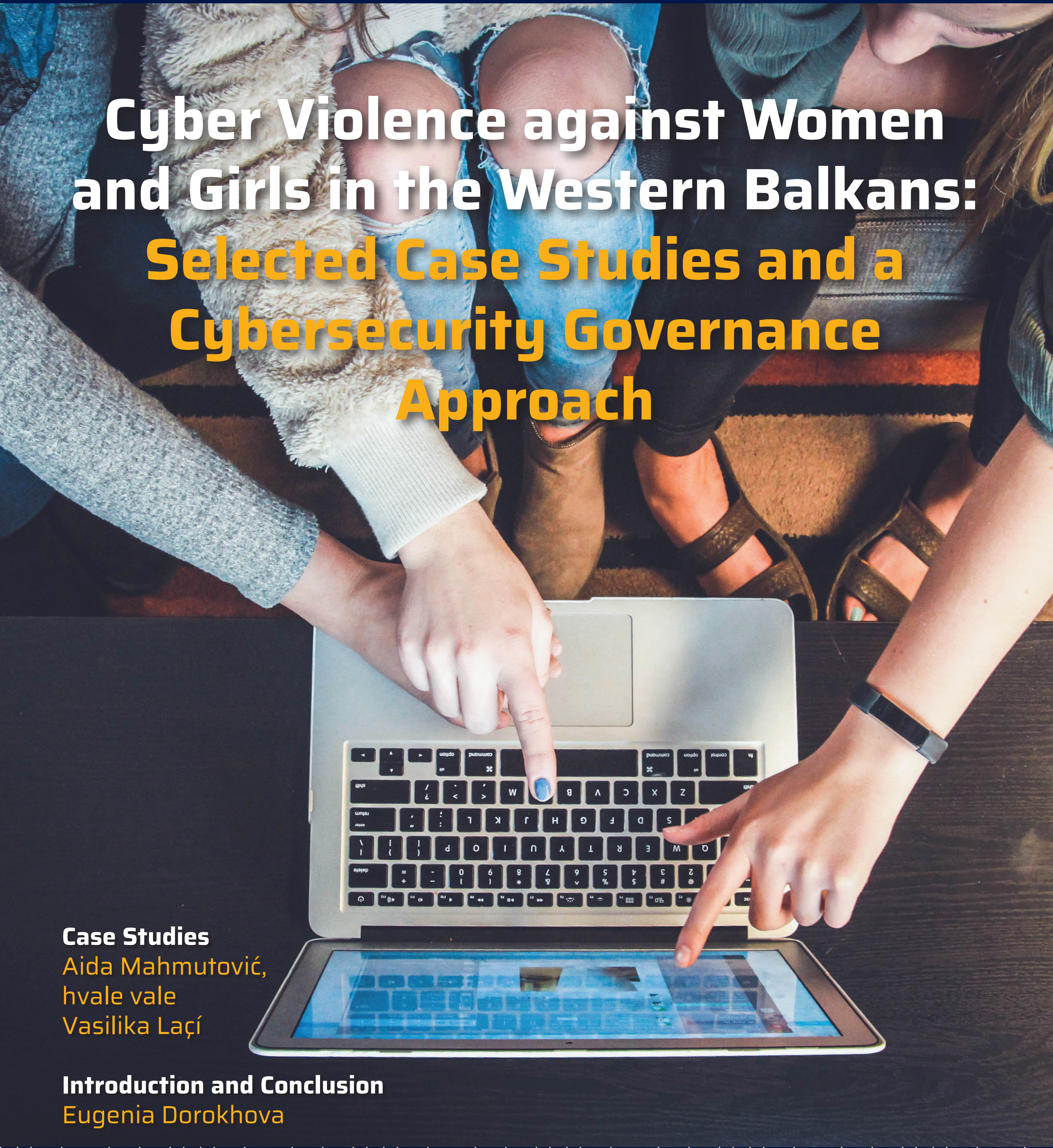
DCAF Geneva Centre for Security Sector Governance



Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach

Case Studies
Aida Mahmutović,
hvale vale
Vasilika Laçí

Introduction and Conclusion
Eugenia Dorokhova

Copyright page

Published in Switzerland by the Geneva Centre for Security Sector Governance (DCAF)

DCAF Geneva

P.O. Box 1360

CH-1211 Geneva 1

Switzerland

First published March 31st, 2021

Authors: Eugenia Dorokhova, hvale vale, Vasilika Laçí, Aida Mahmutovic

Editor: Franziska Klopfer

Design by DCAF and DTP studio

Cover photo: John Schobrich @johnschno

Copy-edited by Cherry Ekins

About this Publication

This text was produced as part of the DCAF project 'Enhancing Cybersecurity Governance in the Western Balkans' (2018–21) and funded by the United Kingdom's Foreign, Commonwealth and Development Office. The views expressed are those of the authors alone.

Acknowledgements

The authors of this paper wish to thank Vasilika Laçí for her generous support and voluntary contribution in co-authoring the Albania case study. Vasilika Laci`s knowledge of the context, language and politics in Albania, as well as her friendship and trust, made the research for this case study possible.

The authors would like to sincerely thank Callum Watson and Megan Bastick for their invaluable expertise and suggestions on earlier drafts of this publication.

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders.

DCAF's Foundation Council is comprised of representatives of about 60 member states and the Canton of Geneva. Active in over 80 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on Twitter @DCAF_Geneva.

DCAF - Geneva Centre for Security Sector Governance

Maison de la Paix Chemin Eugène-Rigot 2E

CH-1202 Geneva, Switzerland

Tel: +41 22 730 94 00

info@dcaf.ch

www.dcaf.ch

Twitter @DCAF_Geneva

Table of Contents

Introduction:

CYBERSECURITY GOVERNANCE AND CYBER VIOLENCE AGAINST WOMEN AND GIRLS IN THE WESTERN BALKANS – CONNECTING THE DOTS

EUGENIA DOROKHOVA

Introduction: **Cybersecurity Governance and Cyber Violence against Women and Girls in the Western Balkans – Connecting the dots**

Eugenia Dorokhova

Over the last two decades, the internet has become embedded into nearly all areas of our day to day lives, in both noticeable and silent ways. We have become dependent on Information Communication Technologies (ICTs) and access to online services for work, pleasure, information, and communication. Such access is increasingly important for human development and networked ICTs have become a driving force in global economic growth. State infrastructures in sectors such as transportation, finance, commerce, medical care, and military defence are becoming ever more reliant on network connectivity.

The possibility of any networked device receiving communications requests has, however, in many ways introduced new vulnerabilities and security risks. These security risks in cyberspace – or cybersecurity risks – need to be addressed and mitigated. Cybersecurity can be defined both as the state of being protected in cyberspace and the measures taken to protect cyberspace and its users' assets.[1] As such, cybersecurity not only requires technical solutions that help keep ICTs and services safe against attacks and incidents, it also requires a system of governance that sets out the roles and responsibilities of those involved in providing, managing, and overseeing cybersecurity.

When thinking about possible models of cybersecurity governance, it seems useful to look at the concept of good governance in the security sector (SSG). Good SSG aims to make the state's security sector more effective and accountable within a framework of democratic civilian control, respect for human rights and the rule of law.[2] It therefore addresses many of the challenges that cybersecurity governance is also faced with.

Good Governance and Cybersecurity

Good SSG applies principles of good governance to the security sector, including: Accountability, Transparency, Rule of Law, Participation, Responsiveness, Effectiveness and Efficiency.[3] Good security sector governance furthermore requires the justice and security sectors to understand people`s diverse needs and meet these needs as part of security provision, management and oversight.[4] Applying the human security lens to cybersecurity means that this safety in

[1] The Oxford Dictionary online defines cybersecurity as: "The state of being protected against the criminal or unauthorised use of electronic data, or the measures taken to achieve this."
The International Telecommunications Union has the following definition of cybersecurity: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets." (Recommendation ITU-T X.1205)

[2] For more information, see: DCAF Security Sector Reform Backgrounder, Security Sector Governance: Applying the principles of good governance to the security sector (2015). Available online at: https://www.dcaf.ch/security-sector-governance-applying-principles-good-governance-security-sector-0

[3] DCAF Security Sector Reform Backgrounder, Security Sector Governance: Applying the principles of good governance to the security sector (2015), p. 3. Available online at: https://www.dcaf.ch/security-sector-governance-applying-principles-good-governance-security-sector-0

[4] DCAF, OSCE/ODIHR, UN Women (2019), Security Sector Governance, Security Sector Reform and Gender, in Gender and Security Toolkit, Geneva. Available online at: https://www.dcaf.ch/tool-1-security-sector-governance-security-sector-reform-and-gender

cyberspace should not only concern itself with protecting data and networks but also aim to enhance human security online.

Below follows a description of these principles and an explanation of how they could be applied in cybersecurity.[5]

- **Accountability:** There are clear expectations for security provision, and independent authorities oversee whether these expectations are met and effectively impose sanctions if they are not. Cybersecurity requires the close cooperation between public and private actors, much more so than any other security sector. For example, state cybersecurity actors need to work closely with providers of online services and telecommunications networks, which are usually owned by private businesses. Oversight actors should therefore look beyond the work of state actors, and also consider the roles and responsibilities of non-state actors involved in cybersecurity.

- **Transparency:** Information is freely available and accessible to those who will be affected by decisions and their implementation. The principle of transparency also needs to apply to cybersecurity. Moreover, the division of roles and responsibilities of different actors in cybersecurity need to be clearly defined and transparently verifiable, so that the process of security provision can run smoothly with different actors working together.

- **Rule of law:** all persons and institutions, including the state, are subject to laws that are known publicly, enforced impartially and consistent with international and national human rights norms and standards. Cybersecurity governance requires a novel approach to regulation because it needs to take account of the roles and responsibilities of state- and non-state actors in effective cybersecurity provision. Legal and regulatory frameworks pertaining to cybersecurity provision and oversight must be based on the rule of law and should be developed in line with principles of good governance.

- **Participation:** Women and men of all backgrounds have the opportunity to participate in decision-making and service provision on a free, equitable and inclusive basis, either directly or through legitimate representative institutions. Due to the many actors involved in cybersecurity provision, a multi-stakeholder approach should be fostered in cybersecurity governance and oversight in order to accurately reflect the needs of the diverse cybersecurity beneficiaries.

- **Responsiveness:** Institutions are sensitive to the different security needs of all parts of the population and perform their missions in the spirit of a culture of service. Cybersecurity should take on an approach wherein the security needs of the individual and population at large are at the core of its protection. Policies relating to cybersecurity provision and oversight should therefore ensure that the need of all members of society to participate fully and safely in online life is accurately reflected and protected.

- **Effectiveness:** Institutions fulfil their respective roles, responsibilities, and missions to a high professional standard. Cybersecurity needs to be provided effectively to networks and citizens, along clearly defined parameters based on an analysis of the needs of the state and its population.

- **Efficiency:** Institutions make the best possible use of public resources in fulfilling their respective roles, responsibilities, and missions. Moreover, cybersecurity governance and oversight processes need to be tailored in a way that will allow them to most efficiently support the provision of security to the various actors in cyberspace.

[5] Based on Franziska Klopfer, Irina Rizmal and Milan Sekuloski`s Good Governance and Cybersecurity, DCAF internal document, not published.

Why does gender equality matter in the security (and justice) sector and how does this link to cybersecurity governance?

Gender refers to historically and socially constructed roles attributed to women and men, as opposed to their biological or physical characteristics. As such, gender is one of the most important factors that define inequality in societies, placing people in different positions of power, risk, security, and insecurity, with different possibilities of accessing the services of security and justice providers.[6]

In any society, women, men, and in particular people of diverse sexual orientations, gender identities and expressions, often face specific forms of discrimination, exploitation, abuse, and violence for not adhering to societal gender norms. In conflict and crisis situations, such risks to persons of diverse sexual orientation and gender identities and expressions are often exacerbated even further.[7]

Cybersecurity impacts everyone: every woman, man, girl, boy, any person of diverse gender identity and expression. A lack of equal representation and participation of people of different genders in policymaking and decision-making processes can lead to security needs being overlooked and not addressed as a result of deficient perspectives. Women today are stakeholders with a vested interest and value, who need to have equal opportunities and empowered access to meaningfully participate in policies, decisions and development programs that will affect them and others in the future.

Cyber Violence against Women and Girls (Cyber VAWG)

Cyber violence is a cybersecurity threat which has grown exponentially in the past decade. It has been defined as "the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering, and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities." [8] The internet provides ample opportunity to stay anonymous, while simultaneously allowing deep access into the privacy of its users. The accessibility and nature of online services and ICTs also means that abuse can be done at a distance, not requiring physical presence to inflict serious harm.

Men and women can become victims of cyber violence. However, cyber violence against women and girls (cyber VAWG) occurs much more frequently, perpetuating an enabling environment in which further discrimination, harassment and violence against women and girls (VAWG) is normalised in society.[9] VAWG in the offline world is already present in immense proportions and on a global scale. It exists in every society, encompassing different forms of physical, sexual, and psychological abuse. [10] This violence has further increased exponentially during the Covid-19 crisis.[11]

[6] DCAF, OSCE/ODIHR, UN Women (2019), Security Sector Governance, Security Sector Reform and Gender, in Gender and Security Toolkit, Geneva. Available online at: https://www.dcaf.ch/tool-1-security-sector-governance-security-sector-reform-and-gender

[7] Ibid. p 9

[8] Council of Europe, Cybercrime Convention Committee (T-CY) Mapping study on Cyberviolence (2018), p 5. Available online at: https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914

[9] Tandon, N. and Pritchard, S. for UN Broadband Commission for Digital Development and Working Group on Broadband and Gender, Cyber Violence against Women and Girls: A world-wide wake-up call (2015). Available online at: https://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259

[10] See for example: UN Women, Facts and figures: Ending violence against women. Available online at: https://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures

[11] Ibid.

The many forms of VAWG still devastatingly remain an often culturally accepted practice, the reasons for which are rooted deep in harmful gender stereotypes and attitudes stemming from the continuous acceptance of patriarchal societal norms.[12] As such, violence that is directed against a woman because she is a woman, and violence that affects women disproportionately, must be deemed gender-based violence (GBV). In this publication, we use both cyber VAWG and online GBV as terms to synonymously address acts of online-/technology facilitated abuse against women and girls, which are committed against them because of their gender.

Cyber VAWG, in its most prevalent version, includes straightforward violence in the form of online harassment; online sexual harassment; online defamation; cyber stalking and surveillance/ tracking; hacking; impersonation; identity theft; image-based abuse; malicious distribution (including threats thereof); cyber bullying and many other forms of abuse.

The 2015 UN Broadband Commission for Digital Development report[13] concluded that 73% of women present online have experienced abuse. Particularly women aged 18 to 24 are deemed at greater risk to being exposed to every kind of cyber VAWG, including online stalking and sexual harassment, as well as physical threats online. VAWG perpetuates gender inequality, and has serious negative effects on the health, wealth, wellbeing and rights of all women and girls. Studies have shown a significant link to depression and exponentially higher cases of suicides in children and adolescent girls faced with online harassment and cyber violence.[14]

Cyber violence as a force-multiplier

The use of digital means for technology-facilitated abuse can range from online violence, (sexual) harassment, sexting, revenge-porn, image-based abuse, stalking and tracking, all the way to human trafficking and child sexual exploitation and abuse.[15] The use of cyber violence thereby also acts as an enabling tool leading to the perpetration of a variety of further crimes, with serious human rights consequences.

Technology facilitated abuse is frequently used as an effective tool to silence individuals and oppress their opinions, encroaching upon freedom of speech and human rights advocacy. Women in public and political roles are disproportionately targeted by cyber violence and gendered disinformation campaigns, intending to discredit, humiliate, intimidate and silence them in all spheres of public life.[16] This can have a severely negative effect on women`s participation in democratic processes and intrinsically damages governance structures. Female journalists face

[12] For examples of such societally accepted norms, see for example: Oxfam International, Ten harmful beliefs that perpetuate violence against women and girls. Available online at: https://www.oxfam.org/en/ten-harmful-beliefs-perpetuate-violence-against-women-and-girls

[13] Tandon, N. and Pritchard, S. for UN Broadband Commission for Digital Development and Working Group on Broadband and Gender, Cyber Violence against Women and Girls: A world-wide wake-up call (2015). Available online at: https://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259
See page 22 for an overview of terms.

[14] See for example here: https://www.sciencedaily.com/releases/2018/04/180419130923.htm
And here: https://www.elsevier.es/en-revista-revista-colombiana-psiquiatria-english-edition--479-pdf -S2530312017300577

[15] There are many sources available to those seeking more information on this topic. A collection of resources and further information on technology-facilitated abuse can be found for example on VAWnet. Available online at https://vawnet.org/sc/technology-assisted-abuse

[16] A wealth of information and analysis on this phenomenon is available online from a variety of sources. See for example:
- https://www.brookings.edu/techstream/gendered-disinformation-is-a-national-security-problem/
- https://carnegieendowment.org/2020/11/30/tackling-online-abuse-and-disinformation-targeting-women-in-politics-pub-83331
A practical Quick-read guide: gender and countering disinformation toolguide published 2020 by the UK Government is available online at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866353/Quick_Read-Gender_and_countering_disinformation.pdf

cyber violence and cyberattacks much more frequently than their male colleagues.[17] There is a significant negative impact of cyber violence on women human rights defenders and women`s organisations globally.[18]

Furthermore, domestic violence is often linked to the use of cyber means to stalk, track and harass female victims.[19] Here, the victim of domestic violence can often be further intimidated, controlled, followed, harassed and bullied into submission through technological means and by acts of online abuse. The harm this causes victims is measurable at emotional, psychological and often physical levels, and victims of digital domestic abuse can be left feeling as though they are tethered to their abusers through technology, controlled in all areas of their life and having no safe space to retreat. Significantly contributing to feelings of hopelessness, humiliation, and fear in victims of domestic violence, intimate partner cyber harassment furthermore is "demonstrably a strong and unique predictor of both depression and PTSD, even in the absence of physical violence."[20]

Cyber violence can lead to the further perpetration of transnational crimes with serious human rights implications. Connections made in cyberspace and the use/abuse of social media networks are among the most commonly used tools for human traffickers to entrap victims into sexual exploitation schemes through various manipulation tactics.[21] An analysis of data on trafficking victims over the last 15 years shows that women and girls continuously represent more than 70% of detected trafficking victims.[22] The vast majority of sex-trade victims are female, and are often underage. In Serbia, the Citizens` Association for Combating Trafficking in Human Beings and All Forms of Violence against Women (ATINA) conducted research based on the experiences of 178 girls and women using Atina`s support and protection programs in the period from 2015 to 2020. Their analysis confirms the high prevalence of online abuse and cyber violence that the victims were exposed to prior, during and after a trafficking situation. According to their report, online violence and technology facilitated abuse has "become an almost indispensable form of coercion used by perpetrators of violence and traffickers to blackmail, threaten, belittle the victims, unauthorizedly record, or distribute pornographic material involving children as well."[23]

[17] Quarmby, K. (2020), Female Journalists Still Bear the Brunt of Cyberattacks, truthdig.com, Available online at: https://www.truthdig.com/articles/female-journalists-continue-to-bear-brunt-of-internet-troll-attacks/

[18] See the Statement by UN High Commissioner for Human Rights Zeid Ra`ad Al Hussein at the 38th session of the Human Rights Council, 21.06.2018. Available online at: https://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=23238&LangID=E

[19] Dr. Al-Alosi, Technology-facilitated abuse: the new breed of domestic violence (2017), theconversation.com. Available online at: https://theconversation.com/technology-facilitated-abuse-the-new-breed-of-domestic-violence-74683
On domestic violence in the Western Balkans see for example: https://www.balcanicaucaso.org/eng/Dossiers/The-domestic-violence-in-the-Balkans

[20] King, R. in Victoria University of Wellington Law Review 29 (2017), Digital Domestic Violence: Are Victims of Intimate Partner Cyber Harassment Sufficiently Protected by New Zealand's Current Legislation

[21] UNODC, Global Report on Trafficking in Persons 2018, (United Nations publication, Sales No. E.19.IV.2). pp. 38-39. Available online at: https://www.unodc.org/documents/data-and-analysis/glotip/2018/GLOTiP_2018_BOOK_web_small.pdf

[22] Ibid. p. 25

[23] ATINA Citizens` Association for Combatting Trafficking in Human Beings and All Forms of Violence against Women, Behind the screens: Analysis of human trafficking victims` abuse in digital surroundings (2020). Available online at: http://www.atina.org.rs/sites/default/files/Behind%20the%20screens%20Analysis%20of%20human%20trafficking%20victims%27%20abuse%20in%20digital%20surroundings.pdf

Addressing Cyber VAWG in the Western Balkans: three case studies

In the Western Balkan economies[24] gender-based violence, inadequate female political participation and decision-making, lack of gender mainstreaming, gender stereotyping, and discrimination against women in the labour market have all been recognised as critical gender inequality issues by civil society organisations. [25]

All Western Balkan economies (with the exception of Kosovo*[26]) have ratified the Istanbul Convention on Preventing and Combating Violence Against Women and Domestic Violence,[27] and have introduced legislative changes and policies to combat violence against women and girls. All economies in the region have enshrined in their legal framework the principle of non-discrimination between men and women, as well as certain laws on the prohibition and prevention of discrimination. In reality, the number of cases of cyber VAWG and technology-facilitated abuse in the Western Balkan region are as high as in other European countries.[28] It would therefore be important to examine why the legislation in place is not enough to guarantee effective non-discrimination online.

