risk experienced by women, when data breaches (inevitably) occur;
- All actors involved in cyber incident response (governmental, private sector, and civil society) should be equipped to recognize potential gendered impacts of an operation and respond appropriately, as well as conduct further research into those impacts to improve global understanding and knowledge;
- All actors should call out and condemn online gender-based violence, whether in the context of disinformation activities or otherwise, and draw on and support research done by women, especially minority women, who are best placed to document online GBV; and
- Provide media or digital security training to reduce the personal and professional impacts of online disinformation campaigns, and other forms of online GBV.

Recommendations relating to participation:

- All actors should maintain sex- or gender-disaggregated participation records for all cyber security related work (diplomacy, capacity building, incident response, etc.);
- All actors should build intentionally supportive and inclusive spaces and work cultures in the cyber security policy/diplomacy field that will encourage and act as incentive for greater diversity in participation; and
- States and private companies should allocate resources for further research and knowledge-sharing/capacity-building on the gender dimensions of international cyber security, as well as for programs and initiatives that actively seek to reduce gender inequality.

Recommendations related to the UN's OEWG on ICTs:

- States should specifically acknowledge their obligations to uphold women's rights online, in the context of recognizing the applicability of international human rights law, because of the differential threats they experience due to cyber incidents;
- States should recognize that, as part of the threat landscape, international cyber operations can have gender-differentiated impacts;
- States should encourage further analysis or promotion of the eleven voluntary norms include a gender dimension;
- States should recognize that capacity-building must be gender-sensitive and gender diverse;
- States should commit to gender diversity in delegations to meetings and inclusive approaches to developing positions, statements, or other contributions.

Annex I: Normative Frameworks Relevant to Gender and Cyber Security

The Women, Peace and Security (WPS) Agenda

- The WPS Agenda was established by UN Security Council Resolution (UNSCR) 1325[97] in 2000 and was considered a milestone achievement that emerged from years of advocacy from women-led civil society.[98] It was the first time that the Security Council recognized and addressed the disproportionate impact of armed conflict on women—while also stressing the importance of women's equal and full participation as active agents in peace and security. In doing so it moved beyond framing women solely as victims or a vulnerable group.
- The WPS Agenda is best understood as a set of approaches jointly rooted in the principle that 'effective incorporation of gender perspectives and women's rights can have a meaningful and positive impact on the lives of women, men, girls, and boys on the ground.' [99]
- The WPS Agenda is generally understood to have four pillars: participation, prevention protection, and relief and recovery. The first three are referred to as the 'three Ps'.
- Nine 'follow-up' WPS resolutions have been adopted by the Security Council, which variously address sexual violence in conflict, the role of women in peace processes, resourcing, among other things.[100]
- National Action Plans (NAPs) are a primary vehicle for the implementation and localization of UNSCR 1325 commitments.[101] They are meant to outline a member state's domestic and foreign policy actions undertaken to meet the WPS objectives and are envisioned as a critical way to ensure compliance with the provisions of the resolutions. Yet less than half of UN member states have established a NAP, and implementation those that do exist is uneven, often because of a lack of designated resources.
- There has been insufficient examination of how the WPS Agenda or NAPS could be integrated or leveraged within policy discussions on international cyber security. Given the legally binding nature of UNSCR resolutions on all UN member states, it could serve as a foundation for efforts to close the gender digital divide and prevent better protections online.

Beijing Declaration and Platform for Action[102]

- The Beijing Declaration and Platform for Action was agreed by states during the Fourth World Conference on Women in 1995. Considered by many to be a groundbreaking and historic achievement to advance women's rights and participation, it was negotiated with significant input from civil society and still enjoys wide-ranging support.
- The Platform for Action is organized across 12 areas of concern and is balanced between calls to enhance women's participation and recognizing the unique needs and experiences of women.
- It is highly critical of excessive military spending and armament, noting that "that those affected most negatively by conflict and excessive military spending are people living in poverty, who are deprived because of the lack of investment in basic services." Strategic Objective E.2 outlines multiple actions to reduce excessive military expenditures and control the availability of armaments.

[97] United Nations Security Council, *Women and peace and security,* S/RES/1325, 31 October 2000, http://unscr.com/en/resolutions/1325

[98] PeaceWomen, Background, https://www.peacewomen.org/why-WPS/solutions/background

[99] PeaceWomen, "UN Security Council Resolution 1325", https://www.peacewomen.org/SCR-1325

[100] Highlights of each resolution and links to the resolutions can be found at https://www.peacewomen.org/security-council/WPS-in-SC-Council

[101] The PeaceWomen program of the Women's International League for Peace and Freedom tracks the development and implementation of WPS National Action Plans. See https://www.peacewomen.org/who-implements

[102] *Beijing Declaration and Platform for Action,* 15 September 1995, https://www.un.org/womenwatch/daw/beijing/pdf/BDPfA%20E.pdf

- Section J of the Beijing Platform[103] addresses women and the media, including new communication technologies. Specifically, it recognizes that “During the past decade, advances in information technology have facilitated a global communications network that transcends national boundaries and has an impact on public policy, private attitudes and behaviour, especially of children and young adults. Everywhere the potential exists for the media to make a far greater contribution to the advancement of women.” It also recognizes that the continued projection of negative, violent, and degrading images of women in media communications, including electronic media negatively affect women and their participation in society while also reinforcing their traditional roles.
- Section J calls for women to be involved in decision-making regarding the development of the new technologies in order to participate fully in their growth and impact, and includes a strategic objective to this end (Strategic objective J.1.).

Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)[104]

- CEDAW was adopted by the United Nations General Assembly in 1971 following three decades of work by the United Nations Commission on the Status of Women and is sometimes described as a “bill of rights for women”. As of 2020, there are 189 states parties.
- The preamble acknowledges that "extensive discrimination against women continues to exist" and emphasizes that such discrimination "violates the principles of equality of rights and respect for human dignity". The remainder of the Convention outlines an agenda for equality across three thematic areas.
- Implementation of states parties obligations is monitored by the CEDAW Committee. States parties are obligated to submit a report every four years, which are discussed during an annual session. The CEDAW Committee can also publish general recommendations, which serve as authoritative interpretations articles of the Convention. In recent years general recommendations have taken into account ICTs.
- The CEDAW Committee’s General Recommendation No, 35 on “ gender-based violence against women” [105] includes in its updated understanding of gender-based violence against women the “redefinition through technology-mediated environments, such as contemporary forms of violence occurring in the Internet and digital space”.
- The CEDAW Committee’s General recommendation No. 36 “on the right of girls and women to education” [106] recognizes the underrepresentation of women “in the use of Information Communication Technology (ICT) skills” and further calls on schools to address the barriers that impede access to information and employment opportunities in relevant industries.

The 2030 Agenda[107]

- The 2030 Agenda is a broad and interdependent approach to sustainable socio-economic development that builds on earlier multilateral processes and agreements.
- The 17 Sustainable Development Goals (SDGs) are the primary mechanisms of the 2030 Agenda, adopted by the UN General Assembly in resolution A/RES/70/1 ‘Transforming our world: the 2030 Agenda for Sustainable Development’ (UNGA, 2015) amid strong political support and commitment.
- SDG 5 seeks to “Achieve gender equality and empower all women and girls”. Like all of the Goals, SDG 5 has a set of specific targets and corresponding indicators, some of which are especially relevant:

  » 5.1: End all forms of discrimination against all women and girls everywhere.
  » 5.2: Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation.

[103] Strategic Objective J.1, https://www.un.org/womenwatch/daw/beijing/platform/media.htm

[104] To access an overview of the Convention, as well as its text, status of implementation, number of states parties and other updates visit https://www.un.org/womenwatch/daw/cedaw/

[105] Committee on the Elimination of Discrimination Against Women, *General recommendation No. 35 on gender-based violence against women, updating general recommendation* No. 19, 14 July 2017, https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf

[106] Ibid, paragraph 24.

[107] Sustainable Development Goals Knowledge Platform, https://sustainabledevelopment.un.org/

- » 5.5: Ensure women's full and effective participation and equal opportunities for leadership at all levels of decision-making in political, economic and public life.
- » 5.B: Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women.[108]

Human Rights Council Resolution 38/5 "Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts" [109]

In 2018, the UN Human Rights Council adopted Canada-led resolution by consensus with over 50 co-sponsors from every region, establishing that online GBV is a human rights violation in need of urgent attention. The resolution indicates not just a growing recognition of the risk of violence faced by all women and girls, but also an understanding that there are those who face violence on account of gender and also multiple and intersecting forms of discrimination, and recognises that a multi-pronged approach working with all relevant parties is required. Importantly, the resolution recommends that human rights frameworks guide responses to online GBV, so that they do not further restrict women's human rights, for example, by limiting their use of encryption, or by censoring their own expression.