What other aspects of the national security and cybersecurity governance structure are failing? What considerations need to be taken by Western Balkan economies aiming to tackle these important issues?

Due to a lack of regional and context-specific statistical data and research, we endeavour to draw attention to these important issues through the three case studies that follow. While each case study is unique, the stories of the women portrayed in them are symbolic of the struggles many women face on a daily basis – both online and offline.

[24] The six Western Balkan economies: Albania, Bosnia-Herzegovina, Kosovo*, Montenegro, North Macedonia, Serbia

[25] CSF Policy Brief, No. 04, April 2018, Gender Issues in the Western Balkans, (2018) European Fund for the Balkans and European Policy Centre – CEP. Available online at: https://wb-csf.eu/docs/Gender_Issues.pdf.pdf
See also: Browne, E. (2017). Gender in the Western Balkans. K4D Helpdesk Report. Brighton, UK:
Institute of Development Studies, pp. 7-10. Available at: https://reliefweb.int/sites/reliefweb.int/files/resources/058%20Gender%20in%20the%20Balkans.pdf
* This designation is without prejudice to positions on status and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo declaration of independence

[26] Unable to ratify the treaty without membership to the UN or the Council of Europe, the National Assembly of Kosovo has nonetheless adopted an amendment to its constitution in September 2020, giving direct effect and applicability to the standards and obligations set forth in the Convention. See for example: https://www.coe.int/en/web/istanbul-convention/-/the-national-assembly-of-kosovo-decides-to-apply-the-istanbul-convention
See also https://www.coe.int/en/web/genderequality/reinforcing-the-fight-against-violence-against-women-and-domestic-violence-in-kosovo

[27] Council of Europe, Council of Europe Convention on preventing and combating violence against women and domestic violence, 11 May 2011. Available online at: https://www.coe.int/en/web/istanbul-convention/text-of-the-convention. See here for a quick overview of the Convention: https://ec.europa.eu/justice/saynostopvaw/downloads/materials/pdf/istanbul-convention-leaflet-online.pdf
The Istanbul Convention, also known as the Council of Europe Convention on preventing and combatting violence against women and domestic violence, sets the path to creating a legal framework at pan-European level to protect women against all forms of violence. It further obliges state parties to adopt measures in order to prevent, prosecute and eliminate violence against women within their national jurisdictions.

[28] See for example:
- Online abuse now commonplace for Balkan women reporters on BalkanInsight.com Available online at: https://balkaninsight.com/2019/06/18/online-abuse-now-commonplace-for-balkan-women-reporters/
- ATINA Citizens` Association for Combatting Trafficking in Human Beings and All Forms of Violence against Women, Behind the screens: Analysis of human trafficking victims` abuse in digital surroundings (2020) Available online at: http://www.atina.org.rs/sites/default/files/Behind%20the%20screens%20Analysis%20of%20human%20trafficking%20victims%27%20abuse%20in%20digital%20surroundings.pdf

1. A Case Study from Albania:

UNDERSTANDING GENDERED CYBERVIOLENCE AND DISCRIMINATION: “WHO’S TABU?”

VASILIKA LACI AND HVALE VALE

1. A Case Study from Albania: **Understanding gendered cyberviolence and discrimination: "Who's Tabu?"**

Vasilika Laci[29] and hvale vale

Introduction

Gendered cyberviolence and discrimination, cybersecurity, and governance. Three terms, three universes of practices. Do they cross paths with each other? Are they speaking to the same or different audiences? Is the language used being cryptic and obscure? Is it separated from the lived realities of citizens? Are cybersecurity governance mechanisms accounting for and responding to people's embodied experiences regardless of their gender, power, privileges, age or ability class? Is online gender-based violence (GBV) acknowledged beyond the binary of women/girls and men/boys? Are women and gender-diverse people equally consulted, and offered protection and remedies when cyberthreats occur?

This case study tries to reunite these terms under one roof: the rule of law, human rights and good governance practices. It explores the way a country's relevant institutions and bodies work together to respond to cyberthreats, and suggests ways forward where gaps exist.

Since the field is vast and multi-layered, some general working definitions are needed to set our landscape. The space is the internet, the network of networks we all use and know (or many of us use and mostly know), and the terms we seek to define are governance, cybersecurity and cyberviolence.

Governance: "The act or process of governing or overseeing the control and direction of something (such as a country or an organisation)."[30]

Cybersecurity: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment."[31]

Gendered[32] cyberviolence and discrimination, or alternatively `online gender-based violence`:

[29] The authors of this paper wish to thank Vasilika Laçí for her generous support and voluntarily contribution in co-authoring this case study. Vasilika Laci`s knowledge of the context, language and politics in relation to this case study, as well as her friendship and trust, made this research possible.

[30] Merriam- Webster Dictionary (2021) Governance, available online at: www.merriam-webster.com/dictionary/governance

[31] International Telecommunication Union (ITU) Definition of cybersecurity, ITU-T X.1205 (2021), available at: www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[32] "Gender refers to the roles, behaviors, 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. Significantly, gender constructs determine who holds power, whether in families, societies, and even in global affairs." Deborah Brown and Allison Pytlak, Women's International League for Peace and Freedom and the Association for Progressive Communications, Why Gender Matters in International Cyber Security, Section II: Framing, (2020) Available at: www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf

"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. 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 by 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, use of language and insults that are highly gendered – misogynist or anti-gay rhetoric, threats of rape, etc."[33]

Tabu[34] – A story of love and self-defence

Zhaklin Lekatari is a woman in the Albanian online public arena who has built her own space and created a voice for the issues that matter to her. She responds to and rejects the hate, threats and bullying she receives daily. She is a journalist, a sex educator and a human rights activist. Five years ago Zhaklin launched Tabu, a blog that talks about sexual education, feminism and Lesbian-Gay-Bisexual-Transgender-Queer-Intersex -Asexual (LGBTQIA+).[35]

As Zhaklin told us, "I came out from a bad break-up, and when I healed and rose again, I wanted to do something useful. I was in my early thirties, I knew who I was and I knew what I wanted. And I thought of younger women and girls. How would they respond, how would they know what to do? It is not easy to respond under pressure. You make a bad decision, or you do not decide but you find yourself in trouble. It is important that women and girls understand that a mistake is not the end of the world, that people can move on. I thought it was important to say that we have the right to love ourselves. This is why I started Tabu."

When Zhaklin launched Tabu in 2015 she was working as a TV and radio journalist. Tabu was a project she had wanted to implement for a while, but no one seemed interested, no one "trusted her ability to do it" - and so she decided to go for it on her own. Once launched, it went viral. Men in particular were her followers online, because as Zhaklin puts it, they thought "she would be easy to reach" for them. "I was the new bitch in town." It took more time to "get women's hearts, it is difficult to reach the heart of Balkan women", says Zhaklin. "Women do not trust women in Albania: it is a cultural thing, we do not support each other, there is this thing of shaming and judging, especially by older towards younger women".

Zhaklin talks about sexuality, everyone's sexuality, during the daytime on her blog, her YouTube channel, her Instagram account and her Facebook (FB) page. She uses language in a society where silence reigns and "you asked for it" is the most common response.[36]

From the start, the comments that Zhaklin received on her different online channels have ranged from being distasteful to being full of hate. As Zhaklin says, statements include: "you are bringing shame to Albanian women" ,"you are not a woman at all", "look at your hair, look at your face, you are ugly, awful, you are degenerate, you want people to have orgies." She

[33] Ibid.

[34] Zhaklin Lekatari, Tabu Blog (2021), available at: tabu.al/kontakti/

[35] LGBTQIA+ is being used here as an abbreviation for Lesbian, Gay, Bisexual, Transgender, Queer, Intersex and Asexual communities, the + is to intentionally acknowledge, include and raise awareness of the myriad of other communities under this umbrella term. For more information see: It Gets Better Project, LGBTQ+ Glossary (2010). Available at: https://itgetsbetter.org/blog/lesson/glossary/ and The Safe Zone Project, LGBTQ+ Vocabulary Glossary of Terms (2013). Available at: https://thesafezoneproject.com/resources/vocabulary/

[36] Tabu Albania, FB page (2021), available at:www.facebook.com/tabualbania/

has been accused of being a “feminazi” and called “incompetent”; some wanted to silence her, other would comment that they would “show her what real/good sex is.” People are hateful for no reason, as she explains: “I am constantly blackmailed by people who say I have your photo, pictures ... I will share this and that of you.”

“I am just a normal woman, being myself. Sexual education is about morals, ethics, health, everything. It is about understanding who we are, it is about getting in touch with ourselves, our bodies. Sex education makes people better, it helps you become a human being. Sexual education is about more than the act of intercourse, a lot more.”

The hate is a constant presence, but some posts get higher spikes. Those that attract the most hate can be grouped under a few categories: Posts talking about men’s sexuality or men’s sexual problems, and posts criticizing the behaviour of men towards women.

Posts that address womens` conditions and the gender gap are another red flag – indeed, posts about gender are the most hated, as Zhaklin says, and receive the most negative backlash. Posts on LGBTQIA issues also attract a fair share of hate. But Zhaklin is attacked any time she comments on reality, be it any subject, like traffic or taxes. The hate hits hard. She is reminded that she is online to talk about sex, that she is a “bitch” and “what would a bitch know of traffic, or taxes?”

Recently, Zhaklin found her FB page suspended. She had publicly spoken in favour of a homophobic and misogynist website being taken down by the Albanian authorities. In response, groups of organised homophobic and misogynistic users reported her page to FB, claiming it violated FB policies and distributed content forbidden by FB community guidelines, such as `pornography`, `hate speech` and others. This is not an uncommon practice. In recent years, many activists, organisations and groups have had their accounts and pages suspended and thereby access to their audiences blocked because of organised campaigns falsely reporting/accusing them of not using their real name, spreading antisocial messages, etc. This practice relies on the fact that FB does not always understand the language, or the culture concerned. When FB bans a page, the burden of proving that the page in question did not violate FB community guidelines is on the page owner. Once suspended, the page owner has few alternatives. They can wait for the suspension period to pass, comply with the FB request if the case relates to a specific post or provide proof of identity, if the suspension is based on the requirement for users to use their real name. This real-name policy is especially frequently used against non-binary and trans activists as a way to “out” them and to intentionally misgender them. Sometimes a counter-campaign is organised by the suspended page owner on the same or on sister platforms, such as Instagram, asking for the page to be reinstated and explaining that the owner was not violating any community guidelines, but had instead become the target of a mischievous attack with the purpose of censoring and silencing the page owner.

Zhaklin explains her response as instinctive, as stubbornness: “I was mad. I was so angry. I could not describe myself otherwise. I was beside myself to see and read all of this. I fought back. I did not think. I did not try to be strategic, I just reacted. I responded strongly. They were bullying me, so I was bullying them back. I was saying things like ‘one day you will find someone that is a bigger bully than you and you will be crushed’. I was responding with strong comments. Some of my friends said I was wrong, but I could not act otherwise. Then I realised that Albanian people are used to, and immersed in, a language of violence ... So, I thought, this is the language they understand, and now looking back I think that somehow bullying them back had worked. I do not know if this is the right way, or if there is a right way to manage this kind of constant attack. This is my way. I will not be broken by their messages. I will stand for my work, my time, myself.”

Now, after five years online, Zhaklin has a support group, her “fandom” – consisting of people she has met online, other bloggers facing similar problems, people she has met at events, activists, and friends. When things get bad, when she receives many hateful comments on a post, she shares the link on their WhatsApp group and the counteraction starts: positive posts, supportive comments. As Zhaklin admits, not having to fight alone and knowing that someone is there for you helps. She is also often approached by young girls and women, asking her to help when someone stalks or pressures them, and they do not know how to stop it or how to respond.

Zhaklin has tried to report her attackers. She has used, and still uses an application called the "digital police",[37] to which users can complain about online misbehaviour and send messages, pictures, information and contact details. She has never in all these years gotten a response from the digital police application.

The only time she went to the police in person was in the summer of 2020. She had been contacted via Instagram by a person who had illegally gained access to her digital birth certificate and all her relatives' birth certificates. Birth certificates are stored on an official website as part of the e-government service that Albania has developed. Every citizen has a personal login to access and download personal documents, such as birth certificates, and this service is designed to be accessible only to the owner. The way this person spoke made Zhaklin realise that they knew a lot more about her and the people close to her, so she went to the police to press charges. The answer was discouraging. The police officer said that it was not for the police to open the case, but for the prosecutor's office. Even though he could see she was scared, he did not think the prosecutor would open a case: the unlawful access to her personal data and electronic birth certificate did not qualify as a "threat" but as an offence.[38]

Six months later, Zhaklin received a blue envelope from the prosecutor's office informing her that an investigation would not be opened because the authorities did not regard this action as a "threat," as had been anticipated by the police officer who had first received Zhaklin's complaint. Discouraged by the dismissal, Zhaklin did not pursue additional legal mechanisms, but did not surrender either. She went one step further and met with the Tirana's mayor's office to call for a public campaign against online bullying. But as she explains: "It is difficult to make people collaborate. I would like to see an institutional response at both local and national levels. A campaign saying that bullying is not OK, that hate speech is not OK, and can be sanctioned and punished. I would like to see justice. I would like to see these people punished, stopped."

We asked Zhaklin if she feels tired of always being on the edge, always on alert, and asked where she goes to rest and recharge. She paused, nodded, and answered: "It is tiring, but I have me, myself. I have the education and the information that help me to shift my mind and stop thinking about all the comments. Me and my life are more important than all of them!"

The cultural context

The official data on violence against women and girls in Albania revealed that 52.9% of women had experienced one or more of the following five different types of violence: 47% reported experiencing intimate partner domestic violence; 65.8% dating violence; 18.2% non-partner violence; 18.1% sexual harassment; and 12.6% stalking. In addition, 3.1% reported having been sexually abused as children, and 36.6% of women said they were 'currently' experiencing violence.[39]

[37] Policia Dixhitale in Albanian.

[38] OneTrust DataGuidance – Regulatory research Software Albania – Data Protection Overview (2021) available at: www.dataguidance.com/notes/albania-data-protection-overview;
Council of Europe Repository, Law No. 9887 dated 10.03.2008, On Protection of Personal Data (2021), available at: rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806aef6d

[39] UN Women Europe and Central Asia, Improved data on violence against women catalyses advocacy and legal change in Albania (2020), available at: eca.unwomen.org/en/news/stories/2020/8/improved-data-on-vi-

If we consider that 82.2%of the Albanian population have access to the internet[40], and that the internet reproduces and amplifies offline reality, one can see how the majority of women and girls are exposed to a continuum of violence. In 2017, the European Institute for Gender Equality report on "Cyber violence against women and girls" found that "one in three women will have experienced a form of violence in her lifetime, and despite the relatively new and growing phenomenon of internet connectivity, it is estimated that one in ten women have already experienced a form of cyber violence since the age of 15." [41]

There are some encouraging steps that engage technology to respond to and support victims/survivors, such as the recent development of an app called GjejZâ[42] (Albanian: "Find your voice") which fights GBV. It is programmed by three teenagers, Arla Hoxha, Dea Rrozhani and Jonada Shukarasi, known as the D3cOders. The app, which focuses on domestic violence, has three main sections (Identifying the Problem, Empowering the User, and Taking Action), and the menu helps the user to identify the problem and provides the names and contacts of institutions to ask for more information and/or help. The intention is to give victims/survivors a practical tool that can help them articulate the abuse and look for support. So far, the app has been downloaded by more than 500 users. If successful, it could be further supported and connected with services such as GBV hotlines, or the police.

The ways in which media discriminates against women, especially in the representation of women on TV, constitutes structural discrimination[43] in the sense that it places barriers in the path of women to the enjoyment of their rights and opportunities. Experts on the topic state that reporting on GBV by the media further victimizes the survivors. Sexual assaults are widely undisclosed for fear that someone from the media will find out and make the information public. Reporting often deals with the cause rather than the consequences, and in many cases the headline has nothing to do with the actual content of the story. Victims are often portrayed as the guilty party.[44]

"Nevertheless, public opinion in Albania lacks a gendered understanding of violence against women and tends to view violence restrictively as a by-product of low socio-economic development."[45]

olence-against-women-catalyses-advocacy-and-legal-change-in-albania ; UN Women Europe and Central Asia, Violence Against Women and Girls in Albania, 2019 available at: eca.unwomen.org/en/digital-library/publications/2019/05/violence-against-women-and-girls-in-albania

[40] INSTAT (2019) "Survey on information and communication technologies (ICT) usage in households and by individuals in 2018-2019" (2019), available at: instat.gov.al/media/6436/survey-on-information-and-communication-technologies-ict-usage-in-households-and-by-individuals-in-2018-2019.pdf

[41] European Institute for Gender Equality EIGE, Cyber violence against women and girls (2017), available at: eige.europa.eu/publications/cyber-violence-against-women-and-girls

[42] UNICEF, Three teenagers in Albania develop an App that fights gender-based violence,(2020), available at: www.unicef.org/eca/stories/three-teenagers-albania-develop-app-fights-gender-based-violence

[43] Article 6 of the Law on Protection from Discrimination, No. 10221/4.2.2010, as amended by Law No. 12/2020.

[44] Zëri i Amerikës, Shqipëri, pasqyrimi në media i dhunës me bazë gjinore (Albania, reporting of GBV in the media – Interviews with Iris Luarasi and Majlinda Angoni), 2018, available at: www.zeriamerikes.com/a/4279081.html

[45] Arkiva Inovacioni Albania, Ligj nr 9918 date 19 5 2008 Per komunikimet elektronike ne Republiken e Shqiperise perditesuar me Ligjin nr 102 date 24 10 2012, (2012), available at: arkiva.inovacioni.gov.al/mitik/legjislacioni/Ligj_nr_9918_date_19_5_2008_Per_komunikimet_elektronike_ne_Republiken_e_Shqiperise_perditesuar_me_Ligjin_nr_102_date_24_10_2012.pdf

Relevant legal and governance framework

Albanian law does not regulate online GBV directly, but Article 108/a of the Penal Code states that "Committing sexual acts that violate the dignity of a person, by any means or form, creating a threatening, hostile, degrading, humiliating or offensive environment, is considered a criminal offense and is punishable by imprisonment of one to five years."[46] Gender constitutes an aggravating circumstance (Article 50, point j, of the Penal Code of Albania, 1995/Updated). It is noteworthy that definitions on incitement of hatred or quarrels do not make a differentiation on grounds of gender.[47]

Recent changes in the Law on Protection from Discrimination have added sexual harassment as a form of discrimination.[48] This law defines sexual harassment as unwanted behaviour, verbal or non-verbal, of a sexual nature, which has the purpose or effect of violating the dignity of the person and creating an environment of intimidation, hostility, contempt, humiliation or offence. These legal changes entered into force on 15 October 2020, and there has not yet been time to monitor their implementation thus far.