World Summit on the Information Society

- The UN World Summit on the Information Society (WSIS) process and its outcome documents are considered cornerstones of international norms and discourse on internet policy and governance. The two-stage WSIS took place in 2003 (the Geneva phase) and 2005 (the Tunis phase).
- The Geneva Declaration of Principles (the outcome of the first phase), which enjoyed the support of UN member states, and all relevant stakeholders affirmed the importance of ICTs for women's empowerment and that women must participate on equal footing in all spheres of decision making in the information society. Paragraph 12 of the Geneva Declaration reads "We affirm that development of ICTs provides enormous opportunities for women, who should be an integral part of, and key actors, in the Information Society. We are committed to ensuring that the Information Society enables women's empowerment and their full participation on the basis on equality in all spheres of society and in all decision-making processes. To this end, we should mainstream a gender equality perspective and use ICTs as a tool to that end." [110]
- The Tunis Agenda for the Information Society (the outcome of the second phase) reaffirms the commitment of all stakeholders to encourage women's participation in decision-making processes, by calling for "implementing effective training and education, particularly in ICT science and technology, that motivates and promotes participation and active involvement of girls and women in the decision-making process of building the Information Society.[111] Further, it recommits all stakeholders to "building ICT capacity for all and confidence in the use of ICTs by all – including youth, older persons, women, indigenous peoples, people with disabilities, and remote and rural communities – through the improvement and delivery of relevant education and training programmes and systems including lifelong and distance learning."
- In 2015 when the World Summit on the Information Society went through a 10-year review, the UN General Assembly adopted resolution 70/125 "Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society".[112] Resolution 70/125 reaffirmed the importance of promoting and maintaining gender equality and women's empowerment and guaranteeing the inclusion of women in the emerging global ICT society. Specifically, it called for "immediate measures to achieve gender equality in Internet users by 2020, especially by significantly enhancing women's and girls' education and participation in information and communications technologies, as users, content creators, employees, entrepreneurs, innovators and leaders. We reaffirm our commitment to ensure women's full participation in decision-making processes related to information and communications technologies."

[108] "Sustainable Development Goal 5: Targets and Indicators", https://sustainabledevelopment.un.org/SDG5

[109] Human Rights Council Resolution 38/5, *Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts,* https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/5

[110] See https://www.itu.int/net/wsis/docs/geneva/official/dop.html

[111] See https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

[112] UN General Assembly, *Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society,* A/RES/70/125, 1 February 2016, https://undocs.org/en/A/RES/70/125

ITU Resolution 70 (2018)

At its 2018 Plenipotentiary meeting, the member states of the ITU adopted Resolution 70, “Mainstreaming a gender perspective in ITU and promotion of gender equality and the empowerment of women through telecommunications/information and communication technologies” The resolution recognized that:

- equal access to ICTs for women and men and equal participation of both women and men at all levels and in all fields, especially in policy-and decision-making, are beneficial to society as a whole, particularly in the context of the information and knowledge society;
- bridging the gender digital divide requires fostering digital skills, education and mentorship for women and girls, so as to advance their participation and leadership in the creation, development and deployment of telecommunications/ICTs;
- there is a need to continue fostering the participation of women and girls in the telecommunication/ICT domain at an early age and to provide input for further policy developments in the required areas, so as to ensure that the information and knowledge society contributes to their empowerment;

The resolution included a number of commitments of steps to mainstream a gender perspective and advance gender equality within the ITU itself and committed member states to a number of actions, including:

- to review and revise, as appropriate, their respective policies and practices to ensure that recruitment, employment, training and advancement of women and men in the ICT sector are undertaken on a fair and equitable basis;
- to facilitate the capacity building and employment of women and men equally in the telecommunication/ICT field, including at senior levels of responsibility in telecommunication/ICT administrations, government and regulatory bodies and intergovernmental organizations and in the private sector;
- to review their policies and strategies related to the information society so as to ensure the inclusion of a gender perspective in all activities and the fostering of gender balance to secure equal opportunities through the use and appropriation of telecommunications/ICTs;
- to strengthen educational policies and study plans in science and technology and to promote and increase the interest of, and opportunities for, women and girls in STEM and telecommunication/ICT careers, including women and girls in rural and remote areas, during elementary, secondary and higher education and lifelong education;
- to attract more women and girls to study for and to pursue STEM careers, and acknowledge the achievements of leading women in these fields, particularly in innovation;
- to encourage gender-balanced representation in delegations to ITU conferences, assemblies and other meetings, as well as in candidatures for leadership roles;

Feminist Principles of the Internet[113]

The Feminist Principles of the Internet are a series of statements that offer a gender and sexual rights lens on critical internet-related rights. They were drafted in April 2014 at a meeting in Malaysia, which brought together 50 activists and advocates working in sexual rights, women’s rights, violence against women, and internet rights. After a series of local and global follow-up workshops and events a revised set of Principles was released in August 2016. Currently there are 17 Principles in total, organized in five clusters: Access, Movements, Economy, Expression, and Embodiment. Within these clusters, relevant issues like privacy, surveillance, anonymity, and violence are covered. Together, they aim to provide a framework for women's movements to articulate and explore issues related to technology.

[113] The Principles are available at https://feministinternet.org/en

Gender matters in international cyber security. It shapes and influences our online behaviour; determines access and power; and is a factor in vulnerability. As a result, malicious cyber operations can differently impact people based on their gender identity or expression.

Yet much of what is known about gender and cyber security comes from studies of online gender-based violence and gender inequality within the information and communications technology sector. Less is known about how malicious international cyber operations between states affect people differently on the basis of gender or other characteristics that may put them in positions of vulnerability.

This report helps to fill that gap. It identifies multiple gender-differentiated impacts of cyber operations with an international dimension, such as internet shutdowns, data breaches, and disinformation campaigns, and builds the case that these differentiated impacts need to be better accounted for and understood by policy-making and technical communities. The report explores the digital gender gap that exists within cyber diplomacy and policy professions. In order to improve gender diversity and women's meaningful participation, the report advocates for solutions that also address problematic underlying gender norms and stereotypes.

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Association for Progressive Communications

PO Box 29755, Melville 2109
South Africa

T +27 11 726 1692
E info@apc.org

WOMEN'S INTERNATIONAL LEAGUE FOR
PEACE & FREEDOM

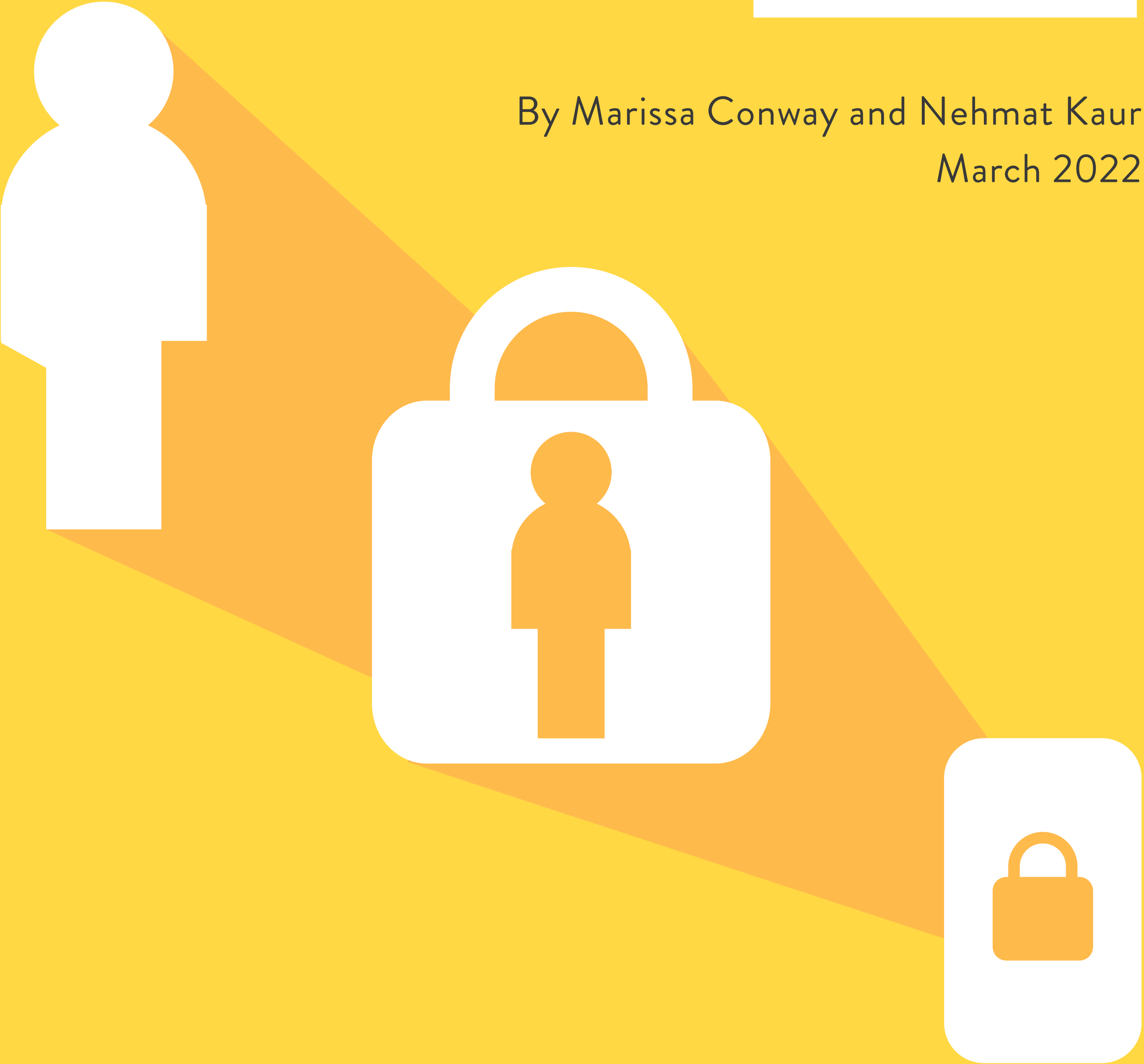
Women's International League for Peace and Freedom