The National Strategy for Gender Equality in Albania 2016–2020 does not provide measures to address the issue of online harassment. Though it claims zero tolerance for GBV and aims to decrease societal tolerance of such acts, it has not planned any concerted action on the online manifestation of GBV. This is one indicator of how little understanding there is of this type of violence and how it affects, harms and pushes women to self-censor in the internet sphere. As this strategy ended in 2020, there is now an opportunity to analyse the scope and impact of sexual harassment on women and girls, and measures that could be taken to address this issue.

The Albanian cybersecurity governance model and legal framework

Albania ratified the Convention on Cybercrime in 2002, and this has subsequently been incorporated in various laws of the criminal code. In 2014 the government, led by the Ministry of Infrastructure and Energy, launched the "Albanian Digital Agenda 2015–2020". A new action plan, revised in March 2020, is still pending approval by the Council of Ministers.[49]

In 2014 the Ministry of Defense approved the first Strategy for Cyber Defence, followed in 2015 by the Document on Cyber Security Policy (2015–2017). The new national cybersecurity strategy drafted by the National Authority for Electronic Certification and Cyber Security (NAECCS) was not yet adopted at the time of writing.

Albania strives for a multi-stakeholder approach to cybersecurity,.[50] Two basic concepts are highlighted in a paper by Desara Dushi on collective responsibility among all users of cyberspace:

[46] Kodi Penal I Republikës Së Shqipërisë, Added Article 108/a with Law No. 144, dated 2.5.2013, Article 24, (2016), available at: www.pp.gov.al/web/kodi_penal_2016_1033.pdf

[47] Kodi Penal I Republikës Së Shqipërisë, Article 256, "Incitement of hatred or quarrels" (amended by Law No. 144, dated 2.5.2013, Article 41), (2016), available at: www.pp.gov.al/web/kodi_penal_2016_1033.pdf

[48] Albanian Parliament, official website, Ligjnr. 124/2020 Për Disa Shtesa Dhe Ndryshime Në Ligjin Nr. 10221, Datë 4.2.2010 "Për Mbrojtjen Nga Diskriminimi" (additions and amendments in the Law on Protection from Discrimination No. 10221, dated 4.2.2010), (2020). Available at: www.parlament.al/Files/ProjektLigje/20201020143441ligj%20nr.%20124%20dt.%2015.10.2020.pdf

[49] European Commission, Brussels, 6.10.2020, Albania 2020 Report, SWD 354 final, Commission Staff Working Document (2020), available at: ec.europa.eu/neighbourhood-enlargement/sites/near/files/albania_report_2020.pdf

[50] Desara Dushi, Cybersecurity in Albania: A multi-stakeholder approach (2017), available at: www.researchgate.net/publication/315495692_Cybersecurity_in_Albania_a_Multistakeholder_Approach

- collaboration and coordination among all stakeholders, and
- international cooperation.[51]

Cybersecurity governance in Albania is a crowded space. The Ministry of Defense has an oversight role, and other key actors are the Albanian State Police and Cybercrime Investigation Unit, who are responsible for cybercrime incident response; the National Authority for Electronic Certification and Cyber Security, incorporating the National Computer Incident Response Team, which is the coordinating body with responsibility for protecting Albania's national network, public awareness raising on protection against harassment, etc.; the Authority of Electronic and Postal Communications; the National Authority for Electronic Certification; and the National Agency for Information Society. Albania has a distributed set of cybersecurity provisions in various laws: the Criminal Code, the Electronic Communication Law and Personal Data Protection Laws, which, according to the Cybersecurity Capacity Review of Albania, constitute "the most relevant legislative frameworks and guidelines related to Albania's Internet landscape."[52]

A specific mention must be made of amendments to the Law on Audiovisual Media and the Law on Electronic Communications.[53] The former were at the centre of a successful campaign organised by journalists, members of the media and civil society to contest the institution of a Complaints Commission within the AudioVisual Media Authority. The Commission would have been able to review content produced by online media, thus creating a dangerous precedent and giving rise to content censorship, limiting freedom of the media, including bloggers. In January 2020, following a negative opinion of the Venice Commission which underlined the risk such a commission would pose to media freedom, the parliament voted to not amend the Law on Audiovisual Media.

[51] Ibid.

[52] List of relevant laws:

- Law No. 7895 of 27.01.1995, Criminal Code of Albania
- Law No. 7905 of 21.03.1995, Criminal Procedure Code of Albania
- Law No. 9918 of 19.05.2008, On Electronic Communications
- Law No. 9887 of 10.03.2008, On Protection of Personal Data
- Law No. 8888 of 25.4.2002, Ratification of "Convention on Crime in the Cybernetic Area"
- Law No.9880 of 25.02.2008, On Electronic Signature
- Law No.10128 of 11.05.2009, On Electronic Commerce.
- Law No. 9643 of 20.11.2006 amended, On Public Procurement that Enables Electronic Procurement
- Law No. 9723 of 3.5. 2007, On Registration of Businesses at the National Centre of Registration
- Law No. 10273 of 29.4.2010, On Electronic Documents
- Law No. 2/2017, On Cyber Security

Law No.107/2015, On Electronic Identification and Trust Services

Global Cyber Security Capacity Centre and Oxford Martin School, University of Oxford, Cybersecurity Capacity Review of Albania (2018), available at: cesk.gov.al/Publikime/2019/AlbaniaCMMReport.pdf

[53] Balkan Investigative Reporting Network in Albania "Internet governance in Albania and its role in media freedom", July 2020. Available online at: https://birn.eu.com/wp-content/uploads/2020/08/Internet-Governance-1-1.pdf

Best practice and gaps in the legal and governance framework revealed by the case study

- **"... gender can be analysed as an abstract system of power and representation through which the dominant, hegemonic forms of masculinity are negotiated. Here, gender remains implicit because the institutions, constituencies and issues appear deceptively gender-blind"**[54]

While preparing and researching for this case study, what struck us the most was the perception of two parallel and disembodied worlds.

There is the world of Zhaklin, who shared her past and current experience of safety on the internet. Her story typifies and echoes the experiences of many other female-identifying journalists in Albania and the Western Balkans, who experience online violence but find it difficult to get access to justice.

For example, Law No. 2/2017, "On Cybersecurity", protects communication networks and information systems, "the violation or destruction of which would affect the health, safety, and/or economic well-being of citizens and the effective functioning of the economy in Albania", but seems unable to extend protection when the exercise of individual rights is in question.

Similarly, Law No. 8888, following the ratification in 2002 of the Convention on Cybercrime (Budapest Convention), introduced into the Criminal Code activities such as unauthorized access (hacking) (Article 192/b/1), possession of hacking tools (Article 293/c/1) and denial-of-service attacks (Article 293/c). However, it does not seems to be consistently used or promoted as part of the institutional response against online GBV.

Moreover, there are offences relating to computer systems that are punishable under the Criminal Code, such as hate crimes. But in the Criminal Code gender is grouped along with ethnicity, nationality, race and religion. It is only under data protection laws that data on sexuality or sexual orientation are named and labelled as sensitive in relation to a social identity.

In contrast, there is the arena of national Cybersecurity with its capital C, concerned with critical and important infrastructure, "cyber warfare" and large-scale attacks that can derail trains, wipe data centres and create blackouts. This is a world where states need and depend on corporate knowledge to assess, prevent and respond to attacks; a world that advocates for acquisition and monitoring of large datasets and data flows, surveillance, suspension of rights and secrecy behind closed doors. But breach and violation of citizens' personal data do not seem worth opening a case for, or even redirecting a complaint to the competent authority.

Then there is the world of GBV, which most of the time is reduced to domestic violence and violence against women and girls. These worlds seem to have no contact with one another. Even if the violence is perpetrated through technology, they never seem to intersect. There is a historical reason for this: security of the state and citizens are seen as a public issue, while violence against gendered citizens (females) until 50 years ago – was considered a private issue. It is only as a result of struggles by feminist and social justice movements that violence against

[54] Heike Jensen GISWatch, Gender and ICTs, Whose internet is it anyway? Shaping the internet – Feminist voices in governance decision making, (2013) available at: giswatch.org/institutional-overview/womens-rights-gender/whose-internet-it-anyway-shaping-internet-feminist-voice

women and more recently GBV[55] were brought first into the realm of human rights, later into the domain of legislation, and eventually labelled as a public issue.[56]

The internet and its infrastructure have been mainly regarded as an economy whose assets and capital need protection. It is no surprise that the original definition of cybercrime concerns the interests of banks and protection of their transactions. It is thus understandable why the cybersecurity/cybercrimes sector looks at systems and infrastructure as assets to be protected, regulated and maintained, but that these are viewed as detached from the human security dimension.

From our limited review of legislation and strategy the possibility for a person to access and exercise their individual rights seems to be relegated to being just one last option at the end of a long list of cases.

The kind of cybercrimes addressed by cybersecurity national bodies are gender-blind in their definition and understanding. In our reading we were not able to find any reference that could point out to a recognition which elevates online GBV to the realm of cybercrime definition and response, despite the fact that they are perpetrated using the very same technological tools. As seen from the definition below, acts of online gender-based violence equate to:

Acts of gender-based violence that are 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.[57]

If the cybersecurity sector is really willing to provide the best frame and protection to its citizens, it is imperative for a reflection and understanding of the role which gender plays to be incorporated. In its simplest and binary definition, this should at least address the structural discrimination suffered by half of the population (women) whose interests and assets cannot be discarded by the argument of infrastructure or technology neutrality. The biases, as we will explain in more details further in this case study, have been inherent to decision makers and industry, and are heavily embedded in patriarchy and patriarchal beliefs.

Listening to Zhaklin, we realise that the question of governance, with its emphasis on accountability, transparency and participation of all actors, might offer an alternative to the current mainstream cybersecurity model. Zhaklin's story reveals and voices the disconnect

[55] "Association for Progressive Communications (APC), From impunity to justice: Exploring corporate and legal remedies for technology-related violence against women (2015). Available at: https://www.genderit.org/onlinevaw4 ; citing, in its footnote 3: 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, available at: https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf
"While APC initially used the term "technology-related violence against women" (see https://www.genderit.org/onlinevaw), more recently we refer to "online gender-based violence" to communicate our intersectional understanding of violence against women which considers race, class, sexuality, age and other locations, to be able to reflect the findings of research on sexual rights and the internet (see erotics.apc.org) and also, because the term "online" has become more commonly understood and used. It must be noted, however, that we deliberately chose to use "technology-related" versus "online" or "on the internet" until 2015 in order to a) recognise that this violence can affect women who are not "online" themselves; b) incorporate those experiences that were impacted by digital technologies that did not make use of the internet, such as digital recordings, sharing via Bluetooth or other means, etc. (see for example the case study from Pakistan, "When a sex video is used as blackmail", available at https://www.genderit.org/sites/default/upload/case_studies_pak3_1.pdf); and c) avoid falling into a binary of online vs. offline violence that can feed the perception that these expressions of violence are distinct and separate from systemic gender-based discrimination. Although we use the term "online" currently, it incorporates these considerations as well. We argue that more work needs to be done to describe this type of violence in order to reflect this multiplicity of experience"

[56] Shazia Qureshi, "Feminist analysis of human rights law", Journal of Political Studies, Vol. 19(2) (2012)., pp. 41-55,

[57] Association for Progressive Communication, 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, available at: https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf

between the reality of routine harassment, of diminishing and threatening someone online because of their gender and in a gendered way, and the highly specialised cybersecurity sector administered by the state. A cybersecurity sector currently "run" by large private companies, which remains inaccessible to citizens. This creates an awkward hierarchy where threats to money and data are far more important, and prioritized in terms of identification and prosecution, compared to threats experienced by citizens. Existing gender discrimination is dismissed when the intent to intimidate, harass or use violence is directed at women or people of diverse genders and sexualities.

What Zhaklin's story tells us is that national, as well as global, conversations and hype about cybersecurity miss both the human aspect of security and the gendered aspect of cyberthreats. It is this piece of the conversation that we bring to the table: we need inter-ministerial and truly multi-stakeholder processes where each stakeholder plays its part. Access to justice and human rights have to apply across the board of national cybersecurity. We need to make visible and then discard the hidden hierarchy of cybercrimes that consider gendered/online cyberviolence as separated from the overall state cybersecurity response and governance model.

Showcasing the gender equality gap is always a complex exercise. Absolute numbers only scratch the surface and refer to the binary of women/men and girls/boys. Until a new model of structuring statistical data that considers gender more fluidly emerges, we can use and cross-reference sets of data provided by INSTAT, the Albanian statistical office, in its annual "Women and Men" reports[58] and its 2018 report on "Violence against Women and Girls".[59] Three sets of data are of particular interest to our case, taken from INSTAT's "Women and Men". We report here on the sets on education, crime, and criminal justice decision-makers.

The first set of data shows that women represent 66.4 % of graduates (2018/2019), despite a negative trend of 6.6% compared to the previous year. If we look at ICT studies, we see that in 2019, 45.7 % of graduates were female, and 54.3 % male. The difference is that while ICT studies are the third most preferred option for males, with 8.6 % enrolling, for females it is among the least preferred, with 3.7 % enrolling.

The second set of data shows us gender in police structures, with the number of female employees equal to 14.5 %. The trends show a gradual increase in women among lower-grade employees. At higher levels women make up 43.7 % of inspectors and only 11.4 % of deputy commissioners. If we look at civilian personnel, women are in higher numbers.

The third set on decision-makers shows 29.5 % of women parliamentarians compared to 70.5 % of their male counterparts. If we look at the participation of women in commissions, they are mostly represented in the Commission for Labour, Social Affairs and Health (with 44,4%) while in the Commission on National Security only 26.3 % are women, as opposed to 73.7 % men. The overall gender balance in managerial positions is 34.7 % women versus 65.3 % men.

Numbers are telling us that there is a gap, but this is just half the story. The lack of gender representation cannot be understood and addressed if it does not touch upon or analyse the underlying causes that perpetuate existing discrimination, how they are entrenched in individual and collective consciousness and behaviour, and how they are then reproduced in legislation, policy and governance structures to create a vicious circle of injustice and an absence of institutional remedy.

[58] Institute of Statistics (INSTAT) Albania, "Women and Men" (2020) available at: www.instat.gov.al/media/7376/burra-dhe-gra-2020.pdf

[59] INSTAT, Violence against Women and Girls in Albania 2018, available at: http://www.instat.gov.al/en/statistical-literacy/violence-against-women-and-girls-in-albania/

For all these reasons we need to understand the combined role played by the gender gap, gender bias, gender stereotypes, patriarchal control and patriarchal belief,[60] to name just a few underlying causes that perpetuate the existing power disparity between genders. This disparity is not going to dissolve just by simply increasing the number of the less represented gender – or in our case an increased number of female bodies in the various sectors of our society.[61]

We need to change the paradigm that informs social norms as well as legal norms. Two useful gender frameworks, one published in 2005 (Gender Evaluation Framework - GEM) and the second in 2013 (Gender at work framework), apply gender analyses specifically to the intersection of gender and ICTs. Regardless of the passage of time, they are both very helpful in understanding why certain strategies address only the gender gap and why structural discrimination, cultural norms and patriarchal beliefs not addressed will fail in their stated intent. They also offer concrete, rigorous, and tested tools to institutions that are willing to try and change the status quo.

The 2013 framework is taken from an article by Joanne Sandler, part of the GISWatch publication "Gender and ICTs", wherein Sandler applies a gender at work framework to "generate a broader view of some of the options, opportunities and challenges for advancing and protecting women's human rights online."[62]

Two texts published in 2002 and 2005 have pioneered a Gender and ICT framework, one written by Sara Longwe,[63] "Spectacles for seeing gender in project evaluation", and one by Peregrine Wood, entitled "Gender and information and communication technology: Toward an analytical framework". Fifteen years after these publications, GEM provides a still relevant theoretical framework to address the intersection of gender, the internet and ICTs.[64] Both publications show how the online world is a continuum of the offline world, where patriarchal norms and gender discrimination applies the same way, but where online spaces are amplifying and accelerating the harm and negative impacts. All the underlying causes that are integral to the existing structural gender exclusion mean that women's experience of cyberthreats and violence online is not considered relevant. Women who have experienced this problem and are actively and publicly dismantled, and their interests are not consulted or included where decisions on cybersecurity strategy and policy are being made. In a world where women's experience and knowledge are not considered relevant, and regulations and laws are not designed with them in mind, it is not difficult to imagine how all the complaints and requests directed by Zhaklin to the police and the prosecutor were dismissed.

If we want women and men to have equal opportunities to participate in the provision, management and oversight of cybersecurity governance we need more women to be active and present where strategy, policy and decisions are made. We also need a better analysis of the gendered aspects of cybersecurity.

If we want cybersecurity frameworks to extend to the everyday lives of women/girls and to

[60] "Patriarchal belief is the system of belief that serves to legitimise male domination and gender discrimination. It relies on patriarchal interpretations of biblical/religious texts, beliefs in male biological superiority (sexism) claiming that the unequal gender division of rights and duties is either natural (biological), or God-given, or too difficult to change because they are irretrievably embedded in culture.." Sara Longwe, "Gender evaluation methodology for internet and ICTs. A learning tool for change and empowerment", (2005). Available at: https://assets.publishing.service.gov.uk/media/57a08c5ae5274a31e000116e/GEMEnglish.pdf

[61] Jensen, noted above.

[62] Joanne Sandler, GISWatch Gender and ICTs, "The online terrain for women's rights" (2013), giswatch.org/en/report-introduction/online-terrain-women-s-rights

[63] Sara Longwe, 2021 available at: genderlinks.org.za/about-us/who-we-are/board-of-directors/sara-longwe/

[64] Association for Progressive Communication (APC), "Gender evaluation methodology for internet and ICTs. A learning tool for change and empowerment" (2005). Available at: https://assets.publishing.service.gov.uk/media/57a08c5ae5274a31e000116e/GEMEnglish.pdf

make it possible for women to access justice when their security is threatened, we need a gender lens to review and include the human and gender component of security side by side to the current cybersecurity. We need to make sure that the knowledge and means allocated to the cybersecurity sector are accessible and accountable to female researchers, journalists and all women and girls; it must not remain inaccessible behind a male "power wall."

While we admire Zhaklin's strategy of survival, her braveness and resilience, the absence of any institutional response is astonishing. Over the years, Zhaklin has experienced various forms of attack, from hate speech to defamation, discrimination, intrusion of privacy and personal data breach. As she states, such online violence and cyber bullying should receive zero tolerance, and perpetrators should be identified and sanctioned.

While looking at the various gender and cybersecurity frameworks, a few other points emerge. Defamation, for example, is still punishable by a fine in Albania.[65] Although it is mostly used by people in power to silence and threaten their opponents and journalists, it could be argued that the years of abusive messages and threats that Zhaklin has collected, and the many other women who receive the same as a way to threaten and silence them, might be worthy a moment of reflection. If, on the other hand belittling and smearing is not deemed to be "so threatening", could it instead be seen as defamatory? It is important to be aware of the objection and concerns civil society actors and the media have against the instrumental and censoring use of "defamation" by powerful actors. It might be interesting, as an exercise, to apply the defamatory framework to the comments which Zhaklin, as well as countless other women and gender diverse people are receiving. The comments and messages are surely untrue, yet intentionally aim to target and disqualify the victims of such attacks. These are all elements that resonate with defamation.

The organised response and mobilisation of journalists and rights-based organisations against the amendment to the new Law on AudioVisual Media opens up an interesting reflection.

First, due to the concrete risk to the freedom of media, independent journalists and bloggers have created an awareness around the internet ecosystem and its governance. A report on "Internet governance in Albania and its role in media freedom"[66] produced by the Balkan Investigative Reporting Network in Albania demonstrates a change of attitude towards internet governance. The study positions itself as a useful toolkit offering an updated and extensive look at the internet governance ecosystem while privileging the multiple intersections between media development and internet governance. It has a specific aim "to inform involved stakeholders and the public debate", and adds that "when the abuse or poor definition of these regulations leads to restrictions on freedom of the media and on freedom of expression in the country" it can become useful for raising awareness among various stakeholders, helping them to understand the intersection between their struggles and issues of national governance of cyberspace.

While the BIRN report mentions that "a rising number of defamation lawsuits, orchestrated smear campaigns and verbal attacks, sometimes coming from the highest echelons of power, both offline and online, have created an environment in which journalist often resort to self-censorship and avoid coverage of sensitive topics", what is missing is an explicit mention of the gender dimension of the threats and violence suffered by female journalists.

The education and information that this report offers about the internet ecosystem and its

[65] Defamation is defined as "Intentional distribution of untrue data and of having full knowledge of the untrue nature of the data for the purpose of infringing the dignity and the honour of another person." Punishments can vary from 50,000 to 1,500,000 leks (€400–12,000). Civil Code of the Republic of Albania, Balkan Investigative Reporting Network in Albania, Internet governance in Albania and its role in media freedom", July 2020.Available at: qbz.gov.al/preview/f010097e-d6c8-402f-8f10-d9b60af94744

[66] Ibid. Balkan Investigative Reporting Network in Albania

governance could open the door to new actors engaging in other internet governance areas, such as cybersecurity, which intersects with rights such as access to information, privacy and surveillance.

Recommendations for decision-makers and legislators of the Albanian Cybersecurity Institutional ecosystem and in particular:

the Ministry of Defense, National cybersecurity strategy drafted by the National Authority for Electronic Certification and Cyber Security, Cybercrime Investigation Unit, the Albanian CERT and National Agency for Information Society, Albania

- Actors responsible for the development of a new strategy should apply a gender lens when identifying issues, and include their recommendations in national strategies and any other documents.

- In the short term create open spaces for discussion and knowledge sharing, and in the longer term promote a national programme or devise financial mechanisms for awareness raising and education, training and skills on gendered cyberviolence and cybersecurity for girls and women as well as the public and civil society.

- In the short term create open spaces for discussion and knowledge sharing, and in the longer term promote a national programme or devise financial mechanisms for awareness raising and education, training and skills on gender cyberviolence and cybersecurity addressed specifically at the needs of prosecutors, police officers, expert bodies and decision-makers in developing strategy and policies on cybersecurity and/or gender.

- Introduce an analysis of the legal mechanisms and protections from cybercrimes, including GBV and online violence and harassment based on other vulnerabilities/aspects as manifested in the Albanian society. Promote awareness among the public on the changes provided in this law and the potential remedy avenues to survivors of sexual harassment. Publicising legal avenues can offer women and girls who are more frequently the target of such harassment, but also all citizens at large, the possibility to make use of protective standards already in place.

- Translate the 11 voluntary norms of the 2015 Report by the United Nations Group of Government Experts on developments in the field of information and telecommunications in the context of international security into Albanian language, and implement the information as a collaborative learning exercise. This will help illustrate the 11 voluntary norms in the specific Albanian context. Simultaneously within this context it would be helpful to run a participatory gender analysis exercise with all interested parties / stakeholders from gender mechanism representatives, women's rights organisations active in field of security; regulators and technical community.[67]

[67] UN General Assembly UN Doc. A/70/174, 22 July 2015,Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security, Section III, para. 13 (a)-(k). Available at: undocs.org/A/70/174

- Engage in a process to review the existing framework and mechanisms through a gender lens, and develop a gender analysis of Albanian cybersecurity mechanisms, policy and strategy with the inclusion of women journalists, women IT professionals and women from academia.

Ministry of Health and Social Welfare

- Expand the National Strategy for Gender Equality and Action Plan, Objective 4.4, on "Raising societal awareness on the acceptance of gender equality as a necessary condition for the development of the country," and specifically include actions for fighting online GBV.

- Support the engagement of gender mechanisms and social protection in the cybersecurity space.

2. A Case Study from Bosnia and Herzegovina:

GENDERED CYBERVIOLENCE ENABLED BY LOOPHOELES IN THE TRADITIONAL LEGAL FRAMEWORK: “SHE WHO DARES TO CHALLENGE PATRIARCHAL STRUCTURES SHALL FACE NEVER-ENDING CYBERABUSE”

AIDA MAHMUTOVIĆ

Trigger Warning - Alert for emotionally difficult material

This section contains information, readings, and discussion about harassment, threats, body-shaming and/or violence which may be triggering to survivors. We encourage you to care for your safety and well-being.

2. A Case Study from Bosnia and Herzegovina: **Gendered cyberviolence enabled by loopholes in the traditional legal framework: "She who dares to challenge patriarchal structures shall face never-ending cyberabuse"**

Aida Mahmutović

Introduction

Perhaps the most deceitful form of female oppression in a patriarchal society is when gendered violence is publicly condemned while simultaneously shaming the victim by claiming that the violence, while wrong, was a natural reaction to the victim provoking her assailant(s). This manipulation of the truth automatically publicly prosecutes the victim, compelling her either to defend herself and her actions or to remain silent and accept her fate with no hopes of justice. Unfortunately, the latter is the route women have been forced to take for generations. They stay silent about the violence they experience, while society condemns the violence they "should not" speak about.

What if a woman were to break the silence and decide to talk and write about what she believes is right and just? What if others followed her example and supported her? Would she feel safe to voice her thoughts? Would violating her safety, be it perceived as physical or "online", be met with any real consequences?

While recognised by the United Nations (UN) [68] as a new form of violence, online gendered violence is unlike other types of violence in having an unusual dual role. Not only does it reflect the biases and prejudice in the "offline" world, it amplifies these by combining several forms of violence (sexual, psychological, economic, cultural, and others) without perpetrators ever having to face the person mutilated by their words. In 2015, the Broadband Commission Working Group on Gender recognised violence against women and girls (VAWG) as a problem of pandemic proportions. One in three women will experience some form of violence in her lifetime. It also noted that cyber VAWG could significantly increase numbers: at the time of writing, 73 % of the surveyed women had already been exposed to some form of online violence. [69]

[68] UN Women, Urgent action needed to combat online violence against women and girls, says new UN report (2015). Available online at: www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release

[69] Final report of the Broadband Commission Working Group on Gender, Combatting Online Violence Against Women & Girls: A Worldwide Wake-up Call (2015). Available online at: https://en.unesco.org/sites/default/files/highlightdocumentenglish.pdf

To make matters worse, online violence facilitated by information and communication technologies (ICTs) does not fall under any specific provision in the legislative framework. Victims of such violence and abuse are left to defend themselves, and the system fails to protect them. Unfortunately, the few statistics that are made available on such cases in Bosnia and Herzegovina (BiH) show an alarming increase in severe online harassment targeting women, especially those who lead public lives.

The case of Martina

“Martina, bukača,[70] boob-less, bitch, slut [who’s child should be killed], traitor, Her Excellency”, is how a TV host introduces Martina on his show[71] by quoting some of the online insults she has received over the years.

Martina Mlinarević Sopta is a famous writer from BiH, author of Firentnske suze, Otok u Prosincu, Neprocjenjivo, Ljetos drugi ledovi, Huzur and Bukača*. She is a freelance journalist and a human rights activist. Recently she became the ambassador of BiH to the Czech Republic and to Slovakia.

People who know her describe her as a fierce woman. She is from a traditional family, but she stands up to patriarchy. She has been vocal about nationalism and hate. Her activism has helped others, but has resulted in an ongoing backlash of attacks on her job, her freedom to express herself, and quite literally her life. Her activities, successes, personal life and appearances in public are underlined and followed by orchestrated online attacks against her persona.

Martina`s exposés threaten the very heart of the patriarchal ethno-nationalist structure that administers public discourse in BiH. Her writing and speeches enter the domain reserved to men, unforgivable in the eyes of her detractors. This becomes visible in the very gendered nature of the attacks to which she is subjected. Her femininity and womanhood are questioned, ridiculed and threatened. “A long tongue that does not suit an honest woman in our region” was one comment aiming to bring Martina Mlinarević Sopta back to the modesty, silence and the lowered head that befits an “honest” woman.

After recovery from breast cancer, she appeared naked on the cover of a magazine, showing the scar from her breast surgery. In the interview accompanying the photograph she said: “What am I in this world we live in now? I like to describe the mental backwardness of the palanquin and the hypocrisy of the hood. In our country, such women are called freaks. All right, here I am, a freak, and as such I’m showing you that it could be you tomorrow.”

That was when she started receiving ever more vicious and never-ending online attacks against her person.

“Die bitch. If God permits your children will also die from cancer. You piece of shit…”

“I personally hope the disease you had comes back to you and ends your life.”

“I pray the cancer multiplies a thousand times and eats all of you alive. You uneducated, filthy bitch.”

[70] “Bukača” stands for a terrible, non-existent woman, a mythical creature used by adults to frighten children. “Bukača” is also the title of Martina`s latest book.

[71] FACE TV (2019), TV show, Interview with Martina Mlinarević Sopta. Available to watch online at: www.youtube.com/watch?v=Nrouifco-pO

The photo became the target of many comments describing the image as inappropriate, indecent and disturbing, so the online platform chose to remove it "due to sensitive content." Martina publicly replied: "The picture bothered individuals because it 'surpassed the Balkan [mentality]." It became the excuse for a prolonged series of hateful and insulting posts.

Martina responded the best way she knew. As a writer, she felt that this was not only her fight, but an opportunity to break the silence and help other women and girls who might find themselves in a similar situation. She wrote a book entitled Huzur (translated: to be in peace with life, to have balance in the soul, serenity). The book, in the form of Facebook diary entries, tells the story of her fight against breast cancer in chronological order, from the discovery and diagnosis, through her struggle with the disease, to the surgery and therapy. "I have been writing about everything for years. A lot of my texts provoke reactions, but this particular one about the disease and the fact that I had to move with a small child to another city due to threats and cyberbullying has been met with extreme reactions, and I realised that it is necessary to talk about it, to put it between hard covers in one place."

While the book received praise and admiration, and was inspirational, at the time when it was published in BiH and in the region, online attacks against Martina resurfaced.

"This stupid hoe is calling herself a writer. People in this country love women with big breasts. What can you do there with one breast you have now? You stand no chance!"

"Single-breast woman."

"Sincere condolences to the Mlinarević family… you are a dead woman… both on paper and your soul… you betrayed your people, the people you live among… you are shameless…"

"For the way you speak, you could lose your other breast too."

Attacks followed her public writing relentlessly. Her texts and commentary on women's empowerment and on the ruling politics of BiH invariably became occasions for public backlash, with Martina enduring enormous pressures both offline and online. As she explained in one TV interview,[72] "Due to the stress I experienced from the threats and abuse, I had a miscarriage and it has contributed to me getting cancer." Eventually she decided to drop out of the public eye.

However, the attacks kept on coming. Her personal and medical conditions were considered to be fair game and a matter of public opinion. Every aspect of her personal and professional life became a subject for further attacks on social media.

When her participation in a festival where she had been invited to present her latest publication was cancelled, Martina declared that the ban was politically motivated and the festival organisers were blackmailed into cancelling her appearance. This provoked a new spiral of comments. Martina did not lack support, but the hate speech and insults were uncontrollable. They ranged from posts on her personal timeline on social media accounts to comments appended to articles mentioning her. It was a persecution campaign to punish her not only for the exposure of the scar on her breast but also for having dared to comment on politics and promote gender issues. Unpunished, the attacks escalated into misogynistic, intimidating threats to her personal safety and "promises" of imminent attacks against her family and loved ones.

"You ugly bitch. You are a real bitch. How many beds have you changed?"

[72] FACE TV(2018), TV show, Interview with Martina Mlinarević Sopta. Available online at: https://www.youtube.com/watch?v=8RO3xWqjHIs

“You are as ugly as [explicit wording], I’ve heard from people from your home-town what you were doing with men, from a very early age. Your career is over. You will go back to working on the streets.”

“I will [explicit wording] your mother. It will happen. Mark my words. My Ultras people[73] are already looking for you, you bitch. I will be your nightmare. Tell your boyfriend the location where to meet.”

“You are a dead body. I swear to you. I will screw with your life until you’re not breathing. I will spill yours and your boyfriend’s brains out.”

“You are sick and retarded.”

“She is not a woman. How can she be called a woman and a mother?”

“She should be raped and sent to a psychiatrist for life. Dumb as a wheel.”

With their normal impunity, the attackers escalated the threats. No longer satisfied with verbal abuse, they decided to bring their hate into the streets of Mostar, the town where Martina lived. In February 2020, during the town’s annual carnival, a doll resembling Martina, and alluding to her name, was set on fire. The organisers of the festival explained that each year, as a propitiatory rite, it is a tradition to burn the image of a person to represent all the evil that has happened during the year. “This is not the burning of the character and work of Martina Mlinarević as a person, but a phenomenon related to her,” the organisers stated.[74] Once again, an avalanche of comments followed on social media, and the image of the doll moved online and went viral, pushed by sensationalist media. “Satan cow” and “Burn the witch” typify the comments that followed. Uninterrupted, the threats moved from the internet on to the streets of Mostar and back again online, continuing their demolition of the “witch” Martina.

Eventually national groups, organisations and representatives of the international community in BiH expressed their public solidarity, condemned the violence and called for action. The Women’s Network of BiH demanded institutions should “adequately respond to hate speech and provide a safe and secure environment for Martina and her family”. The Society of Journalists of BiH called on institutions “to conduct an investigation and identify persons calling for her murder”, stating that “it all affected her family and especially her child.”

The Organisation for Security and Co-operation in Europe (OSCE) Mission to Bosnia and Herzegovina publicly condemned “all forms of violence, both offline and online, against journalist and writer Martina Mlinarević. One of the characteristics of democratic societies is that they allow the full enjoyment of fundamental freedoms, including freedom of opinion, conscience and expression, as well as the equal participation of men and women in public life.” The OSCE called on the institutions in Bosnia and Herzegovina to protect her. The British ambassador[75] and the US embassy[76] in BiH condemned persistent personal attacks on Martina Mlinarević and her family. They noted that “the attacks and comments online crossed the line of acceptable,” while calling upon institutions to investigate Martina’s case fully.

[73] A football club fan group, often problematic. Media reports their involvement in hooliganism, vandalism, causing disorder in the streets.

[74] N1 TV news portal, 2020, article Mlinarević nakon spaljivanja lutke sa njenim likom: Kad misliš da si vidio sve. Available online at: https://ba.n1info.com/vijesti/a412379-mlinarevic-nakon-spaljivanja-lutke-sa-njenim-likom-kad-mislis-da-si-vidio-sve/.

[75] Twitter, tweet by HE Matt Field, British Ambassador to Bosnia and Herzegovina. Available online at: https://twitter.com/MattFieldUK/status/1201168465140355073?s=20.

[76] Twitter, tweet by US Embassy in Bosnia and Herzegovina. Available at: https://twitter.com/USEmbassySJJ/status/1201217433765322752?s=20.

Today, as a high-ranking government official in BiH, Martina continues to receive hate comments on her social media accounts. She was the victim of new online attacks in February 2021.

Relevant legal and governance framework

Agencies

In Bosnia and Herzegovina there are three gender centres established as public institutions (governmental bodies), namely the Agency for Gender Equality of BiH, the Gender Centre of the Federation of BiH and the Gender Equality Centre of the Government of Republika Srpska. The Agency and Gender Centres are crucial instruments in initiating and implementing activities in the area of gender equality.

In both the executive and the legislature institutional mechanisms on gender equality include bodies at the municipal, cantonal, entity and state levels. The Committee for Gender Equality of the BiH Parliamentary Assembly[77] exists at the state level. At the entity level there are Committees for Gender Equality of the House of Peoples and the House of Representatives of the Parliament of the Federation of BiH[78] and the Equal Opportunities Committee of the National Assembly of Republika Srpska.[79]

Cantonal assemblies in the BiH Federation have established committees for gender equality. At the local level there are also committees within municipal assemblies in almost all municipalities across BiH.

Public policies and legislative frameworks

The law in BiH does not explicitly regulate online gendered violence. However, there are a number of frameworks and conventions that can form the foundation for such regulations:

gender equality frameworks, violence against women frameworks, criminal codes (BiH and entities), international treaties and conventions.

Gender equality frameworks

The principle of gender equality and the obligation to achieve gender equality in BiH are guaranteed by numerous legal acts within the national legislation and international legal documents which BiH has signed and ratified.

Public policies are also in force. One of the most important is the BiH Gender Action Plan 2018–2022.[80] The obligation to adopt the Gender Action Plan is envisaged in the Law on Gender

[77] Parliamentary Assembly of Bosnia and Herzegovina, Committee on Gender Equality website. Available online at: www.parlament.ba/committee/read/21?lang=en

[78] House of Representatives of the Parliament of the Federation of BiH, Committee for Gender Equality website. Available online at: http://predstavnickidom-pfbih.gov.ba/bs/page.php?id=35

[79] Equal Opportunities Committee of the National Assembly of Republika Srpska website. Available online at: www.narodnaskupstinars.net/?q=la/narodna-skupština/radna-tijela/odbori/odbor-jednakih-mogućnosti

[80] Agency for Gender Equality of Bosnia and Herzegovina, Gender Action Plan of Bosnia and Herzegovina 2018-2022. Available online at: https://arsbih.gov.ba/project/gender-action-plan-of-bosnia-and-herzegovi-

Equality.[81] This law addresses the key problems of men and women in the country, with the aim of achieving real gender equality. It regulates, promotes and protects gender equality, guarantees equal opportunities and equal treatment of all persons regardless of gender in the public and private spheres of society, and regulates protection against discrimination based on gender. Specifically, the law prohibits discrimination on grounds of gender, direct and indirect gender-based discrimination, harassment, sexual harassment, gender-based violence and victimization.

The Law on the Prohibition of Discrimination[82] [83] establishes a framework for the exercise of equal rights and opportunities for all persons in BiH and regulates the system of protection against discrimination. Discrimination is defined as "any different treatment, including any exclusion, restriction or preference based on actual or presumed grounds towards any person or group of persons and those related to them on the basis of their race, colour, language, religion, ethnicity, disability, age, national or social origin, affiliation with a national minority, political or other beliefs, property status, membership in a trade union or other association, education, social status and gender, sexual orientation, gender identity, sexual characteristics, as well as any other circumstance that has the purpose or consequence of preventing or endangering any person's recognition, enjoyment or realisation on an equal basis, rights and freedom in all areas of life."

Sexual harassment is defined in both, the Law on Gender Equality BiH and the Law on Prohibition of Discrimination[84] as: "any unwanted form of verbal, non-verbal, or physical behaviour of a sexual nature which seeks to violate the dignity of a person or group of persons, or which achieves such an effect, especially when such behaviour creates a frightening, hostile, degrading or abusive environment."

- Public policies for specific sectors, coordinated by the Agency for Gender Equality or the Gender Centres, include:
- Action Plan on the Implementation of Security Council Resolution 1325 on Women, Peace and Security;[85]
- Strategy to Implement the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence;[86]
- activities on gender-responsive budgeting;[87]
- Gender Equality Act.[88]

na-2018-2022/

[81] Law on Gender Equality in Bosnia and Herzegovina, consolidated version. Available online at: https://arsbih.gov.ba/wp-content/uploads/2014/02/GEL_32_10_E.pdf

[82] The Law on Prohibition of Discrimination (available on local language as: Zakon o zabrani diskriminacije). Available online at: https://www.osce.org/files/f/documents/1/1/378877.pdf

[83] Following amendments to the Law on the Prohibition of Discrimination in 2016, Bosnia and Herzegovina became the second country in Europe to prohibit discrimination based on "gender characteristics," thus providing protection for intersex persons.

[84] See the subsection on Criminal codes (BiH and entities) in this case study.