Rue de Varembé 1, Case Postale 28
1211 Geneva 20, Switzerland

T +41 (0)22 919 70 80
E info@wilpf.org

The Intersectionality and Cybersecurity Toolkit

By Marissa Conway and Nehmat Kaur
March 2022



CFFP THE CENTRE FOR FEMINIST FOREIGN POLICY

Centre for Feminist Foreign Policy UK

Company registration no. 11858782

Regency Court 62-66 Deansgate Manchester
M3 2EN United Kingdom

The Intersectionality and Cybersecurity Toolkit
March 2022

Authors: Marissa Conway, Nehmat Kaur

Editor: Katie Washington

Design: Brand Temple

This publication was made possible by a grant from the Foreign, Commonwealth and Development Office's Conflict, Stability and Security Fund. The statements made and views expressed are solely the responsibility of the authors.

Copies of the report can be downloaded from the CFFP website at:
www.centreforfeministforeignpolicy.org/reports

Please contact CFFP for permission to reproduce any part of the content of this report.

Email: hello@centreforffp.org

Contents

SECTION 1:KEY CONCEPTS

SECTION 2:TAKING ACTION

ANNEXE

Introduction

In 2021 the UK Government published its Integrated Review, detailing its foreign policy goals and objectives for the coming years (*Cabinet Office, 2021*). It outlined the UK Government's clear interest in acting as a 'force for good' across all aspects of foreign policy, with commitments to defend universal human rights, promote gender equality, and promote effective and transparent governance. The review also highlights the UK Government's priority in becoming a responsible and leading cyberpower, which is echoed in the *2022 National Cyber Strategy*.

This toolkit looks at how these two goals overlap: as the UK Government continues to invest in cyber, how can cybersecurity prioritise human rights, equality, and transparency?

To explore this question, this toolkit offers an intersectional lens as an ideal method to understand and encourage the nexus of these interests. In doing so, we provide a new vision of who cybersecurity is for: instead of the needs of the state, the focus falls to the needs of people.

Intersectionality refers to the way that social categories, like gender, race, and class, overlap to shape how a person experiences discrimination *(Dunkley, Conway and Messmer, 2021).* The term ‘intersectionality’ was originally coined by Kimberle Crenshaw (1991) to describe the compounded discrimination faced by Black women in the legal system due to both their gender and race.

This toolkit will connect the local with the global and explore how individuals experience cybersecurity issues, making the case that such an approach contributes to a prosperous digital economy and resilient state. State security, too, is automatically strengthened when the needs and safety concerns of everyday people at home and abroad are kept at the core of policy decisions and implementation.

The UK’s investment in cyberinfrastructure comes at a time when our lives are increasingly taking place in the digital sphere. During the first year of the pandemic, Ofcom reported that internet access in UK homes went up from 89% in 2019 to 94% *(Ofcom, 2021).* In an increasing number of countries, accessing the online world is not a novelty but a necessity in participating fully in today’s economy and society. Different groups of people have different digital needs. For example, for immigrants who are reliant on accessing the online world to communicate with their families or to receive money, participating in the online world is requisite. The digital world is for everyone, and cybersecurity must be designed to ensure this.

About this Toolkit

This toolkit aims to equip its readers with how to use an intersectional lens to explore and rethink cybersecurity. Specifically, it seeks to:

1. Introduce intersectionality
2. Reconceptualise cybersecurity's purpose as protecting people
3. Provide pathways for actioning an intersectional lens in cybersecurity
4. Share complimentary resources for further learning

We align the focus of this toolkit with the fourth pillar of the National Cyber Security Strategy, which cites that an **"open, peaceful and secure cyberspace remains critical to our collective security and prosperity"** *(Cabinet Office, 2022).* This pillar speaks to the holistic ecosystem of cyberspace and orientates its purpose toward peace.

By invoking an intersectional lens to unpack this pillar, we can:

- ✓ **Understand how marginalised and protected communities are impacted differentially and specifically by cyber threats**
- ✓ **View cybersecurity issues from multiple perspectives**
- ✓ **Identify a wider range of available solutions to cybersecurity challenges**

The first half of this toolkit will explore the concept of intersectionality and how it can be used as a lens to reconceptualise the purpose of cybersecurity. The second half of this toolkit will examine what it means to have an 'open, peaceful and secure cyberspace'. We have also built an Intersectionality and Cybersecurity Resource Dashboard with further resources and recommended readings for those interested in continued learning.

Who can use this toolkit?

This toolkit is first and foremost designed for civil servants and policymakers at all levels working on cybersecurity issues in the UK Government. It can be used either in tandem with existing gender-sensitive resources and methods or as a stand-alone introduction to inclusivity and equity. The UK Government has the power and a unique opportunity to set the standards for how our online world evolves and develops. As such, this toolkit encourages its readers to engage more deeply in exploring power dynamics and the responsibility to craft an open, secure, and peaceful cyberspace. That said, we believe that anyone interested in the subject matter will find its contents of use.

Methodology

We are grateful to the cohort of cybersecurity and intersectionality experts who contributed to the production of this toolkit. A combination of roundtable discussions, 1:1 conversations, and peer review processes were held in shaping this toolkit's formation. We conducted further desk research to identify existing resources compiled in the Intersectionality and Cybersecurity Resource Dashboard.

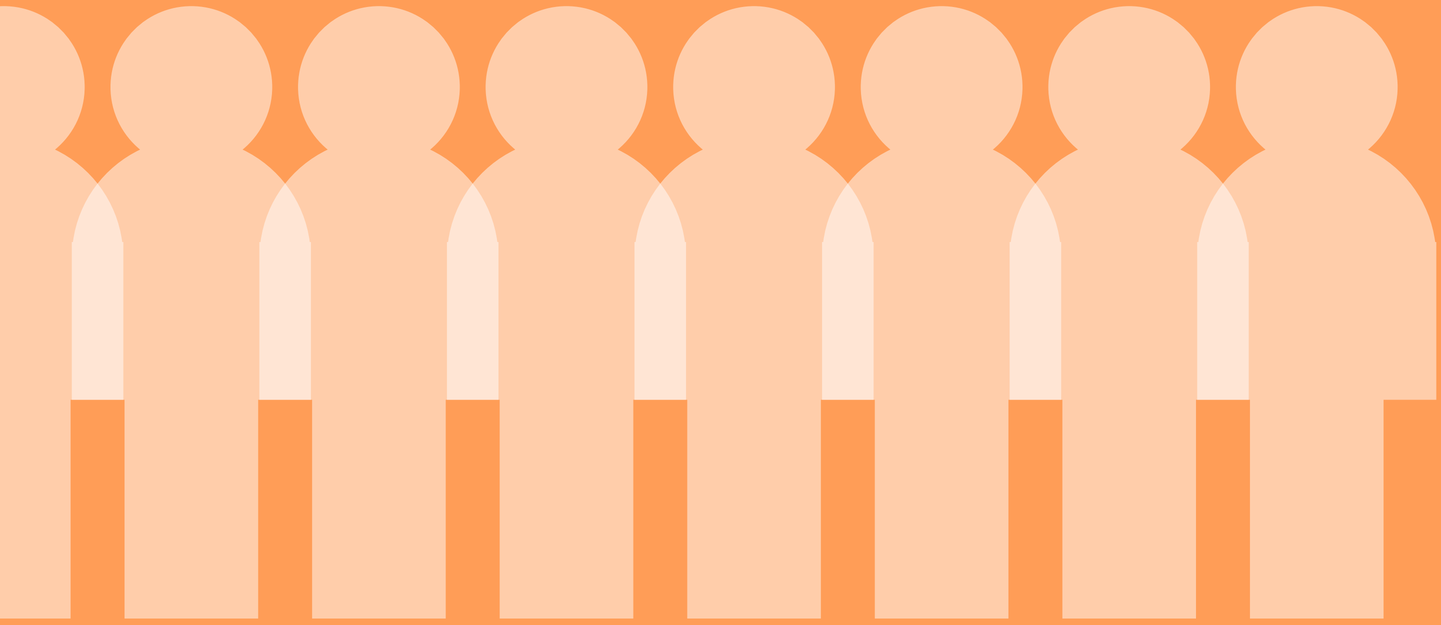
Limitations and further research

This toolkit is an ambitious exploration of intersectionality and cybersecurity, and we recognise that there is only so much content that can be covered in one publication. It has been designed as a first step in encouraging continued conversations on intersectionality as the UK Government builds its cyberinfrastructure.