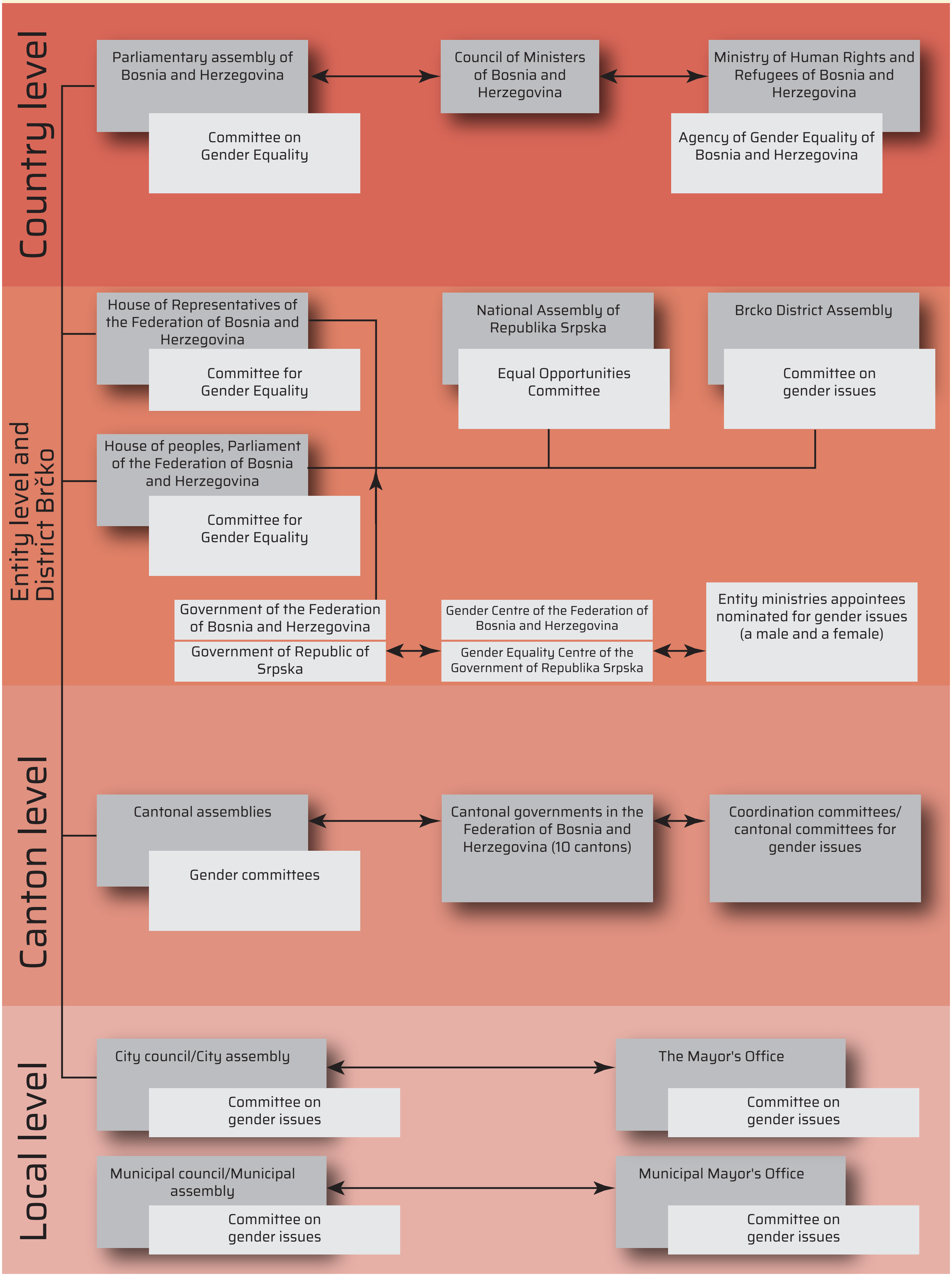
[85] Ministry for Human Rights and Refugees, Gender equality Agency of Bosnia and Herzegovina, A Report on the Implementation of Security Council Resolution 1325 on Women, Peace and Security in Bosnia and Herzegovina, 2015-2016. Available online at: https://arsbih.gov.ba/wp-content/uploads/2019/04/Annual-report_AP-UNSCR_01-08-2015-01-08-2016-Eng.pdf

[86] Ministry for Human Rights and Refugees, Framework strategy for the implementation of the convention on preventing and combating violence against women and domestic violence in Bosnia and Herzegovina, 2015-2018. Available online at: https://arsbih.gov.ba/wp-content/uploads/2015/10/CAHVIO_Strategy.pdf

[87] Agency for Gender Equality of Bosnia and Herzegovina, Gender responsive budgeting, resources. Available online at: https://arsbih.gov.ba/oblasti/rodno-odgovorno-budzetiranje/

[88] Gender Equality Act in Bosnia and Herzegovina. Available online at: https://arsbih.gov.ba/wp-content/uploads/2014/01/ZoRS_32_10_B.pdf

Institutional mechanisms on gender-related issues



Country level

Parliamentary assembly of Bosnia and Herzegovina

Committee on Gender Equality

Council of Ministers of Bosnia and Herzegovina

Ministry of Human Rights and Refugees of Bosnia and Herzegovina

Agency of Gender Equality of Bosnia and Herzegovina

Entity level and District Brčko

House of Representatives of the Federation of Bosnia and Herzegovina

Committee for Gender Equality

National Assembly of Republika Srpska

Equal Opportunities Committee

Brcko District Assembly

Committee on gender issues

House of peoples, Parliament of the Federation of Bosnia and Herzegovina

Committee for Gender Equality

Government of the Federation of Bosnia and Herzegovina

Government of Republic of Srpska

Gender Centre of the Federation of Bosnia and Herzegovina

Gender Equality Centre of the Government of Republika Srpska

Entity ministries appointees nominated for gender issues (a male and a female)

Canton level

Cantonal assemblies

Gender committees

Cantonal governments in the Federation of Bosnia and Herzegovina (10 cantons)

Coordination committees/ cantonal committees for gender issues

Local level

City council/City assembly

Committee on gender issues

The Mayor's Office

Committee on gender issues

Municipal council/Municipal assembly

Committee on gender issues

Municipal Mayor's Office

Committee on gender issues

Violence against women frameworks

Violence against women is recognised in law in Bosnia and Herzegovina. However, there are no specific provisions in the laws related to the use of ICTs to perpetrate such violence. There is no lex specialis that directly recognizes violence (against women) involving the use of technology. Family Laws address violence against women in BiH, yet there is still no consolidated family law at the national level. There are three laws that regulate issues of the family: Family Law of the Federation of BiH[89], Family Law of Republika Srpska[90] and Family Law of Brčko District.[91]

Specifically, domestic violence is regulated in more detail by the Law on Protection from Domestic Violence (LPDV): LPDV of the Federation of BiH[92], LPDV of Republika Srpska[93], and LPDV of Brčko District[94]. LPDVs have the function of protecting survivors of violence, while the processing of violence is based on the Criminal Law/Code. Domestic violence is recognised in the criminal law as a criminal offence. In addition, domestic violence is also defined as a form of gender-based violence.

Criminal codes and framework

BiH, due to its divided competences, has four Criminal Codes and Laws on Criminal Procedure: Criminal Law of BiH,[95] Criminal Law the Federation of BiH,[96] Criminal Code of the Republika Srpska [97] and Criminal Law of Brčko District of BiH.[98]

The criminal laws in BiH criminalise domestic violence and other offences; these are defined in a gender-neutral manner, except for those offences which by their nature can only have women as victims, but the laws provide a basis to prosecute perpetrators and protect victims in terms of gender-based violence. This creates a framework for the general prevention of violence against women, among other crimes.

A significant legislative change happened in 2017, when the new Republika Srpska Criminal Code was adopted and harmonised with the Istanbul Convention. The Criminal Code in Republika Srpska now provides for crimes such as persecution/harassment, association for the purpose of committing the criminal offences of trafficking in human beings and children, sexual blackmail, criminal offences of satisfying sexual passions in front of a child (also recognised in the criminal laws of the Federation of BiH and Brčko District of BiH) and the criminal offence of harassment or bullying at work (mobbing).

[89] Family Law of the Federation of Bosnia and Herzegovina. Available online at: https://advokat-prnjavorac.com/zakoni/porodicni_zakon_Federacije_BiH.pdf

[90] Family Law of Republika Srpska. Available online at: https://advokat-prnjavorac.com/zakoni/porodicni_zakon_RS.pdf.

[91] Family Law of Brčko District. Available online at: https://advokat-prnjavorac.com/zakoni/porodicni_zakon_brcko_distrikta.pdf

[92] Law on Protection from Domestic Violence of the Federation of Bosnia and Herzegovina. Available online at: www.paragraf.ba/propisi/fbih/zakon-o-zastiti-od-nasilja-u-porodici.html

[93] Law on Protection from Domestic Violence of the Federation of Republic Srpska. Available online at: https://advokat-prnjavorac.com/zakoni/zakon_o_zastiti_od_nasilja_u_porodici_RS.pdf

[94] Law on Protection from Domestic Violence of the Federation of Brčko District. Available online at: https://advokat-prnjavorac.com/Zakon-o-zastiti-od-nasilja-u-porodici-Brcko-distrikt.html

[95] Criminal Law of Bosnia and Herzegovina. Available online at: https://advokat-prnjavorac.com/zakoni/Krivicni_zakon_BiH.pdf

[96] Criminal Law the Federation of Bosnia and Herzegovina. Available online at: https://advokat-prnjavorac.com/zakoni/Krivicni_zakon_FBiH.pdf

[97] Criminal Code of the Republika Srpska. Available online at: https://www.paragraf.ba/propisi/republika-srpska/krivicni-zakon-republike-srpske.html

[98] Criminal Law of Brčko District of Bosnia and Herzegovina. Available online at: https://advokat-prnjavorac.com/zakoni/Krivicni-zakon-Brcko-Distrikta-BiH.pdf

The Criminal Laws of the Federation of BiH (Article 183) and Brčko District of BiH (Article 180) and the Criminal Code of the Republika Srpska (Article 150) recognize, inter alia, the following criminal offences:

- endangering security
- persecution/harassment (defined only by the Criminal Code of the Republika Srpska – the Federation of BiH and Brčko District Criminal Laws do not define it)
- unauthorised wiretapping and audio recording
- unauthorised optical imaging, i.e. photography
- sexual harassment (defined only by the Criminal Code of the Republika Srpska – the Federation of BiH and Brčko District Criminal Laws do not recognise it, which implies unequal protection of victims of sexual harassment throughout the country)
- coercion to sexual intercourse[99] (Criminal Laws of Federation of BiH and Brčko District)
- sexual blackmail (Criminal Code of the Republika Srpska)
- blackmail
- lewd and lascivious conduct.

It is unfortunately true that the relationship between the online digital world and the physical one is a continuum and not separated. As recording and circulation via the internet of rape videos[100] amplify and perpetuate the trauma and violence suffered by the victims/survivors, similarly in cases of sexual coercion the internet become the means to access and maintain control over the victims. The fact that the law does not contain the explicit mention of the word “online” or “internet” does not prevent law enforcement, prosecutors and judges from extending the protection of the law to victims/survivors.

International treaties and conventions

BiH is a signatory to numerous international conventions and legal documents that guarantee the full enjoyment of human rights and freedoms, as well as gender equality. [101] The most important among them, which can be invoked in cases of violence against women with the use of technology, are:

- Universal Declaration of Human Rights and Freedoms, 1948
- European Convention for the Protection of Human Rights and Fundamental Freedoms, 1953
- Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), 1979

[99] Office on Women’s Health, resources on sexual coercion. Available online at: www.womenshealth.gov/relationships-and-safety/other-types/sexual-coercion.

[100] Anita Gurumurthy and Amrita Vasudevan, GenderIT.org,2018, Hidden figures - a look at technology-mediated violence against women in India. Available online at: www.genderit.org/node/5104/.

[101] Ministry of Justice of Bosnia and Herzegovina, overview an overview of all international agreements on legal assistance that are binding for Bosnia and Herzegovina. Available online at: http://www.mpr.gov.ba/organizacija_nadleznosti/medj_pravna_pomoc/bilateralni_ugovori/Konvencije.aspx?langTag=bs-BA&s1=34&pageIndex=1.

- Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention), 2011
- Convention on Cybercrime (Budapest Convention), 2001.

CERT in Bosnia and Herzegovina

A computer emergency response team (CERT) is a group of information security experts responsible for protection against, detection of and response to an organization's cybersecurity incidents. A CERT may focus on resolving incidents such as data breaches and denial-of-service attacks, but also provides alerts and incident-handling guidelines. CERTs conduct ongoing public awareness campaigns and engage in research aimed at improving security systems.

In 2011 the BiH Council of Ministers considered and adopted a strategy[102] for establishment of CERTs in BiH by the Ministry of Security. To the date there is no CERT on a state level. In June 2011 the Law on Information Security of the BiH Republika Srpska defined the national computer security incident response team of the entity and placed it within the Republika Srpska Agency for Information Society. In June 2015 the Republika Srpska CERT became operational.

Proactive measures[103] of the Republika Srpska CERT include dealing with online threats. The incident report form[104] includes sending SPAM messages, distribution and sharing of copyright-protected content, dissemination of content forbidden by law and incidents not covered in the existing classification. It is important to note that this CERT covers only incidents in the cyberspace of the Republika Srpska entity.

BiH has not yet adopted the strategy on cybersecurity and/or cybercrime, but the issues of cybercrime and cyberterrorism are addressed in the strategy for fighting organised crime in BiH (2014–2016[105]) and the strategy for prevention of and fighting against terrorism (2015–2020[106]) – both with national security in mind.

Best practices/gaps in the legal and governance framework revealed by the case study

Martina started seeking protection and justice for everything that had been happening to her, using what she thought would be proper legal means. She had endured enough insults, threats and hate speech, directed both at herself and at her family, and sought to take legal action against her assailants. Martina filed a report at the police station. She spent many hours going over every comment she had received, trying to explain the seriousness of these online attacks. She says that, to her knowledge, to date the "police never knocked on anyone's doors, and that this will be where the story ends."

[102] Ministry of Security of Bosnia and Herzegovina (2011), Strategy for establishing CERT in Bosnia and Herzegovina. Available online at: www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=bs-BA

[103] Republika Srpska CERT website. Available online at: certrs.org/en/about

[104] Republika Srpska CERT incident reporting form. Available online at: certrs.org/en/report-an-incident

[105] Ministry of Security of Bosnia and Herzegovina, Strategy for fighting organized crime in Bosnia and Herzegovina (2014-2016). Available online at: www.msb.gov.ba/dokumenti/strateski/default.aspx?id=11926&lang-Tag=en-US.

[106] Ministry of Security of Bosnia and Herzegovina, Strategy of Bosnia and Herzegovina for preventing and combating terrorism (2015-2020). Available online at: http://msb.gov.ba/dokumenti/strateski/default.aspx-?id=12786&langTag=en-US

As a journalist she received support from the Association of Journalists, which reported her case on two different occasions. Each time she was invited to make a statement at the Ministry of the Interior. “I spent five hours in both of these cases, again replying to questions and going through my feelings on how I felt each time I received such messages.”

What especially struck Martina was the fact that the case of two high-ranking individuals, a male and a female, who had also received a threat (to life and safety) in the comment section on a portal was solved within hours. [107] The person who had made the comment was identified by the email address and/or public profile he used. The threats were officially identified as a threat to attack life and safety. A prosecutor of the Special Department for Organised Crime, Economic Crime and Corruption filed an indictment against this person. [108]

“Most of them wrote under their real names. I wanted to speak out and show the amount of torture not only I but other colleagues go through. No one has been sanctioned for the threats yet, despite the fact that the identities of most people are known. The man who threatened [one of the high-ranking individuals] was sanctioned, he was found and sanctioned within two hours. […] When I reported to the police, I did not ask for anyone to be arrested, I asked for something like this to be stopped. This was literally cyber bullying to which my family and I were exposed. Responsibility is paramount – of the judiciary, the prosecution, the police, the portals, but they missed it. “

In a similar instance, in Republika Srpska, a man who threatened two high-ranking individuals using social media was arrested very quickly. Officers of the Department for High-Tech Crime of the Criminal Police Directorate of the Ministry of Internal Affairs interrogated the suspect for the criminal offence of “endangering security.” He was handed over to the competent district prosecutor’s office to be charged with committing the crime.

Martina wonders why in her case it was not possible to identify a single person over the years, although she also received threats to her life and safety. For now, all the attacks on her remain unsolved.

Recommendations

Women in general face major barriers in navigating the formal justice system,[109] including cost, lack of knowledge of their rights and distrust of the penal and judicial systems.[110] Due to the prevalence of traditionalist patriarchal attitudes and values, revictimization and threats of social sanction or stigma are additional problems faced by women if they approach the justice system.

The following recommendations need to be adopted by various stakeholders to break a cycle that is hurting more and more women as uptake of the internet and its usage in BiH increases.

[107] ABC portal info, article (2019), Mlinarević kaže da je u Hercegovini doživjela linč i da se preselila u Sarajevo. Available online at: https://www.abcportal.info/novosti/vijesti/mlinarevic-kaze-da-je-u-hercegovini-dozivjela-linc-i-da-se-preselila-u-sarajevo

[108] N1 TV news portal, article (2020), Optužnica zbog prijetnji na internetu Gordani Tadič i Larsu Gunnaru Wigemarku. Available online at: https://ba.n1info.com/vijesti/a461921-optuznica-zbog-prijetnji-na-internetu-gordani-tadic-i-larsu-gunnaru-wigemarku/

[109] World Justice Project (2019), Women’s Access to justice: A Global Snapshot. Available online at: https://worldjusticeproject.org/news/womens-access-justice-global-snapshot

[110] United Nations, UN Women (2018), A Practitioner’s Toolkit on Women’s Access to Justice Programming. Available online at: https://www.unodc.org/pdf/criminal_justice/WA2J_Consolidated.pdf

Legislators and public policymakers: Raise the profile of these issues in public policy debates

At the European Union level, the concept of gendered online violence is still not fully defined and not yet regulated entirely by law. However, considering that the existing legislation at the national level in Bosnia and Herzegovina recognises and defines violence against women and gender-based violence on the one hand and criminal acts and cybercrime (such as threats, extortion, etc.) on the other, relevant consequences for offenders might be established.

With the broad use of online tools in our day-to-day life, the topic of gendered online violence needs to be given the attention it deserves by legislators and public policymakers.

- Legislators and public policymakers should work in consultation with relevant stakeholders to develop guiding principles for legislation on violence against women and coordinate a gender-sensitive implementation of legislation.

- Laws and policies that affect women should be distinguished and separated from those addressing the rights and protection of children. While children are minors and therefore in need of protection, women are adults, capable of self-determination. of the fact that new draft legislation constantly groups women and children on issues of safety and violence is the expression of a paternalist and traditionalist approach that de facto perpetuates and underlines the status of women as “eternal minors.”

- Laws and policies that affect women need to be formulated at the national level. This case study shows the importance of recognising sexual harassment as a crime in the laws of the BiH Federation and Brčko District BiH, as it is already recognised in Republika Srpska. This should include online sexual harassment.

- Legal and programmatic measures taken by the government to deal with this plague of violence against women have been fragmented, dealing separately with domestic violence, femicide,[111] rape and assault (under the Criminal Code) and sexual harassment.

Governmental agencies

The existing Commissions for Gender Equality and Gender Centres should collaborate with other similar agencies in regional countries and the European Union to develop and adopt best practices through twinning and exchange programmes. They should also seek better coordination with other relevant entities, institutions, women’s rights and human rights groups, journalists’ associations, etc.

[111] World Health Organization (2012), Understanding and addressing violence against women - Femicide. Available online at: https://apps.who.int/iris/bitstream/handle/10665/77421/WHO_RHR_12.38_eng.pdf.

Prosecutors and judiciary

- The prosecutor’s office should create a permanent working group for the safety of women (including in digital space) to consider establishing an integrated legislative policy. This must include exemplary sanctions and intensify prevention mechanisms, including gender-sensitive training for (criminal law) enforcement officers.

- The prosecutor’s office should also work on documenting precedents in cases of both digital harassment and violence against women and making them available for purposes of training and familiarity.

Law enforcement agencies and competent authorities

- Law enforcement agencies and competent authorities should provide gender-sensitive training for (criminal law) enforcement officers.