The experts we consulted with represented a range of age, gender, race, ethnicity, disability, and sexual orientation, among other social categories, however most were from High-Income Countries (HICs). Further research that incorporates an even broader range of perspectives, especially from Low- and Middle-Income Countries (LMICs), can only benefit this conversation.

We hope that this toolkit will inspire different ways of thinking about cybersecurity and emphasise the usefulness of incorporating an intersectional lens across cybersecurity and all foreign policy.

SECTION 1: KEY CONCEPTS



An Introduction to Intersectionality

"An intersectional approach allows us to see who falls through the cracks and how combined identities means some people fall further – and thus are harder to see – than others." *Seyi Akiwowo, Glitch UK Founder and Executive Director*

The term 'intersectionality' was originally coined by Kimberle Crenshaw *(1991)* to describe the compounded discrimination faced by Black women in the legal system due to both their gender and race. The term, with roots in critical race theory and feminist theory, has evolved and expanded and today is used to describe how the discrimination and marginalisation someone experiences isn't solely isolated to a single social category, like gender. Instead, a person's different social categories, like gender, class, race, ethnicity, language, age, ability, citizenship status, religion, among others, all interact to shape how they have access to power or are prevented from accessing power *(Carastathis, 2014).*

Intersectionality also understands social categories and their relationship to power and vulnerability relative to time and space *(Carastathis, 2014).* For example, certain groups, such as journalists, political dissenters, or whistle-blowers, have concerns about secure and safe internet access and usage. However, in an internet shutdown, every person affected has increased vulnerability due to the increased difficulty accessing information or urgent services in real-time.

'Marginalisation' refers to the processes or conditions that prevent people and communities from accessing social, economic, political, or symbolic power. Structural discrimination due to a person's social categories, such as gender, race, or class, are the root causes of marginalisation *(Mannon Daniels, 2022).*

Despite increasing efforts to address inequality within and through foreign policy initiatives, this toolkit recognises that systemic oppression due to a person's social categories is still too commonplace. Using an intersectional lens can reveal 'hidden' inequalities and paint a more comprehensive picture of how and why people are experiencing oppression. If we take this lens to cybersecurity, intersectionality can shed light on different perspectives, experiences, and power dynamics by asking questions like:

- **Whose views are reflected in cybersecurity policy, and whose views are left out?**
- **Who will be impacted, positively or negatively, by cybersecurity policy?**
- **How are vulnerabilities exacerbated or remedied by cybersecurity policy?**

Asking such questions means an open, peaceful, and secure cyberspace becomes more possible.

Questions for reflection:

- How does my identity shape my access to power?
- How does my access to power influence how I do my work?
- What blind spots might I have because of my access to power?

Gender Equality vs Intersectionality: What's the Difference?

Intersectionality and gender equality are related concepts but have important distinctions.

Gender is a power hierarchy typically expressed through masculine or feminine coded characteristics. Gender exists on a spectrum with various gender identities, yet the term is often conflated with 'woman' or understood as a binary of man or woman *(Dunkely, Conway, and Messmer, 2021)*. Gender equality refers to the ambition that a person's quality of life and access to opportunities isn't dependent on their gender *(UN Women, 2022)*. An increasing number of states and multilateral institutions have focused on gender equality as an objective and implemented mechanisms like gender mainstreaming or gender-responsive budgeting.

Intersectionality speaks to how overlapping identities produce oppression, of which gender is one. An intersectional analysis goes beyond the scope of gender equality initiatives as it draws attention to the systemic and hierarchical nature of oppression across multiple social categories. Despite the distinctions between the two, gender equality and intersectionality are united in their quest to set new equity norms.

Balancing Short-Term and Long-Term Goals

To achieve this new norm, the path forward must balance short-term and long-term goals.

Short-term goals focus on inclusion in existing systems, such as greater diversity in representation. These aspects are necessary to ensure that any policy creation process includes diverse voices and perspectives, both within the government and externally with stakeholders.

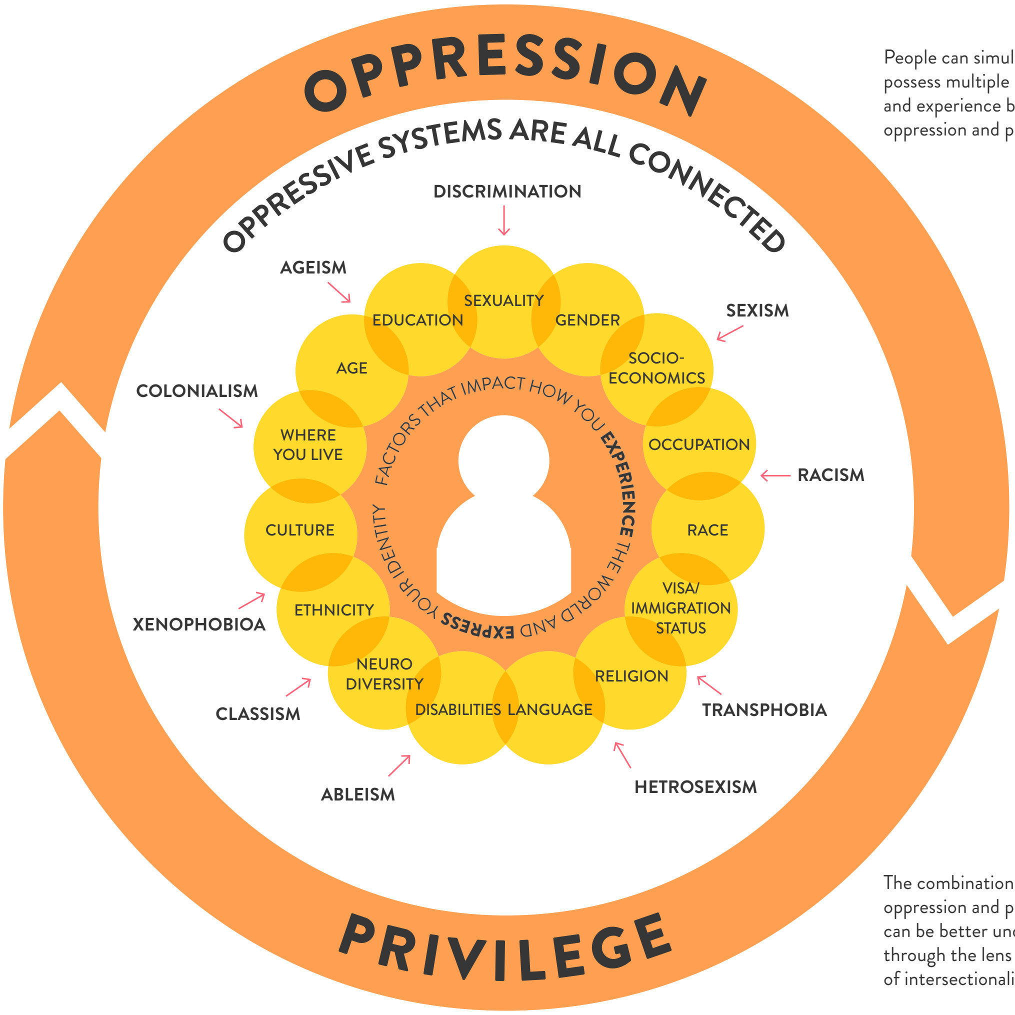
Long-term goals focus on addressing the root causes of inequality at a systemic level with an eye to institutional reform and culture change.

Some states are beginning to engage with the concept of intersectionality, predominately through Feminist Foreign Policy frameworks. In most cases, this type of engagement focuses solely on short-term goals and inclusion in existing systems, with little to no thought about systems change. However, without an explicit aim of implementing systems change, the symptoms of inequality will continue to perpetuate, and no real progress toward equality will be made.

It is important to note, however, that intersectionality isn't an end goal, but a process in and of itself. It is not a state to be achieved, but an action to be continually implemented that has associated norms and aims.

Questions for reflection:

- What is the balance between short-term and long-term equity and equality goals in my work?
- What steps can I take to ensure an even balance between the two?



People can simultaneously possess multiple identities and experience both oppression and privilege

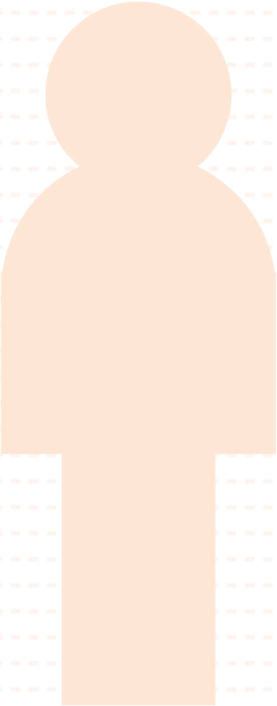
The combination of oppression and privilege can be better understood through the lens of intersectionality

This image has been adapted from the YSCA Australia's toolkit *"Y Advocacy? An Intersectional Feminist Toolkit."* Image description: An oppression/privilege wheel demonstrating how oppressive systems are all interconnected. The first layer of the when includes discrimination, sexism, racism, transphobia, heterosexism, ableism, classism, xenophobia, colonialism, and ageism. The next layer includes sexuality, gender, socioeconomics, occupation, race, visa/immigration stats, religion, language, disabilities, neurodiversity, ethnicity, culture, where you live, age, and education. The innermost layer says 'factors that impact how you experience the world and express your identity'.

Unpacking the Idea of 'Security'

This toolkit uses human security in outlining a definition of 'security'.

According to the CRISE Network at the University of Oxford, the purpose of human security is to "safeguard the vital core of all human lives from critical pervasive threats, in a way that is consistent with long-term human fulfillment" *(Alkire, 2003).* It aims to protect people from events beyond their control and centres people, not states, as subject.



Safety means more than physical protection from conflict or war. Human security looks at what makes people, not states, safe. Threats to safety include unstable economies, human rights violations, social and political discrimination, unaffordable housing, food insecurity, and unaffordable healthcare. All of these issues fall outside the sole domain of military force, where the responsibility for security has traditionally been thought to lie, but robust national security means taking these aspects seriously *(Tadjbakhsh, 2005).*

Security is subjective and personal and what makes someone feel safe differs from person to person *(Holistic Security, 2022a).* Here the necessity of an intersectional lens becomes clear. Human security disrupts traditional and mainstream ideas about security as state-focused, but an intersectional lens is necessary to further point to how modern social, political, and economic systems often function to prevent marginalised people from feeling safe and secure and how policy has the power to exacerbate or reconcile this.

Looking at Cybersecurity Differently

According to the *National Security Cyber Centre (2022)*, cybersecurity is defined as how people and organisations reduce the risk of a cyberattack. Cybersecurity aims to protect hardware, software, and digital services from theft or damage.

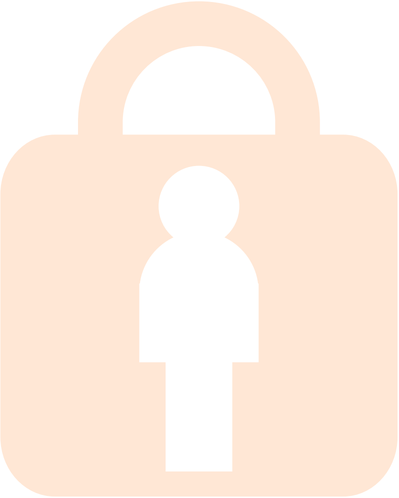
This toolkit offers a new definition of cybersecurity:

The purpose of cybersecurity is to make cyberspace safe for all. People have a right to safely access and participate in the online world free from persecution. This includes protection from online violence, cyberattacks, and privacy infringements. When this right has been violated, clear and victim-supportive pathways to seek justice are in place.

This definition dramatically expands the scope of cybersecurity, yet still sits comfortably alongside the UK Government's intentions with cyberinfrastructure. In Pillar 2 of the *UK's National Cybersecurity Strategy (2022)*, the reduction of cyber risks is prioritised, in part, so that "citizens are more secure online and confident that their data is protected." Pillar 4 of the strategy highlights a commitment to address global governance challenges in cyberspace in keeping with its stated human rights and democratic values. These ambitions can be read harmoniously alongside this toolkit's definition of cybersecurity and the objectives of creating and maintaining an open, secure, and peaceful cyberspace.

Questions for reflection:

- What makes you feel safe and secure *(Holistic Security, 2022b)*?
- What actions do you regularly take to ensure the safety of you and your loved ones *(Holistic Security, 2022b)*?
- How does your access to power influence how you stay safe and secure?



SECTION 2: TAKING ACTION

How to: Build Greater Transparency in Cyber Practices

Building an ***open****, peaceful and secure cyberspace*

An open cyberspace means a transparent cyberspace. However, many cybersecurity practices are shrouded in secrecy, presenting ill-intentioned actors with opportunities to exploit weak self-regulatory structures *(di Meco, 2022)*. Private technology companies, in particular, have historically been unwilling to share information about their algorithmic, data, and privacy practices and policies as they currently profit from them *(Engler, 2020)*. This murky cyber environment prevents accountability, allows unethical actors to evade oversight, and further impedes many marginalised groups of people from feeling like the online world is a safe space for them.

Two key questions can frame approaches to transparency when designing regulatory frameworks and systems:

- When the needs of marginalised people are centred and prioritised, what should the online world look like?
- What measurement and accountability systems must be built to know this is being achieved *(Beall, C., 2022)*?

Transparency in data practices

Data is a form of power and can be used to obscure or reveal, exploit or empower. Current data practices, when uncritical, reflect the patriarchal, capitalist, and racist status quo. Ensuring open cyberspace is accessible and safe for all means reforming how we collect, use, and understand data so that biases found in society aren't further perpetuated. In the long term, this means creating an online space where human rights are safeguarded, where technology corporations operate under clear accountability frameworks, and transparency across the sector is standard *(G7 Information Centre, 2021).* In the short term, it means reforming how data is used to shape the world around us.

Data alone cannot fix the root causes of systemic oppression. However, it can be a useful resource to understand the breadth of compounding disadvantages and discrimination and, therefore, understand how to redress them *(Christoffersen, 2017; Global Partnership for Sustainable Development, 2021).*

Intersectional approaches to data take a particular focus on data collection and disaggregation and query the following *(Balestra and Fleischer, 2018; United Nations Office of the High Commissioner for Human Rights, 2018)*:

Are current data collection processes and methodologies conducive to generating disaggregated data?

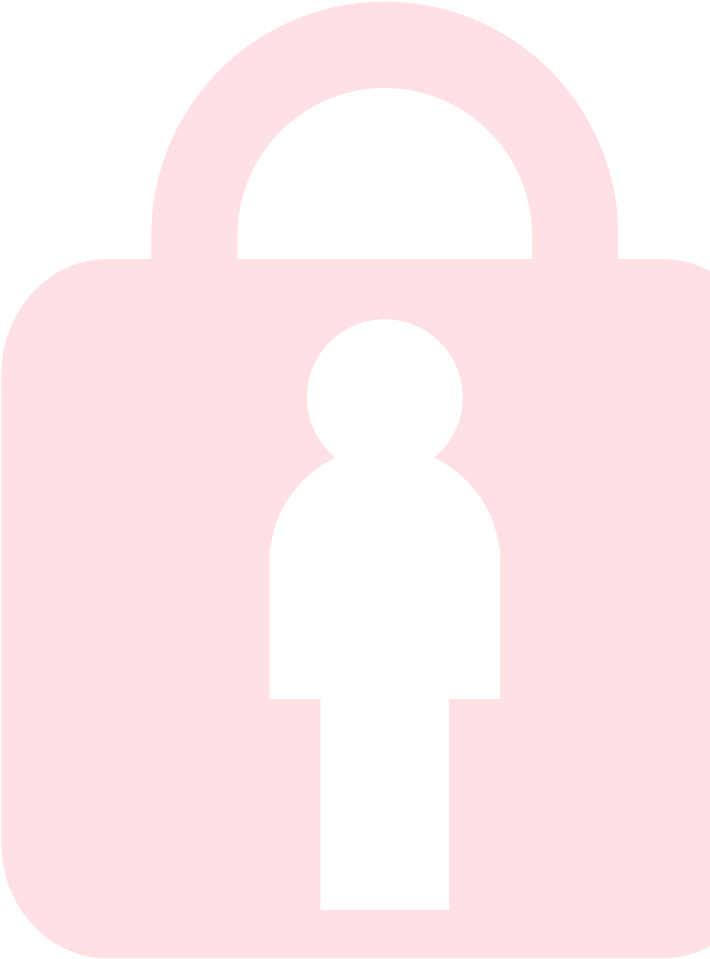
- In what ways do current data practices put marginalised people at risk? How can this be remedied?
- What standards for disaggregated data exist in your work, and how do they compare to standards in other countries or multilateral bodies?
- What steps can be taken to ensure better recording of disaggregated data in your work?
- How can published data more effectively identify and analyse intersecting identities and hidden inequalities?
- What processes must be implemented to ensure that data privacy protection mechanisms are continually improved?

Building institutional transparency with reflexivity

A common feminist practice is the act of reflexivity, which is the process of reflecting on your own social power and biases. It encourages greater awareness of how "social, cultural, political, economic aspects of their own background, experience, education and embodied presence in the world" have shaped your worldview and intellectual standpoint *(University of York, 2022).*

The creation of more transparent practices starts with reflexivity. Reflecting on how policy institutions can adapt and transform to better meet the needs of marginalised people is the first step to reforming the patriarchal, capitalist, and racist norms that shape modern UK policy to begin with. But reflexivity isn't just a practice for institutions, it's also a practice for individuals *(Knowledge Translation Network, 2022).* Engaging with the following questions can serve as a jumping off point to fortifying more robust systems of accountability:

- Whose point of view is reflected when defining cybersecurity and data practice problems?
- Who decides what information gaps are being systemically addressed, and how is this being acted upon?
- How is the quality of data regulated?
- How are staff made aware of and included in ongoing institutional reflexivity practices?
- How are avenues for civil society to feed into transparency efforts being increased?



How to: Ensure Safe Internet Access

*Building an open, **peaceful** and secure cyberspace*

A peaceful cyberspace means building processes and infrastructure so that experiences of online violence and harassment are outliers, not the norm. In the short term, this begins with addressing and preventing the high rates of online abuse experienced by marginalised groups. In the long term, this includes addressing the root causes of inequality in society, including sexism, racism, and classism (among others).

This section of the toolkit will build on the short-term goal of addressing and preventing online abuse. In the past few years, as we increasingly spend our daily lives online, there has been a rise in online abuse and harassment. For example, the Government Equalities Office reported that in 2019 only 5% of workplace sexual harassment occurred online *(Adams etal. 2020).* In a survey conducted by Rights of Women in 2020, 42% of women reported that workplace sexual harassment occurred online *(Rights of Women, 2020).*

What happens when we take an intersectional look at online abuse? In one study, 29% of women reported worsening online abuse during the pandemic. However, once disaggregated data is taken into account, this figure increases to 38% for Black and minoritised women and non-binary people *(Glitch UK and End Violence Against Women Coalition, 2020).* For disabled people, this figure jumps to 52% *(Freeman-Powell, 2021).*

According to Glitch UK (2022), online abuse refers to the range of harmful tactics and acts experienced by individuals online. This can include (among many other actions) offensive comments, threats of violence, or bullying. It is distinct from offline abuse due to "the reach, speed, amplification and permanence of abusive content".

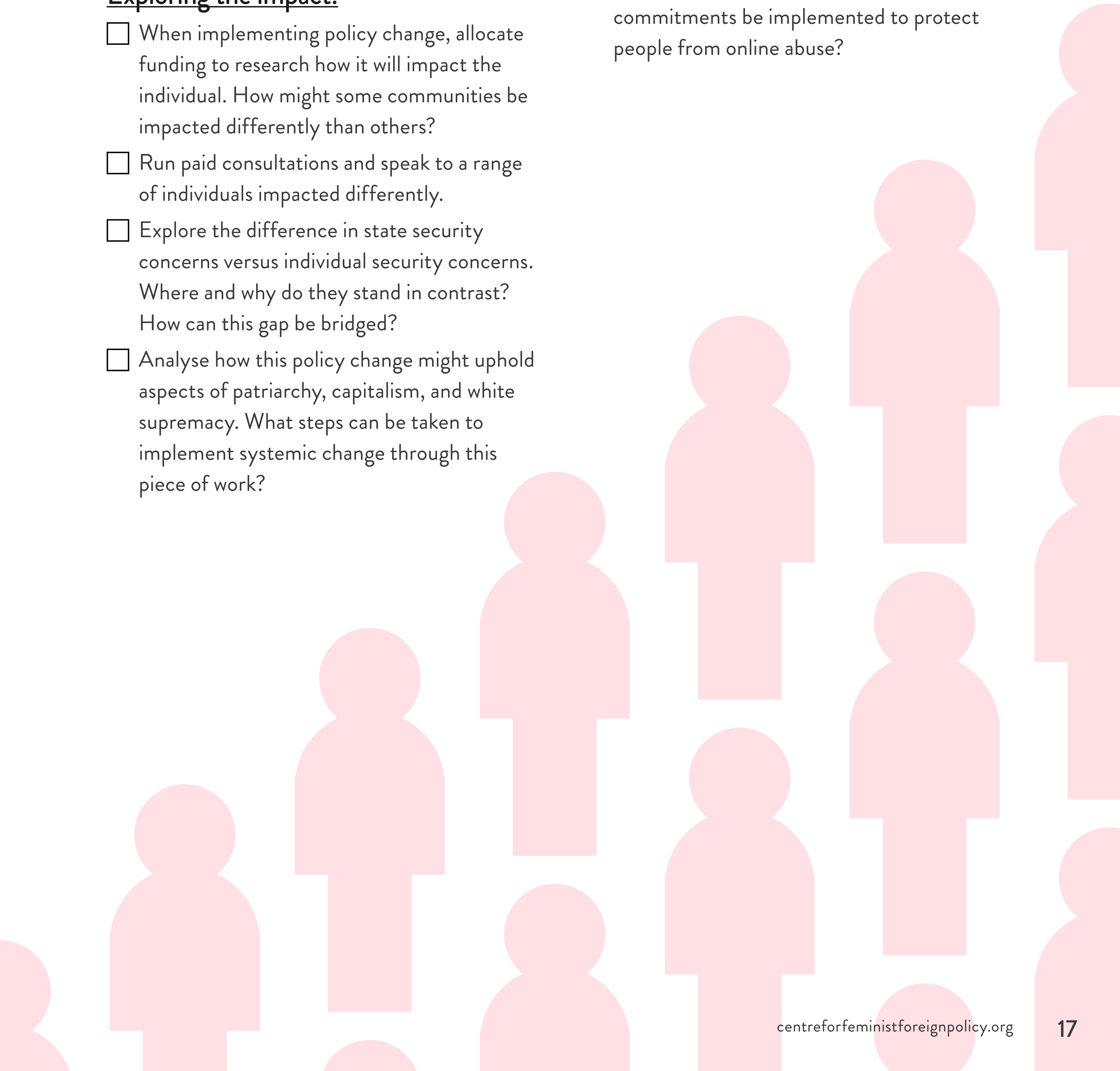
To manage and prevent escalating online abuse, considerations in the project planning phase of policy work hold opportunities to systematically ensure any new projects meaningfully addresses online abuse:

Exploring the impact:

- □ When implementing policy change, allocate funding to research how it will impact the individual. How might some communities be impacted differently than others?
- □ Run paid consultations and speak to a range of individuals impacted differently.
- □ Explore the difference in state security concerns versus individual security concerns. Where and why do they stand in contrast? How can this gap be bridged?
- □ Analyse how this policy change might uphold aspects of patriarchy, capitalism, and white supremacy. What steps can be taken to implement systemic change through this piece of work?

Fortifying Regulations:

- □ Audit the regulatory frameworks concerning with protecting people from online abuse. How does your work incorporate these?
- □ Analyse how existing regulations fall short in the context of your work. How can additional commitments be implemented to protect people from online abuse?



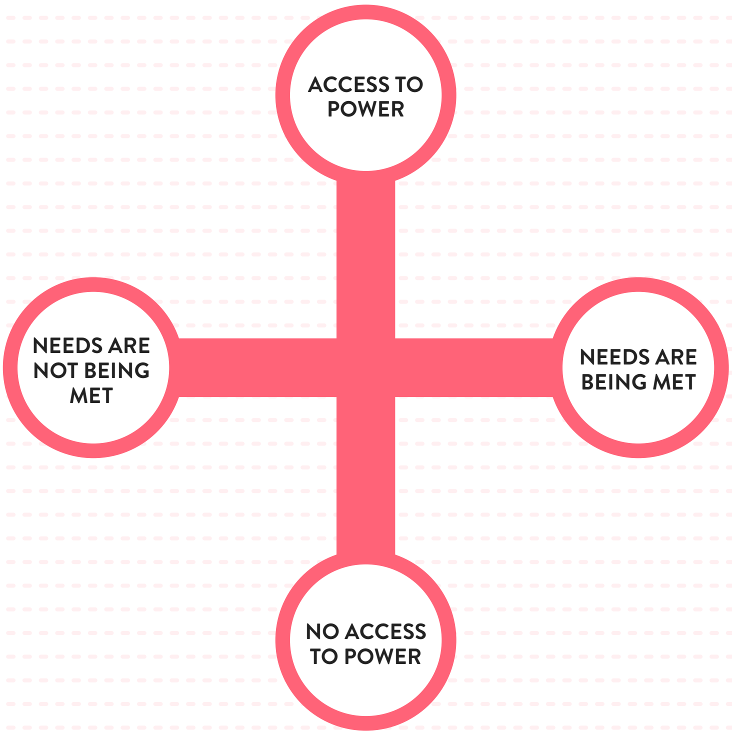
How to: Conduct Intersectional Consultations

*Building an open, peaceful and **secure** cyberspace*

A secure cyberspace means ensuring people feel safe. An intersectional approach means that people's lived experiences are taken seriously when developing and enacting cybersecurity measures. In the long term, this means crafting a space where historically marginalised people can participate online without fear of persecution. This section will detail conducting intersectional consultations to prioritise lived experiences as a key informant for policy formation.

Stakeholder and power mapping

Using intersectionality as an analytical tool to explore invites a curiosity about power dynamics: who has power, who doesn't, and why. Stakeholder mapping through an intersectional lens also invokes a process of power mapping to explore these questions. A list of stakeholders might usually look like a laundry list of names of institutions. Stakeholder mapping through a power map would focus more on the nexus of power and needs:



Adapted from The Change Agency's *(2022)* power mapping exercise. Image description: An XY graph to plot people in relation to access/no access to power, how needs are being met/not met.

Next, it is necessary to ask why different stakeholders are positioned where they are on the map to explore the systems that maintain power hierarchies.

This exercise helps to visualise how diverse consultations are and where the balance of power lies in who is taken seriously in policy formation processes.

Enabling participation in the consultation process *(GAPS UK, 2020)*

□ Audit the tools and mechanisms used to accommodate the needs of those involved in the consultation process. Are people who are not digitally literate, have disabilities, or don't speak English, for example, going to be able to participate fully?

□ Develop clear safeguarding and consent protocols for participation. Will someone's safety and security be at risk if they participate, i.e., undocumented immigrants?

□ Allocate funding to reimburse people for their time and contribution. If travel is necessary for in-person meetings, cover travel and care costs to enable those with caring responsibilities to participate.

Acting on the consultation results *(GAPS UK, 2020)*

□ Audit the systems in already place to ensure the results of the consultation are taken seriously and acted upon. Are they reflected in just this work or incorporated into wider institutional practices?

□ Review how stakeholders are acknowledged and credited for their contributions. When consent is given, how is the time and insight of stakeholders acknowledged?

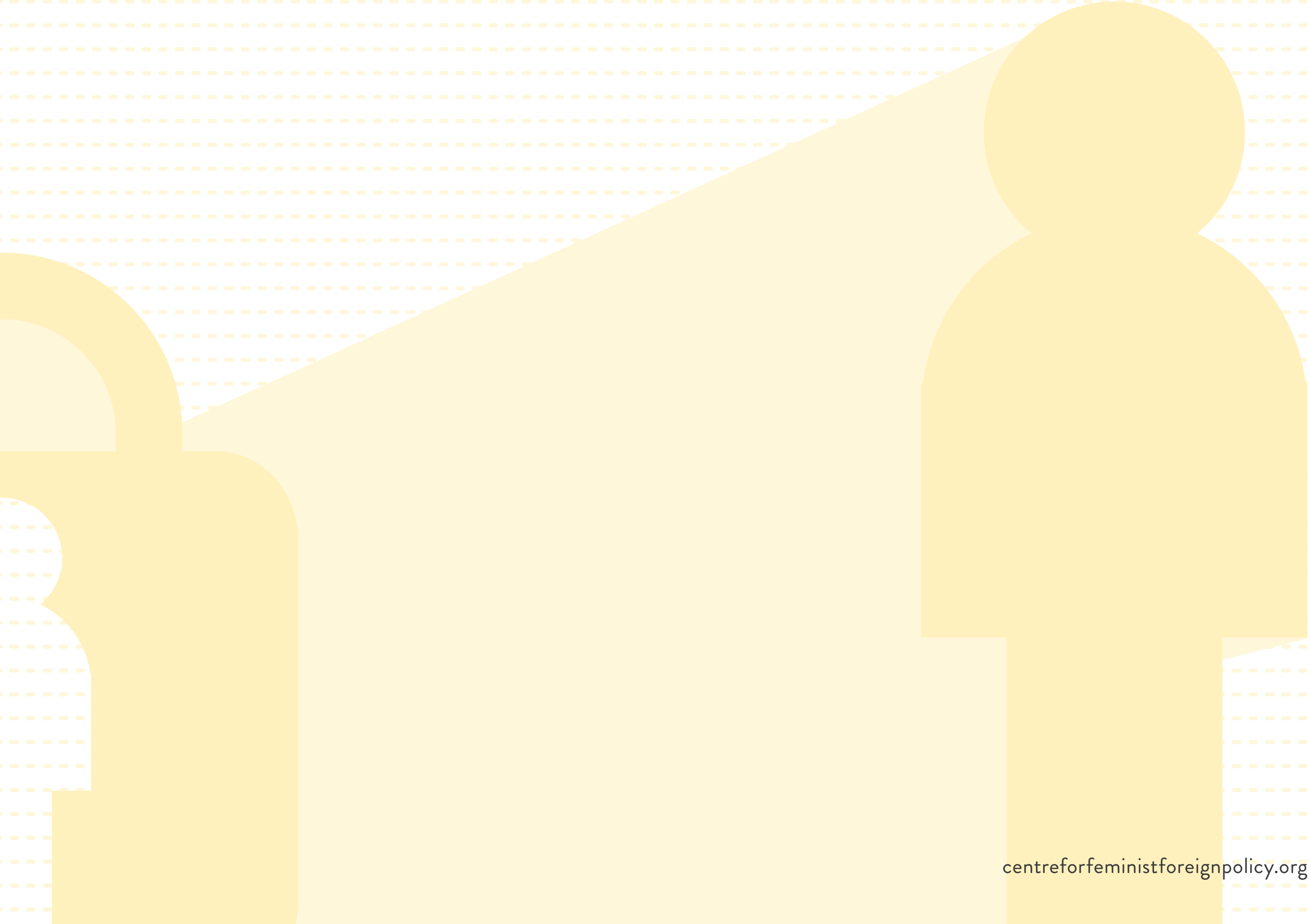
□ Check what feedback mechanisms are in place for comments and concerns after the consultation. Do stakeholders have safe and accessible ways to provide feedback into ongoing monitoring and evaluation practices for consultations?

□ Look at how stakeholder relationships are maintained after the consultation. Do pathways to policymakers remain open, especially for people who are typically ignored in the policymaking process?

ANNEXE

Questions for Self-Reflection

- How does my identity shape my access to power?
- Where might I lack awareness because of my access to power?
- How does my access to power influence how I do my work?
- How am I creating more space to address the needs of marginalised people in my work?
- What steps can I take to learn more about power inequalities?



About the Authors

Marissa Conway is an award-winning activist and Feminist Foreign Policy expert. She is the Co-Founder and UK Executive Director of the Centre for Feminist Foreign Policy. She regularly consults with organisations and governments worldwide to design feminist approaches to longstanding foreign and security policy problems. Marissa's expertise and insights have been featured in the BBC, the New York Times, Foreign Policy, and more. In 2019 she was named on the Forbes 30 Under 30 List 2019 in recognition of her work.

Originally from Silicon Valley in California, Marissa currently resides in the UK. She has a BA in Political Science and BA in Music from Chapman University, an MA in Gender Studies from SOAS, University of London, and half a PhD in Politics at the University of Bristol. Learn more about Marissa's work at www.marissaconway.com

Follow Marissa on Instagram @marissakconway *and Twitter* @marissakconway

Nehmat Kaur is a lawyer by training and has completed her LLM in Human Rights, Conflict, and Justice from SOAS, University of London. At SOAS, her LLM dissertation project focused on the gendered implication of biometric technologies and their transfers as foreign aid. Previously, she has been involved in policy and advocacy of digital civil liberties and used to litigate in the field of anti-discrimination, civil liberties, and constitutional law in New Delhi, India.

Follow Nehmat on Twitter @Nehmat_K

Acknowledgements

Many people fed into the process of this toolkit creation. We are so grateful for the time and expertise of the following people, whose insight has been invaluable and have made this toolkit possible:

Alexi Drew
Ali Dunn
Annalena Pott
Anuradha Damale
Dr Anwar Mhajne
Chris Beall
Crystal Whetstone
Dhanaraj Thakur
Gabrielle Bardall
James Shires
Julia Słupska
Kasey Robinson
Dr Katharine M Millar
Katie Washington
Laia Aycart
Lemona Chanda
Livi Dee
Lucie Goulet
Lucina Di Meco
Luna KC
Marwa Azelmat
Nayana Prakash
Ndidi Olibamoyo
Niamh Healy
Seyi Akiwowo
Tambria Schroeder
Dr Tatiana Tropina

Lastly, we would like to thank the Foreign Commonwealth and Development Office's Conflict Security and Stability Fund for supporting this work.

References

Adams, L., Hilger, L., Moselen, E., Basi, T., Gooding, O. and Hull, J., 2020. *2020 Sexual Harassment Survey*. [online] Government Equalities Office. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1002873/2021-07-12_Sexual_Harassment_Report_FINAL.pdf> [Accessed 11 February 2022].

Alkire, S., 2003. *A Conceptual Framework for Human Security*. [online] Centre for Research on Inequality, Human Security and Ethnicity, CRISE, Queen Elizabeth House, University of Oxford. Available at: <https://assets.publishing.service.gov.uk/media/57a08cf740f0b652dd001694/wp2.pdf> [Accessed 2 March 2022].

Amnesty UK, 2017. *Black and Asian women MPs abused more online*. [online] Available at: <https://www.amnesty.org.uk/online-violence-women-mps> [Accessed 11 February 2022].

Amnesty UK, 2018. *'Toxic' Twitter is failing women by letting online violence thrive – new research*. [online] Available at: <https://www.amnesty.org.uk/press-releases/toxic-twitter-failing-women-letting-online-violence-thrive-new-research> [Accessed 14 February 2022].

Balestra, C. and Fleischer, L., 2018. *Diversity statistics in the OECD: How do OECD countries collect data on ethnic, racial and indigenous identity?*. SDD Working Paper No. 96. [online] OECD. Available at: <https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=SDD%2FDOC%282018%299&docLanguage=En> [Accessed 15 February 2022].

Beall, C., 2022. *Interview about data transparency*.

Cabinet Office, 2021. *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*, HM Government. Available at: <https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy> [Accessed 21 September 2021].

Cabinet Office, 2022. *National Cyber Strategy 2022*. [online] Available at: <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022> [Accessed 18 February 2022].

Carastathis, A., 2014. The Concept of Intersectionality in Feminist Theory. *Philosophy Compass*, 9(5), pp.304-314.

Christoffersen, A., 2017. *Intersectional approaches to equality research and data*. [online] Equality Challenge Unit. Available at: <http://www.ecu.ac.uk/wp-content/uploads/2017/04/Research_and_data_briefing_2_Intersectional_approaches_to_equality_research_and_data.pdf> [Accessed 14 February 2022].

Crenshaw, K., 1991. Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Review*, [online] 43(6), p.1241. Available at: <https://perpustakaan.gunungsitolikota.go.id/uploaded_files/temporary/DigitalCollection/YmQzYTgwNDRiNWQwMWViMGUxOGI0MDI3OGJmZWFhMTdkYTIzZmM3MQ==.pdf>.

di Meco, L., 2022. *Interview about gendered disinformation.*

Dunkley, L., Conway, M. and Messmer, M., 2021. *Gender, think-tanks and international affairs: a toolkit.* [online] Chatham House. Available at: <https://www.chathamhouse.org/sites/default/files/2021-02/2021-02-10-gender-think-tanks-international-affairs-dunkley-et-al_1.pdf> [Accessed 1 March 2022].

Engler, A., 2020. *Tech cannot be governed without access to its data.* [online] Available at: <https://www.brookings.edu/blog/techtank/2020/09/10/tech-cannot-be-governed-without-access-to-its-data/> [Accessed 14 February 2022].

Freeman-Powell, S., 2021. *Online abuse of those with disabilities increases more than 50 percent during lockdown.* [online] Available at: <https://news.sky.com/story/online-abuse-of-those-with-disabilities-increases-more-than-50-percent-during-lockdown-12426989> [Accessed 11 February 2022].

GAPS UK, 2020. *Beyond Consultations.* [online] Available at: <https://beyondconsultations.org/images/Beyond_Consultations_Tool.pdf> [Accessed 7 March 2022].

G7 Information Centre, 2021. *2021 Annex 3: G7 Internet Safety Principles.* [online] Available at: <http://www.g7.utoronto.ca/ict/2021-annex_3-internet-safety.html> [Accessed 15 February 2022].

Glitch UK, 2022. *A Little Means A Lot: How you can be an Online Active Bystander.* [online] Available at: <https://glitchcharity.co.uk/wp-content/uploads/2021/09/Glitch_Online_Active_Bystander_ALMAL_Sept2021.pdf> [Accessed 11 February 2022].

Glitch UK and End Violence Against Women Coalition, 2020. *The Ripple Effect: COVID-19 and the Epidemic of Online Abuse.* [online] Available at: <https://glitchcharity.co.uk/wp-content/uploads/2021/04/Glitch-The-Ripple-Effect-Report-COVID-19-online-abuse.pdf> [Accessed 11 February 2022].

Global Partnership for Sustainable Development, 2021. *Unpacking Intersectional Approaches to Data.* [online] Available at: <https://www.data4sdgs.org/resources/unpacking-intersectional-approaches-data#:~:text=To%20reduce%20inequalities%20and%20practice,discrimination%20or%20disadvantages%20people%20face.&text=Yet%2C%20uncritical%20data%20practice%20can,or%20perpetuating%20disadvantages%20and%20discrimination> [Accessed 14 February 2022].

Holistic Security, 2022a. *Prepare*. [online] Available at: <https://holistic-security.tacticaltech.org/chapters/prepare.html> [Accessed 3 March 2022].

Holistic Security, 2022b. *Reflecting on existing security practices*. [online] Available at: <https://holistic-security.tacticaltech.org/chapters/prepare.html> [Accessed 3 March 2022].

Knowledge Translation Network, 2022. *Intersectionality & Knowledge Translation: Reflection Workbook*. [online] Available at: <https://knowledgetranslation.net/wp-content/uploads/2020/02/IntersectionalityKT_Reflection_Workbook_Draft_Version.pdf> [Accessed 15 February 2022].

Koenecke, A., Nam, A., Lake, E., Nudell, J., Quartey, M., Mengesha, Z., Toups, C., Rickford, J., Jurafsky, D. and Goel, S., 2020. Racial disparities in automated speech recognition. *Proceedings of the National Academy of Sciences*, 117(14), pp.7684-7689.

Mannon Daniels, 2022. *Defining marginalised; DFID's Leave no one behind agenda*. [online] Available at: <https://www.ukaiddirect.org/wp-content/uploads/2017/03/Defining-marginalised.pdf> [Accessed 18 February 2022].

Metz, C., 2020. *There Is a Racial Divide in Speech-Recognition Systems, Researchers Say*. [online] Available at: <https://www.nytimes.com/2020/03/23/technology/speech-recognition-bias-apple-amazon-google.html> [Accessed 14 February 2022].

National Cyber Security Centre, 2022. *What is cyber security?* [online] Available at: <https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security> [Accessed 3 March 2022].

Ofcom, 2021. *Online Nation: 2021 Report*. [online] Available at: <https://www.ofcom.org.uk/__data/assets/pdf_file/0013/220414/online-nation-2021-report.pdf> [Accessed 11 February 2022].

Rights of Women, 2021. *Rights of Women survey reveals online sexual harassment has increased, as women continue to suffer sexual harassment whilst working through the Covid-19 pandemic*. [online] Available at: <https://rightsofwomen.org.uk/news/rights-of-women-survey-reveals-online-sexual-harassment-has-increased-as-women-continue-to-suffer-sexual-harassment-whilst-working-through-the-covid-19-pandemic/> [Accessed 11 February 2022].

Tadjbakhsh, S., 2005. *Human Security: Concepts and Implications with an Application to Post-Intervention Challenges in Afghanistan*. [online] Available at: <https://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/etude117_118.pdf> [Accessed 3 March 2022].

The Change Agency, 2022. *Power mapping*. [online] Available at: <https://thechangeagency.org/power-mapping/> [Accessed 7 March 2022].

United Nations Office of the High Commissioner for Human Rights, 2018. *A Human Rights-Based Approach to Data: Leaving No One Behind in the 2030 Agenda for Sustainable Development*. [online] Available at: <https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf> [Accessed 15 February 2022].

UN Women, 2022. *Concepts and definitions*. [online] Available at: <https://www.un.org/womenwatch/osagi/conceptsandefinitions.htm> [Accessed 2 March 2022].

University of York, 2022. *Reflexivity and Self-reflexivity.* Feminist Research Ethics. [online] Available at: <https://genurb.apps01.yorku.ca/courses/feminist-research-ethics/lessons/reflexivity-and-self-reflexivity/> [Accessed 15 February 2022].

YWCA Australia, 2020. *Y Advocacy? An Intersectional Feminist Toolkit*. [online] Available at: <https://www.ywca.org.au/wp-content/uploads/2020/12/2020_YAdvocacy_IntersectionalFeministToolkit.pdf> [Accessed 1 March 2022].

THE CENTRE FOR FEMINIST FOREIGN POLICY IS SHAKING THINGS UP.

CFFP THE CENTRE FOR FEMINIST FOREIGN POLICY

About CFFP

The Centre for Feminist Foreign Policy aims to smash the patriarchy in foreign policy.

Learn more about our work at
www.centreforfeministforeignpolicy.org

Centre for Feminist Foreign Policy UK

Company registration no. 11858782

Regency Court
62-66 Deansgate
Manchester M3 2EN
United Kingdom