- Efforts must be made to make the justice system gender responsive. Legislation exists, but it is rather dispersed and there are no clear procedures to be followed by the police and throughout the justice system to enforce the laws when it comes to ICT-enabled violence (against women).

- Strengthen specialised, clear and efficient internal and external protocols and codes of conduct for law enforcement officials addressing ICT-facilitated violence against women.

- Invest in specialisation in addressing ICT-enabled violence with a human rights and gender approach.

Nonprofits/civil society

- Form and maintain specialised helplines to provide support to women and girls who have been subjected to gender-based violence, with special emphasis on the use of ICTs to enable the violence.

- Work on strengthening the awareness and capacity of women and men advocates, journalists, educators and internet users to identify, react to and report violence facilitated online and by other ICTs.

- Produce resources to identify, and tips and tools to address, online harassment and other forms of ICT-facilitated violence against women.

- Share examples of promising and good practices that effectively address online and technology-facilitated violence to inform a range of stakeholders (women, women’s organisations, authorities, etc.).

3. A Case Study from Serbia:

GENDERED CYBERVIOLENCE: “TO EXIST IS TO RESIST”

HVALE VALE AND AIDA MAHMUTOVIĆ

3. A Case Study from Serbia: **Gendered cyberviolence: "To exist is to resist"**[112]

hvale vale and Aida Mahmutović

Introduction

There is one thing common to all people identifying along the female spectrum, by choice or birth, as cis,[113] lesbian, bisexual, heterosexual, transgender,[114] transwomen, intersexual, genderqueer or non-binary. Whether unknown and invisible or known and hyper visible to larger communities of their country/region because of their role, work, art or activism, or as private subjects expressing their opinions, sharing their preference and love, or as public personae, journalists, artists and performers, activists and politicians: women have experienced, are currently experiencing or will most probably experience or know someone that has been targeted and attacked online.

World statistics estimate that "one in ten women have already experienced a form of cyber violence since the age of 15."[115]

According to the European Institute for Gender Equality, "Young women belonging to the LGBTI community are at particular risk of cyber-harassment."[116]

When women online express their opinions, a backlash is a concrete possibility. Reporting to the UN General Assembly on "the safety of journalists and the issue of impunity" in 2017, the UN Secretary-General wrote: "Women who cover topics such as politics, law, economics, sport, women's rights, gender and feminism are particularly likely to become targets of online violence."[117] Expressing an opinion in any of these areas therefore increases the risk and exposes women to gendered cyberviolence.

And as the Secretary-General explained in the same report: "While men journalists are also subject to abuse online, abuse directed against women journalists tends to be more severe."[118]

[112] The origin of the phrase "to exist is to resist," adopted by transformative justice activists, is referred to have been used for the first time by Palestinian activists after the Israeli bombardment of Gaza in the summer of 2014." Leah Lakshmi Piepzna-Samarasinha, Care Work: Dreaming Disability Justice, Paperback, October 30, 2018; Arsenal Pulp Press

[113] Trans Student Educational Resources website, Definitions (2021), available at: https://transstudent.org/about/definitions/

[114] "Transgender is a broad term that can be used to describe people whose gender identity is different from the gender they were thought to be when they were born. "Trans" is often used as shorthand for transgender. To treat a transgender person with respect, you treat them according to their gender identity, not their sex at birth. So, someone who lives as a woman today is called a transgender woman and should be referred to as "she" and "her." A transgender man lives as a man today and should be referred to as "he" and "him."
National Center for Transgender Equality (NCTE), Understanding Transgender People: The Basics (2016), available at: https://transequality.org/issues/resources/understanding-transgender-people-the-basics;
Trans Mreža Balkan, Identiteti i terminologija (2021), available at: https://www.transbalkan.org/trans101/

[115] European Institute for Gender Equality EIGE, Cyberviolence against women (2017), available at: eige.europa.eu/gender-based-violence/cyber-violence-against-women.

[116] European Institute for Gender Equality EIGE, Gender Equality Index 2020: Digitalisation and the future of work - When gender-based violence goes digital (2020). Available at: eige.europa.eu/publications/gender-equality-index-2020-report/when-gender-based-violence-goes-digital

[117] UN General Assembly, The safety of journalists and the issue of impunity, Report of the Secretary-General (2017), available at: https://undocs.org/A/72/290

[118] Ibid.

The situation in 2020 is no different from that in 2017. One of the many faces of the 2020 Covid-19 pandemic was the rampant continuum of violence experienced by women and gender-diverse individuals. This was confirmed by the newly established SEE (Southeast Europe) Digital Rights Network[119] in a recent statement: "Since the onset of the COVID-19 pandemic, Central and Southeast Europe has seen a dramatic rise in the rate of digital rights violations, in countries where democratic values are already imperilled (...) The online sphere has already become a hostile environment for outspoken individuals and especially marginalised groups such as minorities, LGBTIQ+ community, refugees and women."[120]

Even though it is difficult to think of women as a minority, since they make up half the population in any given country, their marginalisation is undoubted, as is the gendered nature of the violence they face. It is important to understand why we speak of gendered cyberviolence or

online gender-based violence. The phrase not only points to the communities targeted, but to the way the violence is perpetrated.

The body is central to such violence. It is dissected, belittled, derided, weighted, shamed, blamed and threatened. Measured against traditional and patriarchal aesthetics and performative traditional roles, gendered cyberviolence invariably became: "threats of sexual assault and physical violence, abusive language, harassing through private messages,"[121] hacking, manipulation and non-consensual sharing of intimate images, targeted lies to damage professional or personal reputations, ransom demands and financial threats.

Sometimes an attack is perpetrated by an unknown individual, sometimes it is launched by partners extending their abuse into the digital realm, and sometimes the attacks are part of an orchestrated campaign directed by powerful individuals.

In some cases, the attacks rely on a more structured and strategic use of technology entailing distributed denial-of service (DDoS), or bots which are used to fuel hate in the online space by flooding the profile of the women and people under attack with hundreds and sometimes thousands of hateful and threatening messages.

All these forms of gendered cyberviolence focus on what is perceived and described as a wrong-female-body, or not-female-enough body or not-normatively-accepted-female body. The attackers leverage populism and chauvinistic and misogynistic mobs, and they are all rooted in patriarchal ideas of femininity and gender roles. The more the body escapes the patriarchal norms, the more the hate escalates, and the more the response from institutions, even when formally asked to investigate and react, becomes blatantly absent.

It is difficult to get accurate statistics on online gender-based violence: as with the traditional form of gender-based violence, victims/survivors mostly choose not to report attacks because they are questioned, judged, blamed and shamed by the very institutions that are responsible for administering justice, identifying and sanctioning perpetrators and, most importantly, stopping the abuse.

For all these reasons we asked Sonja Sajzor, a well-known and outspoken transwoman, to share her story and reflections. We feel that her experience is illustrative of the need for change. It

[119] CIVITATES, BIRN and Share Foundation, Declaration of the SEE Digital Rights Network (2020), available at: https://balkaninsight.com/wp-content/uploads/2020/08/SEE-Digital-Rights-Network-Declaration-English.pdf

[120] Share Foundation, SEE Digital Rights Network established (2020), available at: www.sharefoundation.info/en/see-digital-rights-network-established/

[121] Julie Posetti, Nermine Aboulez, Kalina Bontcheva, Jackie Harrison and Silvio Waisbord Online Violence Against Women Journalists: A Global Snapshot of Incidence and Impacts. UNESCO (2020), available at: https://unesdoc.unesco.org/ark:/48223/pf0000375136

is also an example of active resistance and freedom, and acts as an incredible inspiration for many women who share the same or similar online experiences.

Sonja's case shows structural discrimination[122] and the homophobic and transphobic fabric that cuts across social and institutional structures. But Sonja also speaks of strategies and networks that can help address this discrimination.

Sonja Sajzor

"You don't need to censor anything about my story. Not anymore." This is how Sonja Sajzor, a 28-year-old transwoman from Serbia, begins the conversation. She is an artist, an activist, one of the most loved and best-known drag queens, a DJ and a rock musician, and has recently become a YouTuber.[123].

Sonja Sajzor defines herself as a transfeminist, with a focus on women's rights from the perspective of a transgender person. Her left-wing activism interlinks the transgender cause with multiple issues, such as poverty, homelessness and the lack of healthcare.

"I've always been very feminine, which is something still tolerated in early childhood." Growing older Sonja was increasingly exposed to harassment – her first memories are from the second grade, when she was labelled as "gay". She didn't report the harassment, afraid that she would be reprimanded even more "because she is gay."

To the best of her recollection, she was first confronted with online violence in February 2009. That was the first time an internet provider entered the village where she lived. As soon as Sonja created her personal profile on Facebook, she immediately started receiving numerous comments and messages about being "GAY." At the time, she did not share what was happening with anyone.

In 2011, when she was still a high-school student, she posed for the yearly "Queeria"[124] calendar. That same year, Facebook changed its algorithm to publicise to users timeline posts that had been "liked" by their Facebook friends. "This is where I made a mistake. I 'liked' my own photo in the calendar. So then it became visible to others too," explains Sonja.

The photo went viral, and people started posting her photo as their own profile picture with inscriptions: "We will find him" and "We will kill him." Sonja had no friends to advocate and stand for and with her. One of the teachers reported one of the boys for starting a lynch mob; the police interrogated him, "and that was it," Sonia recalls.

"I didn't have friends in real life. I only knew a few people online. But online, I used a different name and someone else's photo." When she turned 18, she left her home-town of Sabac and moved to Belgrade, hoping to escape the continuous harassment. After looking unsuccessfully for a job, she returned home.

At that time, she discovered the true power of the internet and spent her time online, making

[122] European Union Agency for Fundamental Rights, Challenges Facing Transgender Persons (2009), available at: fra.europa.eu/sites/default/files/fra_uploads/1228-Factsheet-homophobia-transgender_EN.pdf

[123] YouTuber, also known as a YouTube personality or YouTube content creator.

[124] Wikipedia, Queeria - Centar za promociju kulture nenasilja i ravnopravnosti(Kvirija), (2021), available at: sh.wikipedia.org/wiki/Queeria

and posting arty pictures of herself. This created interest and many people contacted her with ideas for collaboration. Ida Prester,[125] a well-known Croatian singer, invited her to take part in one of her music videos, and Sonja accepted.

The cyberbullying was relentless, but Sonja re-enrolled at high school and graduated. She continued to maintain her presence online, document her transition, and sustain a public and very visible persona.

"I find it difficult to remember all the things I've experienced online," explains Sonja. "There were many threats. In the small town where I lived, there was a story going around about a gang who kidnapped a young homosexual and buried him alive in concrete. No one ever confirmed this case. However, I kept receiving messages and comments saying: 'You are next.'

Facebook changed its rules again and started enforcing its real-name policy, where users needed to use the name indicated on their identity card. [126] "It became that much easier for people to find me on the internet,"[127] remembers Sonja. "Threats such as 'We will find you' and 'We will beat you' increased and became much more common. Until then, I was able to use different names and change them when I needed, to protect myself. Now, I started noticing more glances and ugly words on the street."

In 2014, she moved to Belgrade again, found a job as a waitress, assumed Sonja Sajzor as her permanent name and joined online spaces using it. In the same year she started performing in a club as a drag artist.[128] In 2015, a man who had seen her photo online recognised her, approached her and hit her. Sonja ended up with a broken rib. No one was ever held accountable for the attack.

"Apart from this physical attack, I have been followed many times, but managed to escape each time."

When, in 2016, she began her transition, which she documents online as part of a seven-year artistic project and personal journey, her inbox was flooded with large numbers of unsolicited explicit photos sent by men.

"When people find out that I am a transperson, they become mad. They start insulting me directly, or call for public provocations and a lynch."

In 2018, Sonja decided to fight back against what she described as a year of "fascism overflow." All minorities, including LGBTIQ and Roma, were harassed and humiliated. In those circumstances, as a left-wing transfeminist activist she was in the spotlight again, awakening new hatred.

"Poverty is the biggest problem of trans people," says Sonja. Stigmatism and transphobia make it difficult to get a job, find an apartment and afford the cost of the medical transition, which is a long and expensive process. For all these reasons, in 2018 Sonja participated in Transgender Awareness Week in the second week of November[129] and the International Transgender Day of Remembrance on 20 November.[130] Her public participation triggered a new wave of online threats and harassment. "'We will find you, rape you, and kill you,' this is what they kept writing

[125] Wikipedia, Ida Prester (2019), available sh.wikipedia.org/wiki/Ida_Prester

[126] Wikipedia, Facebook real name policy controversy (2021), available at: https://en.m.wikipedia.org/wiki/Facebook_real-name_policy_controversy

[127] See edition.cnn.com/2014/09/16/living/facebook-name-policy/

[128] RuPaul's Drag Race Dictionary, Drag Queen (2009), available at: https://rupaulsdragrace.fandom.com/wiki/RuPaul%27s_Drag_Race_Dictionary# D.

[129] GLAAD ,Transgender Awareness Week (2020), available at: www.glaad.org › transweek.

[130] GLAAD, Trans Day of Remembrance, (2020), available at: https://www.glaad.org/tdor

to me. At that point, all I could answer back was 'Get in line!'" says Sonja jokingly. "My sense of humour kept me going."

In 2018 VICE[131] made a documentary about her life, her art, her transition and rebellion. The film, originally planned to be shown only in the UK, was shown in Serbia. "I was so scared," recalls Sonja. "I knew local media were not sufficiently sensitised to report on LGBTIQ people, especially transgender people. To my surprise, reactions were good. This helped me relax and accept."

Hard work, being out, being known and having a public that loves her have provided Sonja with a sort of shield. "Over time, I stopped paying attention to comments on the internet and threatening messages I receive in my inboxes. I empowered myself both offline and online. I have done nothing wrong – I have never killed or raped anyone, or stolen anything. I am just a transgender person. I am used to comments and threats on the internet. They can't touch me anymore," she tells us.

The only time Sonja went to the police was in 2015, when her phone was stolen. It was one of the most uncomfortable moments she has ever experienced. The police officer asked for her ID and kept giving her strange looks. "He wasn't interested in hearing what happened, he was not interested in hearing a transgender person." Instead of been taken care of and listened to, she felt treated like a felon. The police officer kept misgendering Sonja, addressing her as a male. He threatened her with losing her job and being sent "back home."

She considered this experience as a sign, a proof that as transgender person she would never get protection from the police. "Then and there I realized there is no point in reporting any type of violence I am going through, especially not something that is happening to me 'online'."

It was a turning point at many levels. She remembers running back home and changing all her passwords. Ever since, she has deleted all her correspondence regularly. She wants to make sure that if anyone hacks her private communication, there would be nothing left to find. "I occasionally take screenshots of a funny conversation I have with my friends, just so I can get back to it and read it again," she adds.

Sonja is not the only transgender person to have had bad experiences dealing with police officers. Vanja and Leona are just two of the many people to have had similar experiences recently. In 2016, Vanja, a transman, was physically attacked by three men, who knocked him to the ground, kicked him and insulted him. Police officers laughed at him when he tried to report the violence.[132] In May 2017, Leona, a transwoman, was attacked, kicked, stoned and insulted by four men. She tried to escape by entering a taxi, but the taxi driver threw her out. Other taxi drivers shouted at and insulted her, and at the police station the officers questioned her way of dressing.[133]

Sonja herself recalls that in April 2018, a dozen of her Facebook friends shared information about a transwoman being harassed and insulted by three police officers after she went to report a rape. "She said the police officers humiliated and insulted her, and kicked her out of the police station," Sonja recalls. "So what's the point in reporting?"

At the beginning of the COVID-19 pandemic, Sonja went back to her home-town, where she writes for various media and works on her music and YouTube productions. Two or three times a week

[131] https://www.vice.com/en

[132] Medio.rs, Bacili su me na zemlju i krenuli da me šutiraju, a policija mi se smejala (2016) available at: https://www.medio.rs/vesti/srbija/drustvo/bacili-su-me-na-zemlju-i-krenuli-da-me-sutiraju-a-policija-mi-se-smejala_138943.html.

[133] Portal 021, Pretučena trans osoba u Beogradu, taksisti i policija nisu hteli da joj pomognu (2017), available at: www.021.rs/story/Info/Srbija/161991/Pretucena-trans-osoba-u-Beogradu-taksisti-i-policija-nisu-hteli-da-joj-pomognu.html.

her inbox is full of messages from transgender people asking for advice: employment, health, renting an apartment, etc. As she wrote in an article titled "The position of the trans population in the class struggle" for the Elektrobeton portal: "There is no safe place for transgender people whether online or offline. Mutual support is the only kind of safe support we have."

Public policies and legislative frameworks

Gender-based violence

International regulations play an important role in legal frameworks and can often be consulted when it comes to the regulation of digital violence. The Constitution of the Republic of Serbia stipulates that human and minority rights are guaranteed by generally accepted rules of international law and ratified international treaties.

- International documents of the United Nations:
- 1945 Charter of the United Nations[134]
- 1948 Universal Declaration of Human Rights[135]
- 1966 International Covenant on Civil and Political Rights[136]
- 1966 International Covenant on Economic, Social and Cultural Rights[137]
- 1979 Convention on the Elimination of All Forms of Discrimination against Women[138]
- 1993 UN Declaration on the Elimination of Violence against Women[139]

Council of Europe documents:

- 1950 European Convention on Human Rights and Fundamental Freedoms[140]
- 2011 Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention)[141]

[134] UN, Charter of the United Nations, 1945, available at: https://www.un.org/en/charter-united-nations/

[135] UN, Universal Declaration of Human Rights, 1948, available at: https://www.un.org/en/universal-declaration-human-rights/

[136] OHCHR, International Covenant on Civil and Political Rights, 1976, available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[137] OHCHR, International Covenant on Economic, Social and Cultural Rights, 1976, available at: https://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx

[138] OHCHR, Convention on the Elimination of All Forms of Discrimination against Women New York, 18 December 1979, available at: https://www.ohchr.org/en/professionalinterest/pages/cedaw.aspx

[139] OHCHR, Declaration on the Elimination of Violence against Women, 1993, available at: https://www.ohchr.org/EN/ProfessionalInterest/Pages/ViolenceAgainstWomen.aspx

[140] COE, Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No.005, 1950, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005

[141] COE, Council of Europe Convention on preventing and combating violence against women and domestic violence, 2011, available at: https://rm.coe.int/168008482e

The Istanbul Convention is of great importance when it comes to various forms of aggression. There is no one term that can sum up and synthesise the various forms and degrees of violence, therefore the importance of the Convention lies in the fact that it includes in its protective standards "all acts that cause or may cause physical, sexual, psychological or economic harm or suffering." This includes all the various forms and degrees of violence from harassment, bulling, stalking, doxing[142] that are perpetrated and practiced in the continuum of our physical and digital lives on the internet with persistence by one or more persons over time.

Article 34 of the Convention stipulates: "Parties shall take the necessary legislative or other measures to ensure that the intentional conduct of repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for her or his safety, is criminalised."

Article 17 of the Convention specifically calls for the private sector, the information and communication technology sector and the media, while respecting freedom of expression and independence, to participate in implementing policies, guidelines and self-regulatory standards to prevent violence against women and enhance respect for their dignity.

In Serbia, a number of legal documents address the issue of violence against women.

It is in this frame that the Serbian legislator introduced in June 2017 new provisions under the Criminal Code, one of this being the crime of "proganjanje." Literally translated as "persecution," it refers to any continuous inappropriate behaviour, indecent offers and comments that harass, make someone uncomfortable and/or through the intentional conduct of repeating threats through the use of digital technology means, cause the victim to fear for their safety.

The Constitution of Serbia explicitly prohibits discrimination on the grounds of sex (Article 21), guarantees the right to dignity and free development of personality (Article 23) and the inviolability of mental and physical integrity (Article 25). Gender equality and other human rights are guaranteed by the Constitution.

Protection against discrimination and violence is regulated by the Law on Gender Equality, the Family Law, the Law on Prohibition of Discrimination, the Labour Law, the Law on Prevention of Harassment at Work, the Law on Prevention of Domestic Violence, the Law on Personal Data Protection, the Criminal Code and the Law on Special Measures for the Prevention of Criminal Offences against the Sexual Freedom of Minors.

Due to the fact that only a small number of domestic laws explicitly mention cyber space as such, a general feeling is that the offences committed in the digital space or through technological means are unregulated or insufficiently regulated. However, unlawful activities remain unlawful, regardless of the manner, venue or tools used to commit them.

As a result, this solely means that it is necessary to approach such cases with a broader interpretation of regulations, and to accept the fact that all illegal activities should be sanctioned, regardless of where they are committed.

The Law on Gender Equality explicitly prohibits direct and indirect discrimination and provides for judicial protection in civil proceedings. Any person whose rights or freedoms have been violated due to their gender may initiate proceedings before a competent court. Civil proceedings, however, come at a cost for the plaintiff. This procedure can be initiated on behalf of a discriminated person, with their consent, by trade unions or associations whose work and goals promote gender equality.

[142] Doxing or doxxing is the act of publicly revealing previously private personal information about an individual or organization, usually through the internet.

The Law on Gender Equality and the Law on Prohibition of Discrimination were passed in the same year, and both stipulate judicial protection against discrimination. However, they are mutually incompatible to some degree. It is necessary to harmonize the provisions of these two laws when it comes to requirements of a lawsuit in civil proceedings. There is also inconsistency when it comes to the provisions governing active legitimacy for filing a lawsuit. According to the Law on the Prohibition of Discrimination, a lawsuit can be filed by the Commissioner for the Protection of Equality or an organisation dealing with the protection of human rights or the rights of a certain group of people.

An advantage of the Law on the Prohibition of Discrimination over the Law on Gender Equality is that it proscribes a wider range of forms of discrimination. The Law on Gender Equality covers only direct and indirect discrimination. The Law on Prohibition of Discrimination, in addition to indirect and direct discrimination, explicitly addresses violations of the principle of equal rights and obligations, invocation of responsibility, acts of association with the aim of discrimination, hate speech and harassment, and degrading treatment.

Hate speech is especially present on the internet when it comes to gender-based violence. The Law on Prohibition of Discrimination (Article 11) recognises and defines hate speech as a form of discrimination. It prohibits the expression of ideas, information and opinions that encourage discrimination, hatred or violence against a person or group of persons due to their personal characteristics, in public media and other publications, at gatherings and places accessible to the public, by writing and displaying messages or symbols, and otherwise. The act of committing hate speech is speech in its broadest sense – the expression of ideas, information and opinions, orally or in writing, explicitly or implicitly, directly or indirectly, through electronic means or print media.

A good practice example is the institution of the Commissioner for Protection of Equality, which offers the possibility to file a complaint online. A complaint may also be submitted by another person or an organisation dealing with the protection of human rights, with the explicit consent of the person whose rights have been violated. Within 15 days from the submission of the complaint, the Commissioner submits the complaint to the person against whom it was filed.

Information security

The Law on Information Security is an umbrella law approved on 26 January 2016. It offers a framework for the "security risks in information and communication systems, defines the responsibilities of legal entities in managing and operating information and communication systems, and determines competent authorities for implementation of protection measures."[143].

Serbia has a Strategy on the Development of Information Security 2017–2020, which was officially published in May 2017, and the Action Plan 2018–2019, which was adopted in August 2018. The Ministry of Trade, Tourism and Telecommunications is responsible for the information and communications technology security of the country, and the implementation of the strategy, while the Ministry of Interior is responsible for cybercrime-related matters, and the implementation of the National Cybercrime Strategy. The latter identifies the need for the National Centre for Prevention of Security Risks or a computer emergency response team (CERT), and the national CERT under the jurisdiction of the Regulatory Agency for Electronic Communications and Postal Services and supervised by the Ministry of Trade, Tourism and Telecommunications. Eight sectors are regarded as critical: energy, traffic, healthcare, supply of water and food, finance, telecommunications, information technologies, environmental

[143] Irina Rizmal, Guide through Information Security in the Republic of Serbia 2.0, Belgrade (2018) OSCE.

protection and the functioning of government entities. The Ministry of Defence is responsible for cyber defence. Serbia has a National Security Strategy and a new National Defence Strategy, which was approved in 2019.

In 2015, cybersecurity experts from the public and private sectors gathered in a process led by the Organization for Security and Co-operation in Europe (OSCE) Mission to Serbia, the Diplo Foundation and the Geneva Centre for Security Sector Governance (DCAF) which became known as the Petnica Group. In October 2020, the Petnica Group registered as a foundation under a new name. The newly created Cyber Security Network foundation aims to provide a platform for public–private exchanges and cooperation in cybersecurity.

The new Law on Personal Data Protection was adopted on 9 November 2018 and came into force on 22 August 2019. In November 2018, it underwent numerous changes with the aim of harmonising it with European Union (EU) law. The EU's General Data Protection Regulation (GDPR) entered into force on 21 May 2018 in all EU countries. The new Serbian law now largely represents the translated and adapted GDPR regulations, and thus it can be reliably considered that the principles of the GDPR have been introduced in Serbia as well. The law also prescribes the obligation to keep data in a form that enables the identification of persons only to the extent and for as long as it is necessary to achieve the purpose of processing.

An interesting office is the Commissioner for Information of Public Importance and Personal Data Protection, which through the years of its operation has contributed to setting the tone of public discourse and provided an important and accessible point for citizens to pose their questions. Every year, the office produces a report that synthesises the status of the implementation of the law on free access to information of public importance and the law on personal data protection in Serbia.

The Criminal Code regulates the protection of victims in criminal proceedings. Its significance is reflected in the definition of the following crimes:

- Violation of equality (Article 128)
- Endangering security (Article 138)
- Persecution / Harassment – Stalking, meaning any "continuous inappropriate behaviour, indecent offers and comments that make someone uncomfortable and when this intentional conduct of repeating threats causes the person to fear for their safety (Article 138a[144])
- Violation of the secrecy of letters and other items (Article 142)
- Unauthorised photography
- Unauthorised publication and display of other people's files, portraits and recordings (Article 145)
- Unauthorised collection of other people's data (Article 146)
- Insult (Article 170)

[144] Paragraf 138a, Law database, Zakona o Izmenama i Dopunama Krivičnog Zakonika 23. Novembra 2016. Published on Službenom Glasniku RS", br.94/2016 available at: https://www.paragraf.rs/propisi/krivicni-zakonik-2019.html and Autonomous Women's Center Belgrade, Nova krivična dela: proganjanje i seksualno uznemiravanje (2017), available at: https://womenngo.org.rs/vesti/961-nova-krivicna-dela-proganjanje-i-seksualno-uznemiravanje

- Exposing personal and family circumstances (Article 172)
- Violation of reputation due to racial, religious, national or other affiliation (Article 174)
- Sexual harassment (Article 182a)
- Displaying, obtaining or possessing pornographic material and exploitation of a minor for pornography (Article 185)
- Abuse of computer networks or other technical means of communication for committing criminal offences against sexual freedom of a minor (Article 185b)
- Domestic violence (Article 194)
- Blackmail (Article 215)
- Racial and other discrimination (Article 387)

Criminal offences against computer data security include: damage to computer data and programmes, computer sabotage, virus creation and distribution, computer fraud, unauthorised access to a protected computer, computer network or electronic data processing, prevention and restriction of access to a public computer network, unauthorised use of computers or computer networks, and the creation, acquisition or provision of funds for the commission of criminal offences against the security of computer data.

The Law on the Organisation and Competences of State Bodies for Combating High-Tech Crime establishes the responsibility of the Higher Public Prosecutor's Office in Belgrade for criminal offences against the freedoms and rights of a person and citizen; sexual freedom; public order and peace; constitutional order and security of the Republic of Serbia; and any acts which, due to the execution or means used, may be considered as high-tech criminal offences. This law places all acts of digital violence against women under the jurisdiction of the Higher Public Prosecutor's Office in Belgrade, in particular the Special Department for High-Tech Crime.

A paper under the working title "Persecution (harassment), legal analyses"[145] looks at the practice of the High Court in Belgrade and the Higher Public Prosecutor's Office Special Department for High-Tech Crime when it comes to the application of Article 138a of the Serbian Criminal Code and related norms on harassment and sexual harassment. The original term proganjanje in Serbian language is very descriptive, making clear that the person receiving this unwanted attention feels subjected to a "persecution." The abovementioned paper looks into ten decisions by the High Court in Belgrade on the criminal offence of proganjanje. Seven verdicts resulted in convictions, one resulted in an acquittal, and two decisions ordered security measures with mandatory psychiatric treatment (one perpetrator was ordered to undertake the treatment from their home and one in a psychiatric institution). In six of the seven convictions, the defendant entered into a plea agreement with the public prosecutor's office, in accordance with Article 313 of the Criminal Procedure Code, which was confirmed by the court in the conviction. Only one verdict resulted in a sentence of two months in prison. In all seven convictions the objects facilitating the crime were confiscated, including mobile phones, personal computers and tablets. In three cases, a security measure was imposed, prohibiting the perpetrator from approaching and communicating with the victim for two or three years. In five cases, men were convicted,

[145] Milena Vasić, author of the forthcoming publication "Persecution (Harassment), legal analyses" (translated), written for the Alternative Center for Girls, has generously shared it with us for the purpose of this case study. The paper is an unpublished draft waiting for final proofreading and publishing. We thank the author and the publisher for the possibility to access it at this stage.

and in two cases the perpetrators were women. In all cases, women were the victims/survivors.

In relation to the criminal offence of proganjanje (persecution / harassment under Article 138a), the Higher Public Prosecutor's Office in Belgrade, Special Department for High-Tech Crime, in the period from 1st June 2017 to 1st March 2020 had issued:

- 111 criminal charges with 11 convictions;
- five convictions punished by a sentence of imprisonment;
- one acquittal;
- 25 proceedings ending with dismissal of the criminal complaint;
- one procedure which resulted in a dismissal of criminal charges ending with the rejection of the criminal report due to fulfilment of the obligation from Article 283 of the Criminal Code;
- no measures under Article 79 of the Criminal Code were imposed for the same offence.

Best practices/gaps in the legal and governance framework revealed by the Serbian case study

Serbia has, what can be described as, an all-encompassing legal framework on the issues of both gender-based violence and the cybersecurity ecosystem, even if awareness and knowledge are not evenly distributed within institutions and among the general public.

As in the other case studies in this publication, what is immediately clear is the separation of power and responsibility between the two areas. The language of information security and cybersecurity has been particularly abstract and detached from the lives and experiences of the citizens, whom critical national assets are supposed to protect.

However, some points of contact appear which can offer a concrete space for potential synergies. These are represented by personal data protection areas and the Special Department for High-Tech Crime under the Higher Public Prosecutor's Office in Belgrade, which by law has all acts of digital violence against women under its jurisdiction.

Serbia has a vibrant civil society, vocal on digital rights and gender-based cyberviolence, which is able to campaign, build important monitoring initiatives and engage in supporting legal cases. Just a few such actors are Share Foundation, BIRN, the Alternative Center for Girls (AczD), which did extensive research on the intersection of gender and information and communication technologies.[146] This included a review of the existing legal framework to understand how better to support victims/survivors of violence, conducted by Milena Vasić. To this we can add a resilient and committed group of alternative and independent media whose journalists themselves are targets of cyber attacks, with several female journalists under persistent attack for their work in investigative journalism.

[146] Alternative Center for Girls and One World Platform"Pregled stanja online rodno zasnovanog nasilja u Bosni i Hercegovini, Hrvatskoj, Crnoj Gori i Srbiji", (2019)

Why then are tools and mechanism in place not used? There are several factors. The pervasive patriarchal and nationalistic culture, as Sonja explained and experienced, is a permanent feature of the distributed culture of violence, and a sense of impunity is perpetrated by the very same institutions. Serbia`s social media space is known for the strategic use of bots,[147] created with the specific intention of increasing traffic against a target. This generates a sense of overwhelming public consent, set against a background of orchestrated campaigns that have become a constant feature in many national and international human rights reports. One must distinguish the public face of a country, with an openly lesbian prime minister and a special status for some of its celebrities, from the application of the rule of law to the general public and the gender sensitivity of public institutions. It is important to remember that one of the slogans featured in the massive protest against the current sets of power has been “Vučić pederu” (Vučić faggot), which reveals the homophobic sentiment felt widely among the population.

To facilitate a gender-sensitive governance structure, and even more to disseminate an understanding of infrastructure as an ungendered, neutral area of intervention requires focused efforts that increase awareness and change the existent power balance. If the cybersecurity sector is closed in a public-private duo, we will not progress. Industry at its core has often demonstrated its slowness in moving from an inherently patriarchal-dominated system to one that questions and opens its ranks to the reality of highly discriminatory practices, which they see and name as a political intervention against the supposed neutrality of the technology tools and environments they program, develop and manage.

The truth is that we need a political intervention with feminist spectacles and feminist lenses which can provide structural applications of a gender analysis framework to render visible the structural absence of and hostility towards gender-aware and gender-sensitive planning.

While victims/survivors have to rely and count on their own personal emotional resources and support networks to resist daily harassment and violence, there is no serious conversation possible. Mechanisms and institutions are prevented from fulfilling their true roles.

Recommendations

National Gender Mechanism:

- Demand and invest in the creation of national statistics and sets of gender-disaggregated data to generate the necessary public evidence of gender-based violence and enable development of adequate policies.

Ministries of Justice, Labour, Employment, Veteran and Social Affairs and Cybersecurity Institutional Ecosystem from the Ministry of Defense to CERT, to Internal Affairs in collaboration with CSOs:

- Promote longer-term national programmes and devise financial mechanisms for aware-

[147] A bot (short for “robot”) is an automated program that runs over the internet. Some bots run automatically, while others only execute commands when they receive specific input. Per Christensson, TechTerms :free online dictionary of computer and Internet terms – Definitions – Bot (2005), available at: techterms.com/definition/bot

ness raising and education, training and skills on gender cyberviolence and cybersecurity. Address specifically the need of prosecutors, police officers, expert bodies and decision-makers developing strategy and policies on cybersecurity and/or gender.

- Transform the police from being a stronghold of prejudice, stigma, homophobia and transphobia into being truly public officials through gender-sensitive training and strong performance monitoring systems.

- Engage in a process to review existing frameworks and mechanisms through a gender lens and develop a gender analysis of Serbian cybersecurity mechanisms, policy and strategy; include LGBTIQ+ and female journalists, IT professionals and academia.

Ministry of Education, Science and Technological Development and National Bodies responsible to advance Serbia Digital Agenda:

- Provide dedicated training for public officials and decision-makers on the intersection of gender and digital technology.

- Run public awareness-raising campaigns on the intersection of gender and digital technology, with special attention to LGBTIQ+.

- Move from a private–public partnership between industry and governments to open consultation, inclusive of civil society and gender and LGBTQI+ advocates.

- Organise local translations of the 11 voluntary norms as proposed by the 2015 report of the United Nations Group of Government Experts (GGE) on developments in the field of information and telecommunications in the context of international security and run local workshops with gender mechanism representatives, LGBTIQ+ women's rights organisations active in the field of security, regulators, and the technical community to raise awareness and produce a contextual gender analysis of the above mentioned norms exercise of the 11 voluntary norms.[148]

[148] UN General Assembly Resolution A/70/174,"Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security", 22 July 2015, Section III, para. 13 (a)-(k). Available at: undocs.org/A/70/174

CONCLUSION

EUGENIA DOROKHOVA

Summary of key findings and trends from the Case Studies; Addressing cyber VAWG through principles of good governance; Recommendations and areas requiring further research

Eugenia Dorokhova

Key findings and trends from the Case Studies

In the three case studies, offline realities of gendered abuse and inequality are not only reproduced, but amplified online. The subjects of the case studies are exposed to a significant continuum of violence, enabled by the anonymity of the internet and a continuous growth in technological means and possibilities. Each case study portrays the difficulties for victims of online abuse in getting access to justice, or in fact any other kind of support. The case studies from Albania and Bosnia and Herzegovina show that law enforcement was not able to register and further pursue the complaints of the victims. In the Albania case study, law enforcement officials failed to see the theft of the subject's personal data in the wider context of a campaign of intimidation and harassment against her. Moreover, the Bosnia and Herzegovina case study portrays how women who are actively involved in politics and not afraid of voicing their opinions, and who "dare" to openly challenge the traditionally accepted role of women in society, are not only more likely to be attacked online; they seem to receive even lesser acknowledgement or support from law enforcement and the justice system. When the subject of this case study complained to the police about the severe abuse she had suffered, no action was taken. Similar complaints from another man and woman active in public life (but who were not seen as voicing 'uncomfortable' ideas) on the other hand, were pursued.

In the Serbia case study, the subject does not even believe or trust that she would receive any kind of support from law enforcement. Previous experience had shown her that reporting a crime to the police as a transgender woman, resulted in her being treated as a suspect rather than a victim.

The result, in all three case studies, is drastic impunity for online abuse and technology-facilitated acts of violence. While the subjects in each of the case studies showed remarkable defiance against the attacks on them online, the attacks were not without consequences.

Systemic and structural discrimination against women and girls online and in media is not only causing significant harm to their physical, psychological, economic and social wellbeing; It places significant barriers to the enjoyment of women`s rights and opportunities in society, and as part of the online community. As the Bosnia and Herzegovina case study shows, after relentless and harmful online attacks, there is almost no choice but to withdraw from online life in order to preserve one's health and sanity. This mirrors the experience of many women present in the public eye. Research has shown that such women are particularly exposed to exacerbated violence and abuse online, causing significant harm to their public personae and infringing upon their freedom of expression, and their access and participation in public life.[149]

[149] A wealth of information and analysis on this phenomenon is available online from a variety of further sources. See for example:

Overall, as the authors of the case studies conclude, there seems to be a lack of understanding and acknowledgement of the gendered aspects of cyberthreats and the implications they have upon society as a whole and upon individuals present online. This may, in large parts, stem from a lack of acknowledgement or response to gender inequality and discrimination present in the region. Legal and policy frameworks on gender equality exist, yet they are not connected to the cybersecurity agenda.

But what can be done to tackle these important issues? Where can Western Balkan cybersecurity actors, policymakers, governance and oversight bodies take effective steps to remedy the situation?

Applying the principles of good governance to cybersecurity and gender

A better understanding of the gendered impacts of cyberviolence both in law and in its application is a necessary first step. As the case study authors point out, laws and policies need to identify the ways in which cyberviolence differently impacts women, men, girls, boys, and people of diverse gender identities and expressions. Awareness needs to be raised, in particular on how cyberviolence further exacerbates discrimination that is already present in the offline world. Law enforcement officials, and other bodies charged with providing support and access to justice for victims, need to be sensitised to these important issues and adequately trained to provide the protections granted by law in a gender-responsive manner.

Gender is a key determinant not only of the security risks women, men and people of different gender identities and expressions face online, but also of the extent to which they are able to access and use online spaces safely. Therefore, aspects of gender and security online which need to be addressed include not only the use of online services, which can result in gender-specific threats and vulnerabilities of cyber incidents and online violence. It is also imperative to address the lack of participation of women and people of diverse gender identities in cybersecurity provision and governance by incorporating a gender perspective to the oversight, provision, and management of cybersecurity.

Cyber VAWG is rooted in, and must be addressed, as both an issue of cybersecurity and of gender equality. Hence the way forward lies in combining both arenas to tackle these and other gendered cyber security concerns.

Good security sector governance (SSG) is a useful concept for framing governance standards for the advancement of gender equality in security and in cybersecurity, as explained in the Introduction of this publication.

In this concluding section, we aim to address how key principles of good governance can be applied to aspects of cyber VAWG, and how an SSG approach could address the governance

- https://www.brookings.edu/techstream/gendered-disinformation-is-a-national-security-problem/
- https://carnegieendowment.org/2020/11/30/tackling-online-abuse-and-disinformation-targeting-women-in-politics-pub-83331

A practical Quick-read guide: gender and countering disinformation toolguide published 2020 by the UK Government is available online at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866353/Quick_Read-Gender_and_countering_disinformation.pdf

See also: Online abuse now commonplace for Balkan women reporters on BalkanInsight.com. Available online at: https://balkaninsight.com/2019/06/18/online-abuse-now-commonplace-for-balkan-women-reporters/

On targeted disinformation and cyber violence campaigns against women in the public eye:

challenges raised in the three case studies. The principles of good SSG include: Accountability, Transparency, Rule of Law, Participation, Responsiveness, Effectiveness and Efficiency.[150]

The NAPRI tool

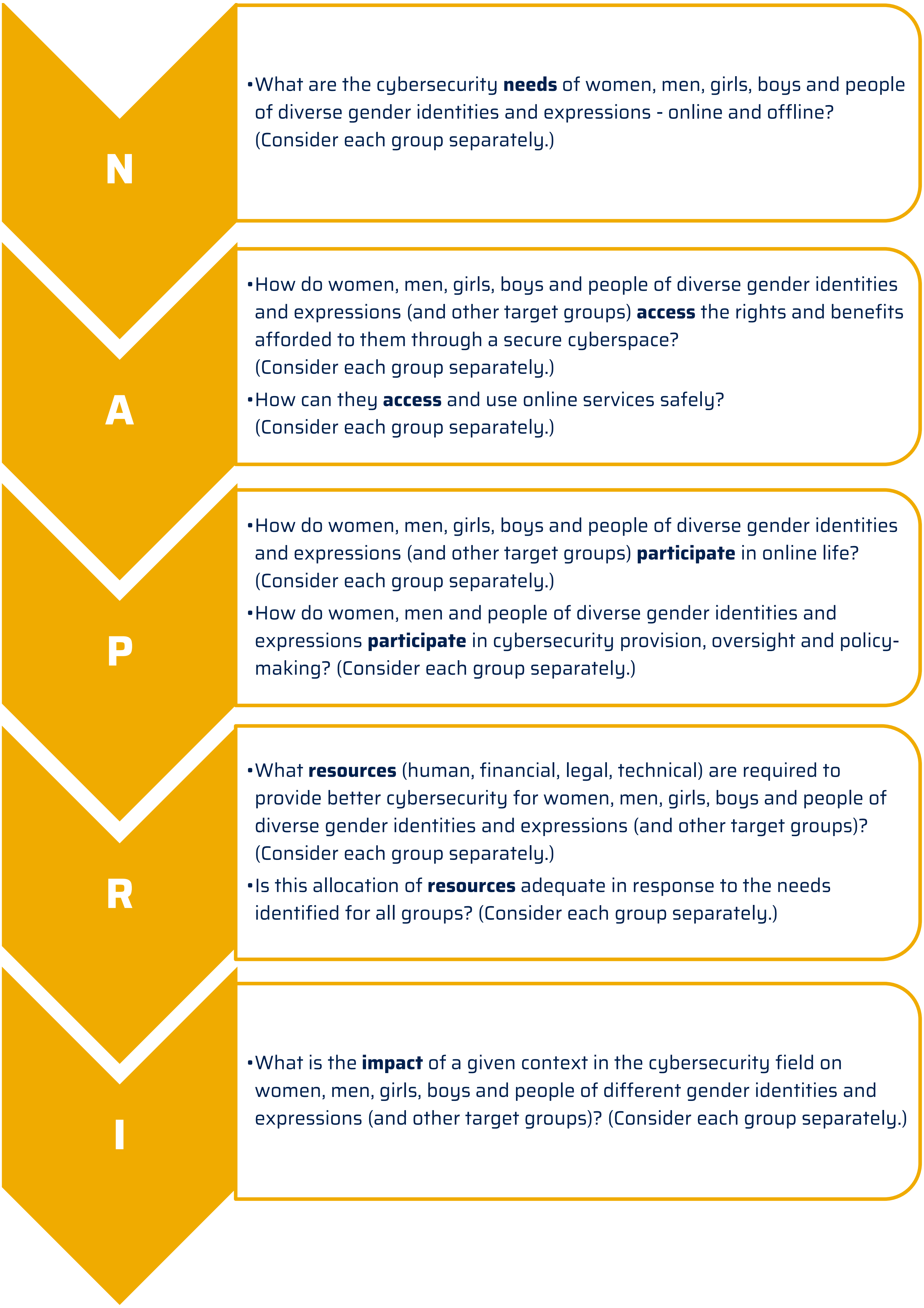
DCAF's NAPRI (needs, access, participation, resources, impact) Tool is a simple means for thinking about how the principles of good governance and gender equality can be applied to the security and justice sector. This tool allows actors working in or with the security and justice sector to conduct a gender analysis, by prompting the user of this tool to ask specific questions across different dimensions of a given context.[151] It can help the user analyse a context, project idea, policy, legislation or any other action/intervention using no more than desk research or reflection. It can also serve as a framework for an extensive participatory gender analysis using a variety of data collection methods.[152] The NAPRI tool can be adapted to any context, and is based on the principles of good governance in the security sector. It presents a good starting point for identifying how and to which extent gender has been taken into account in a context of good SSG.

Applying the NAPRI gender analysis tool to the cybersecurity context reveals the following possible list of questions:

[150] Please see the Introduction for a full explanation of the concept behind these principles and how they can be applied in cybersecurity governance and provision.

[151] DCAF, OSCE/ODIHR and UN Women (2019), Integrating Gender in Project Design and Monitoring for the Security and Justice Sector, in Gender and Security Toolkit, Geneva: DCAF, OSCE/ODIHR, UN Women, p.12

[152] Ibid.



N

- What are the cybersecurity **needs** of women, men, girls, boys and people of diverse gender identities and expressions - online and offline? (Consider each group separately.)

A

- How do women, men, girls, boys and people of diverse gender identities and expressions (and other target groups) **access** the rights and benefits afforded to them through a secure cyberspace? (Consider each group separately.)
- How can they **access** and use online services safely? (Consider each group separately.)

P

- How do women, men, girls, boys and people of diverse gender identities and expressions (and other target groups) **participate** in online life? (Consider each group separately.)
- How do women, men and people of diverse gender identities and expressions **participate** in cybersecurity provision, oversight and policy-making? (Consider each group separately.)

R

- What **resources** (human, financial, legal, technical) are required to provide better cybersecurity for women, men, girls, boys and people of diverse gender identities and expressions (and other target groups)? (Consider each group separately.)
- Is this allocation of **resources** adequate in response to the needs identified for all groups? (Consider each group separately.)

I

- What is the **impact** of a given context in the cybersecurity field on women, men, girls, boys and people of different gender identities and expressions (and other target groups)? (Consider each group separately.)

Of all the questions raised in the NAPRI tool, it may be particularly useful to focus on the principles of responsiveness and participation, as well as the advancement of a gender perspective at institutional levels.

Responsiveness

For cyberspace to be made safer for all, governance mechanisms need to implement a gender perspective and establish sensitivity to the individual security needs of internet and ICT users within their constituency. The security needs of women, men, girls, boys and people of different gender identities and expressions online can differ by a great extent, and it is therefore important to first evaluate and analyse such needs before embarking upon changes to policy and oversight. There is an urgent lack of research, statistical analysis and recognition of the cybersecurity risks that affect people differently on account of their gender, especially in the Western Balkan region.

Participation

To combat gendered effects of cybersecurity incidents and address important issues such as cyber VAWG, actors tasked with cybersecurity provision, management and oversight need be able to understand and represent the perspective and security needs of those they serve to protect. Governance of cybersecurity provision and oversight therefore needs to take a participatory approach.

Implementing strategies to increase women's representation in technical professions of the cybersecurity community will allow the Western Balkan economies to draw on a more diverse, gender-balanced cyber talent pool. There is still a significant gender-gap in IT professions and in cybersecurity oversight functions, and it is therefore necessary to include women at all levels of cybersecurity oversight, decision-making and service provision by encouraging and supporting their meaningful participation within various roles and functions.

BOX 1 GOOD PRACTICE: SPECIALISED GENDER-FOCUSED STAFF

Many justice and security providers globally have instituted roles for specialised gender-focused staff, consisting of part-time or full-time Gender Focal Points or Gender Advisers; gender units; observatories on equality; all female units; units specialised in responding to Gender Based Violence; roles focused on engaging with women, particular groups of women or men or LGBTI people within communities; and associations for women or LGBTI staff within institutions. Instituting varying roles with defined responsibilities for trained experts on gender and cybersecurity in Western Balkan economies could be an important step forward in addressing not only cyber VAWG but many tangential gender and cybersecurity related issues throughout the region.[153]

[153] Tool 1 of DCAF`s Gender and Security Toolkit provides ample guidance and best practices in promoting and achieving gender equality within the security and justice sectors. Section 4 of the Tool provides specific pathways to advancing a gender perspective in SSG processes. Available online at: https://www.dcaf.ch/tool-1-security-sector-governance-security-sector-reform-and-gender

Further Recommendations

Each of the three case studies provides concrete and country-specific recommendations which can be implemented in combination with a greater adherence to principles of good SSG and the advancement of a gender perspective. In addition to the findings of the case studies, as well as the reflections illustrated by the NAPRI tool, the following recommendations could help attain better and more responsive cybersecurity provision and oversight:

All actors involved in the provision, management and oversight of cybersecurity:

- Cybersecurity needs should be defined in an inclusive, gender-sensitive manner;
- Gender mainstreaming efforts should be undertaken, such as gender training for cybersecurity actors;
- Roles should be set up for staff with gender-specialised expertise;
- Masculine institutional cultures should be challenged to increase women`s participation and overall diversity, so as to allow for a more inclusionary and representative workforce and thereby a more responsive cybersecurity provision.[154]

Actors in cybersecurity provision; Providers of online services

- Awareness raising campaigns aimed at warning individual users of the dangers and propagating effects of cyber violence, and tailored to enact positive change in users` behavior online, should be implemented.
- The implementation of regional cyber-hygiene awareness-raising campaigns and campaigns providing information on support structures, targeting vulnerable focus groups (in particular young women and girls), would be an important step towards raising awareness and providing valuable information and support to victims.
- Gender-disaggregated statistics and analyses of women and men working in cybersecurity provision should be assimilated to allow for a comparison of how and by whom cybersecurity needs of the broader population are currently being addressed.
- Effective and easily accessible “flagging” / reporting tools to combat abusive/illegal content on social media, containing an effective review procedure of reported content, should be implemented by online service providers and social media platforms. This will allow victims of online abuse and cyber violence to be able to report the perpetrator to the online service provider/social media platform, for the abusive content to be reviewed and taken down, and for online users` abusive behaviour to be curbed in the long-term.

Academia and Civil Society Organisations

- Statistical analysis and targeted research need to be conducted into online gender-based violence, gendered effects of cyber incidents and other tangential cybersecurity and gender issues present in the Western Balkan Region.

[154] Ibid. See pp. 35-40 for practical guidance on the application of these pathways.

BOX 2 GOOD PRACTICE: CONTRIBUTION OF RESEARCH ON ADDRESSING REVENGE PORN

A short case study in Tool 4 of the DCAF Gender and Security Toolkit demonstrates how research on revenge pornography and "image-based abuse" undertaken by two academic institutions in Australia has had a significant positive impact on legal reform in the country, and promoted a measurable change in public awareness, nationally and beyond. "This research on image-based abuse was used to support recommendations for legislative change across Australia and directly shaped the development of two new internationally ground-breaking laws on intimate image abuse. (…) The research has not only had a direct impact on legal reform, but has helped raise the profile of image-based abuse nationwide and beyond. There has been a positive effect on victims, with their experiences being validated with a clear message that the abuse was not their fault and should not have happened. The possibility that others might not suffer, thanks to legal reform and raised awareness, has had a positive psychological impact on victims. Furthermore, as a result of this and other evidence-based research, Facebook and other social media companies have taken steps to redesign their current tools and policies to improve takedown and reporting mechanisms for victims of image-based abuse. The researchers have also briefed police and members of the judiciary to inform practice. "[155]

Western Balkan Governments; Oversight bodies; Policymakers; Donors:

- Working with a broader range of civil society organisations, in particular women`s organisations and LGBTQI+ organisations, will allow cybersecurity provision and oversight bodies to gain a more holistic understanding of any given situation from a security perspective, as well as to better understand diverse cybersecurity needs and how these can be met.[156]

- Civil Society engagement is strongly conducive to catalysing positive change and raising awareness, and the important contributions of CSOs and academic research groups focusing on these important issues need to be acknowledged, supported and adequately funded.

- Targeting higher (ideally equal) female participation and representation in policymaking and oversight mechanisms will contribute to the individual security needs of women and girls online to be better addressed in law and policy.

- Policymakers should create cybersecurity governance and policy frameworks that not only recognise gendered needs, but create an enabling environment for security and justice providers to act and address these needs.

- Policymakers can draw from a multitude of international instruments, agendas and frameworks, either for informational purposes or to establish policy coherence and har-

[155] DCAF, OSCE/ODIHR, UN Women (2019) Justice and Gender, in Gender and Security Toolkit. Geneva: DCAF, OSCE/ODIHR, UN Women, pp. 48-49. Available online at: https://www.dcaf.ch/sites/default/files/publications/documents/GSToolkit_Tool-4%20EN%20FINAL_1.pdf

[156] DCAF, OSCE/ODIHR, UN Women (2019), Security Sector Governance, Security Sector Reform and Gender, in Gender and Security Toolkit, Geneva. p.6. Available online at: https://www.dcaf.ch/tool-1-security-sector-governance-security-sector-reform-and-gender,

monisation with their country`s existing commitments to gender equality,[157] as well as to the attainment of greater security online.[158]

- Developing policies and legal frameworks that provide effective ways to address and remedy cyber VAWG and other gendered aspects of cybersecurity incidents is an important step to addressing this issue. To mitigate the spread of illegal activity and stop the use of online spaces to commit violence, internet users in many countries can "flag" and report illegal and hateful/abusive content in order for it to be reviewed and deleted, and the offending account to be sanctioned if needed. The best people to monitor what goes on in the internet – are the people using it, therefore providing online users with effective tools to report and mitigate abusive online content can be an effective way to curb the spread of abusive and illegal content online.

BOX 3 GOOD PRACTICE: AN EFFECTIVE COMPLAINT TOOL

In Germany, the Netzwerkdurchsetzungsgesetz[159] imposes a legal obligation on operators of social networks to provide an easily identifiable, immediately accessible, and constantly available method for the transmission of user complaints about illegal content, such as online gender-based violence. It furthermore obligates such online service providers to check content flagged by any user within a reasonable amount of time (24 hours) and adequately respond by either deleting the comment or sanctioning/suspending the violating account. If an affected user wants to achieve criminal prosecution beyond deleting or blocking the content, they are also enabled by this law to file a criminal complaint with the responsible law enforcement authorities. For such a law to take effect, the headquarters of a particular social media company or online service operator do not need to be located in the country of implementation.

[157] Brown, D. and Pytlak, A., WILPF and APC, 2020. "Normative Frameworks" in Why Gender Matters in International Cyber Security, p. 4. Available online at: https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf

[158] Ibid. These include for example:
Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention)
The Women, Peace and Security (WPS) Agenda, as established by the UN Security Council Resolution 1325 and the WPS National Action Plans,
The Beijing Declaration and Platform for Action,
CEDAW (the Convention on Elimination of All Forms of Discrimination Against Women,
The 2030 Agenda, and SDG 5,
UN Human Rights Council (HRC) Resolution 38/5,
Outcome documents of the World Summit on Information Society,
International Telecommunications Union (ITU) Resolution 70,
and the Feminist Principles of the Internet, developed by the Association for Progressive Communications (APC).

[159] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) from 10.09.2017, as amended on 30.11.2020.
See here for the full text of this law (in German): https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html
The Council of Europe has collated key provisions addressing cyber violence in domestic legislations of several countries around the world: https://www.coe.int/en/web/cybercrime/domestic-legislation

Areas of gender and cybersecurity requiring further research and attention in the Western Balkan context

While this publication focuses on cyber VAWG, a multitude of issues revolving around cybersecurity and gender exist at present, and many more gendered cybersecurity concerns exist which need to be addressed.

As was explained above, the lack of participation of women and people of diverse gender identities and expressions in the provision, management and oversight of cybersecurity and cybersecurity policy making, is one possible explanation for the fact that the cybersecurity laws and their application in the three case studies are not sufficiently gender sensitive. Further research on the current representation of persons active in cybersecurity provision, policymaking and oversight should be conducted to point towards gaps in current structures. This is important in order to then accurately define where and why problems arise currently, where problems may arise in future, and what gaps occur as a result of a lack of oversight and equal representation and participation.

On account of recent trends, the use of online tools to stalk and track women, and the important link to domestic abuse and gender-based violence needs particular research and regional attention. Attention also needs to be paid to the gendered effects of new technological developments and their societal implications for the Western Balkan population.

Targeted online disinformation campaigns are on the rise and present a further potential avenue of research, tangential to the issue of cyber VAWG that we aim to address in this paper.

It would also be interesting and important to examine, in a regional context, the gendered aspects of cybersecurity incidents and large-scale cyber-attacks that could occur in the Western Balkans. It has already been asserted that cybersecurity incidents have a gendered impact.[160] Even in cases where a potential data breach, for example, was not aimed at any woman in particular – affected women can suffer disproportionately due to the underlying societal inequality and discrimination they are subjected to in the offline world. [161] As Brown and Pytlak conclude: “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.” Due to a lack of available information, it would be important to conduct more targeted and region-specific research into the gendered aspects of different cybersecurity incidents and cyberattacks in the Western Balkan region.

Moreover, the internet itself is gendered[162] and an individual’s use of and reliance on the internet has to be understood in the specific social and economic context in which they live. For example, some women may be particularly dependent on online services to earn income or for educational purposes, if responsibilities in their home prevent them from pursuing such activities offline. Should such access to online education or income-based activities be interrupted or impeded by a cybersecurity incident or internet shutdown, these women will no longer be able to access these opportunities. Among others, important further examples of women`s disproportionate reliance on the (safe) use of online services have been listed to include: access to information related to their sexual or reproductive rights (which may not always be fully or objectively

[160] Brown, D. and Pytlak, A., WILPF and APC (2020), Why Gender Matters in International Cyber Security. Available online at: https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf

[161] Ibid.

[162] Ibid.

accessible to women offline); access to seeking out services which enhance women`s physical safety and mobility; a safe space to express themselves (in particular on political views, sexual expression and defying gender stereotypes) specifically in cases where women face barriers of societal taboo offline; and for accessing information and exploring their sexual orientation or gender identity. [163] Due to the empowering effects that the internet can have for them, women are therefore likely to be disproportionately affected by cybersecurity incidents. It would be important to examine how the internet is used by the Western Balkan population and what services women, men, girls, boys and people of diverse gender identities and expressions rely on as separate groups, as well as how this reliance on certain internet structures correlates with their offline lived realities.

Beyond the use of online services, a further aspect to analyse more deeply in the region, is access to online services and technologies and the gender-digital divide. There appears to be a relationship between ICT engagement and gender equality from a global perspective: Consistently among low, middle and higher income states, higher levels of ICT and internet usage among women are also accompanied by higher rates of gender equality in their respective countries.[164] On the other hand, more men than women use the internet globally. In its Measuring digital development: Facts and Figures 2020 Report, the International Telecommunications Union (ITU) estimated that in 2019 only 48% of the global female population was using the internet, compared to 55% of the male population.[165] In measuring this against an estimated 7.86 billion people living on the planet today and the respective female and male populations, this means that roughly 312 million more men than women use the internet. While the gender gap for access to online services in Western Balkan region has shrunk significantly, it is nonetheless difficult to empirically measure because internet usage data is often not disaggregated by gender, but by connectivity based on household. This presents a problem, given that the gender digital divide continues to prevail within households.[166] As such, not only internet connectivity and online access, but various further aspects of the gender-digital divide, would be an important direction for further research in the Western Balkan regional context.

[163] Ibid.

[164] Dr. Shoker, S., Global Affairs Canada, Making Gender Visible in Digital ICTs and International Security, Available online at: https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf

[165] ITU, Measuring digital development: Facts and Figures 2020. Available online at : https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf, p.8

[166] Dr. Shoker, S., Global Affairs Canada, Making Gender Visible in Digital ICTs and International Security, p.8. Available online at: https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

✉ info@dcaf.ch
☎ +41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva