CENS & The High Commission of Canada Webinar Series On “Gender, Security and Digital Space : Exploring Risks, Opportunities, and Security Implications”

Event Report

11, 18 and 25 May 2021

Centre of Excellence

for National Security

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

NSCS
NATIONAL SECURITY
COORDINATION SECRETARIAT

Report on the Workshop jointly organised by:

Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore

High Commission of Canada to Singapore

Editors:

Gulizar Haciyakupoglu*, Research Fellow, Centre of Excellence for National Security

Yasmine Wong*, Senior Analyst, Centre of Excellence for National Security

***** Editors have made equal contributions to this report.

Transcription by:

Velia Ng

The panel sessions of the workshop are captured in the conference report with speakers identified. Q&A discussions are incorporated without attribution.

Terms of use:

Table of Contents

Executive Summary

The Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS) in Nanyang Technology University (NTU) and the Canadian High Commission to Singapore collaboratively organised a three-part webinar series on “Gender, Security and Digital Space: Exploring Risks, Opportunities, and Security Implications” on May 11, 18, and 25, 2021.

The webinar series, which featured industry experts and speakers at the forefront of research and practice, explored various issues concerning security in cyberspace, including disinformation campaigns, hate speech, and internet shutdowns. These are burgeoning issues in digital space that have garnered greater attention as security concerns. With growing cognizance that these issues have disproportionate effects on the population by gender, the webinar series visited the concepts concerning security that are traditionally considered to be “masculine,” highlighted the importance of taking a gender-focused approach to security and cyberspace, and discussed policy responses to online threats that have gendered impacts.

The first webinar explored key issues arising in the cyber security landscape and how gender perspectives are often overlooked when discussing their impacts, thus exacerbating vulnerabilities for women and other marginalised groups online. It drew attention to how the assumed gender neutrality of digital spaces results in gender blindness, which overlooks the nuance in capabilities, needs, and priorities of women, men, and non-binary peoples.

The assumption of masculinised norms of vulnerability, threat, and security often project the responsibility of cyber security onto individual users. This emphasises the need for a framework that incorporates a gender-focused perspective into the design and operation of socio-technological systems, the identification of vulnerabilities, and the response to and post-incident reporting of cyber security attacks.

In ASEAN, the persistence of the digital gender gap made particularly salient by the COVID-19 pandemic, threatens the exacerbation of gender inequality in the region. The gendered digital divide puts women at risk of income loss, and impedes access to education and career opportunities, especially with digital acceleration in the wake of the pandemic. This gender divide also affects the participation of women and other marginalised groups in digital space, endangering their security and well-being in the long-run.

Information and Communication Technologies (ICTs) can help mitigate some of the challenges central to the women's equality agenda, for instance, through the facilitation of political mobilisation and freedom of expression, the facilitation of women's economic activity and participation in markets, and the mediation of interaction between individuals and governments. Thus, as Internet shutdowns are increasingly normalised as a security response to political mobilisations and unrest in some countries, it is cardinal to examine its disproportionate impact on women.

The second webinar discussed the gendered implications of disinformation and hate speech with a particular focus on gendered disinformation and hate speech targeting women in politics. It drew attention to how gendered disinformation and hate speech amplifies gender stereotypes, discourages women from participating in politics, and damages democracy and human rights. The webinar highlighted the extent to which women face online disinformation and hate speech, and drew attention to patterns and similarities observed in different contexts while noting the existence of culture and context specific differences in various countries.

The risks to national and individual security in cyberspace, including algorithmic biases, disinformation, and toxic representation of women, diminish advantages brought by the Internet. Social media contributes to the problem, playing host to gender biases and offering few solutions, as perpetrators of gendered disinformation and online abuse often do not face penalties. It is crucial for women experiencing online abuse and disinformation to be vocal and enhancing individuals' media literacy is a part of the solution. However, the speakers acknowledged the burden placed on the victims of hate speech and disinformation to report such acts. They pointed at the need to support individuals suffering from online abuse and disinformation online, and called for a whole-of-society response.

Countermeasures to gendered disinformation and hate speech have to demarcate different types of violence and attend to advancing tactics, instruments, and terminology concerning violence against women. The barriers to countering gendered disinformation and hate in online spaces include limitations to the tools and political will to tackle the problem, lack of gender-focus in examining threats in platforms, absence of intersectional enforcement, victims having to shoulder the task of reporting online harms, and malign creativity.

The third webinar focused on gender-based hate speech and disinformation, and the role of social innovation in addressing these aspects of online insecurity.

The experiences from Taiwan's model of collaboration with its civic-tech community reveal the potential of digital space as a platform for community-driven and collaborative efforts in the battle against misinformation.

Recognising misogynistic disinformation and hate speech as a distinct category of online violence, the webinar discussed a rise in volume of and engagement with misogynistic content during the pandemic. These misogynistic narratives have been found to disproportionately affect the attitudes of followers online.

Countermeasures in practice in multiple case studies across Asia underscore the value of digital literacy, as well as humour when countering online misogyny.

Webinar One: Securing Digital Space with Attention to Gender

11th May 2021

Gendered Approaches to Cyber Security

Dr Katharine Millar, Assistant Professor of International Relations in the Department of International Relations at the London School of Economics

Summary: A report for the United Nations Institute for Disarmament Research proposes a three-pillar framework- Design, Defence, and Response. Each pillar corresponds to key dimensions of cyber security[1] related activities that need to be considered from a gendered perspective. Firstly, the design of socio-technological systems should include security systems responsive and sensitive to gender. Secondly, we should evaluate how defence strategies aimed at reducing risk, identifying vulnerabilities, and ameliorating potential harms to systems, are premised on gendered assumptions. Lastly, the response pillar relates to how states and some private sector organisations respond to cyber security attacks,

[1] Cyber security here is defined as the prevention and mitigation of malicious interference with digital devices and networks. Where malicious interference can be defined as the illegitimate intrusion into, or disruption of networks and systems.

including post-incident investigation and recovery, and legal measures to punish and deter perpetrators.

- Cyber security is often thought of as gender neutral. This results in gender blindness, which ignores differences in the capabilities, needs, and priorities of women, men, and non-binary people and how gender norms can inform our underlying assumptions and priorities within cyber security at large. The three-pillar framework of Design, Defence, and Response can be used as a first step to bringing gender analysis into the more technical elements of cyber security.
    - The Design pillar suggests that the conception of cyber security employed in technological and system designs is gendered, perpetuating masculine gender norms about resources, priorities, and what is good or expected security behaviour. This means that women and non-binary people are more likely to have cyber security threats to them downplayed or omitted, thus having to bear security burdens in addition to being likelier targets of disingenuous cyber marketing. For example, measures aimed at protecting individuals from identity theft often use personal information as the backup for passwords, relying on the assumption that the malicious actor is a stranger who has no access to this information. These assumptions neglect gendered and other intersectional risks,

discounting instances of intimate partner and family violence.

- The Defence pillar argues that how we think about "defence" and what it means to "defend[2]" reflect a series of norms typically associated with masculinity. Often, cyber security imports strategic concepts associated with military security. This results in the prioritisation of threats to the state, military, critical infrastructure, and sometimes, of corporations over civil society organisation and individuals, and of physical harms over non-physical harms such as the harassment of women and queer people online. A gender-focused understanding of cyber security threats also allows the acknowledgement of the gendered outcomes of traditional cyber threats.
- The Response pillar investigates how masculine norms of autonomy, control, and the avoidance of vulnerability can preclude actors from disclosing when they fall victim to cyber-attacks, which impedes important information-sharing regarding threats and thus, the generation of a more robust cyber security system. Cyber security response can also demonstrate gendered and sexualised dynamic of victim blaming, wherein actors with insufficient cyber security defence

[2] e.g., protection, autonomy, technical competence etc.

measures are often framed as “asking to be hacked”, attributing the blame to the victim rather than the perpetrator, or the entity that facilitated it. It also examines ways in which cybercrime legislations can contribute to these dynamics, through the lack of resources, the prioritisation of specific cyber security threats and harms, and/or the perpetuation of harmful stereotypes about who a victim is and what a good victim does, and who is expected to be a perpetrator.

- To this, there are three recommendations. First, public and private sector organisations can a) conduct training on gender equality, diversity, and anti-harassment and discrimination in the workplace; and b) establish and promote the type of gender analysis in cyber security as distinct, valued and required as a professional skill. Second, future cyber security policy could be assessed for gendered impacts, supporting gender audits of existing cyber security, and engaging in gender-disaggregated data collection. It is also important to think of ways to create cohorts of policymakers who are potentially bringing different sets of technical and legal gender analysis, and policy skills to bear on cyber diplomacy and policymaking. Lastly, gender equality should be built into typical mechanisms common to public sector oversight of the private sphere. Examples include legislation, procurement contracts, private sector regulation, standard setting, and ensuring equity and equality and oversight.

ASEAN Gender Digital Disparities

Fitriani B. Timur, Researcher, Centre for Strategic and International Studies (CSIS) Indonesia

Summary: In ASEAN, the persistence of the digital gender gap along with rapid digitalisation brought about by COVID-19 threatens the exacerbation of gender inequality. They create the risk of income loss, impede access to education and career opportunities, and in the long run, threaten the security and well-being of women and other marginalised groups.

- Access to technology remains a core problem in the Southeast Asian region because of structural inequalities posed by income, education, and employment opportunities. Statistics from the International Telecommunication Union (ITU) show that the accessibility for women has become a pressing problem in many countries across the region. Women are 12% less likely to use the Internet than men, in low- and middle-income countries, women are 10% less likely to own mobile phones compared to men and are 20% less likely to have access to the Internet. Women in many Southeast Asian nations are less equipped with digital skills compared to men, they experience fewer benefits from digitalisation and are less visible in STEM and ICT-related industries and policy processes. The lack of digital literacy renders women vulnerable to financial scams, digital phishing, and a slew of other cybercrimes. There is also still a gap in the advancement of women in leadership and decision-making positions in the digital sector, particularly in cyber security and governance.

- In ASEAN, inequality of access and use of digital technologies and the Internet affect women's ability to work, study, or seek help remotely during the pandemic, exacerbating their vulnerabilities. In Southeast Asia, women primarily manage micro, small, and medium enterprises. In developing countries, they contribute to the informal economy and engage in work that is often unprotected. Lockdown restrictions that restrict mobility have rendered women precarious because of the lack of insurance and benefits, and their inability to sustain access to the Internet. Many women bear unequal responsibility for childcare and some are also left vulnerable to domestic violence due to added confinement at home.
- Cases of online gender-based violence have increased, in Indonesia for example, up to 300%. There are cases of sensitive data leaks targeting women working in public-facing roles, such as journalists and human rights activists, and organisations providing information on how officials are handling the pandemic. There is also an increase in threats against women, including threats of physical violence, sexual violence, and threats made against their families. The absence of a serious approach to data protection in some ASEAN countries, and policies that lag behind technological advancements have exacerbated the problem.

- Despite the growth of cyber law in Southeast Asia, there is a need to examine the content and efficacy of these laws and practices, as some may prove to be double edged swords. In Vietnam for example, cyber security laws allow the government to censor social media posts and acquire private information from tech companies. Cambodia’s telecommunication law allows the government to monitor private conversations. Myanmar’s allow providers to monitor communication services, which has now been limited due to the recent political turmoil. In Indonesia and Malaysia, laws are not openly restrictive in comparison, but this is because the language used is ambiguous, creating inconsistencies and problematic judicial rulings.
    - The ASEAN Intergovernmental Commission on Human Rights (AICHR) inaugurated a special session on women’s empowerment, featuring for the first time, a focus on digital gender equality in 2019. Additionally, there are plans by the ASEAN Commission on the Promotion and Protection of the Rights of Women and Children (ACWC) to draft regional action for women, peace, and security which includes digital space. However, more could be done to overcome supply challenges of pricing and affordability to equip more women and other marginalised groups with access to ICTs. Women’s digital skills and access to information on how to safeguard themselves when accessing digital

platforms require improvement. Women have to be provided with relevant services and content to increase their awareness of their rights and opportunities in cyberspace. The provision of cyber security through the formulation of comprehensive and relevant cyber security laws that are sensitive to how gender roles and dynamics shape the region is essential.

Gender, Internet Shutdowns, & International Security

Dr Sarah Shoker, Postdoctoral Fellow, University of Waterloo

Summary: Digital ICTs come with a list of promises central to the women's equality agenda, even as governments try to reconcile the tension between ICTs as tools that both enable political expression and perpetuate gender harassment and violence. The increasing normalisation of Internet shutdowns as a security response to both peaceful political mobilisations and violent political protest should be examined for its disproportionate impact on women.

- Gendered approaches to analysing security aim to make women empirically visible in a field that has historically ignored their role in shaping international affairs. Taking ordinary people as valuable sources of information can aid in the prediction of international events like the Arab Spring, the fall of the Berlin Wall and South Korea's transition to democratic governance. Additionally, some research has indicated that a country’s commitment to gender equality is an excellent predictor of state aggression on the international stage- more so than levels of democracy or wealth.

- Several UN member-states have highlighted critical infrastructure protection as central to their national cyber security strategies, but critical infrastructure is often spoken of in terms of technical and computational vulnerabilities- remnant from traditional security policy that conceptualises insecurity as a threat to state sovereignty. As critical infrastructure protection is necessary for social wellbeing, ICT failures also have negative social and political consequences.
- Internet shutdowns,[3] have gendered consequences and can undermine a commitment to eradicating gender inequality. Some scholars have conceptualised Internet shutdowns as one tactic in an arsenal of tools that include content filtering, coordinated disinformation campaigns, and arresting individuals for online political expression. Several NGOs, however, have opted to mark internet shutdown as a distinctive phenomenon. The frequency of shutdowns increased from 106 in 2017 to 213 in 2019.
- The gendered impacts of ICT shutdowns include NGOs facing blocked communication lines, preventing them from providing services to vulnerable groups faced with the double burden of domestic, and sometimes, government-led violence. ICT shutdowns create more

[3] politically orchestrated critical infrastructure failures

restrictions on women’s mobilities than men as online spaces hold distinct advantages for women where women’s offline mobilisation comes with increased risk to physical safety. For example, during the 2019 Sudanese Sit-In, women and girls were less likely to be allowed to leave the house, and participate in sit-ins and they relied mostly on Internet access for situational awareness. Online communities served as informal crowdsourced violence warning systems, with Twitter and Facebook users broadcasting location data about civil violence. Facebook Live became particularly useful for documenting real-time political violence. Increasingly, women’s rights advocates are using digital ICTs to build resilience in the face of social disruption.

- Research shows that Internet shutdowns are more likely to occur during times of government transition, with low- and middle-income countries particularly prone. A look into Belarus and Myanmar can reveal similarities between new democracies that use Internet shutdowns to facilitate democratic backsliding.
    - In Myanmar, which is currently experiencing internet shutdowns, the government has been conducting internet blackouts in Rakhine province since 2019. The armed forces in Myanmar use Facebook to spread misinformation and ferment often violent opposition against the Rohingya minority. Facebook has been trying to ban accounts associated with the Myanmar armed forces.

The armed forces instructed foreign telecom companies to withhold mobile internet traffic using a legal provision. Telenor, a telecom company from Norway, complied. The disruption of internet access and democratic backsliding is enabled by a transnational supply chain that can have its roots in liberal democratic countries.

- Unlike Myanmar, Belarus did not have a history of internet shutdowns, the 2020 shutdown was a first time in the country’s history. However, they also share a few similarities: relative recent experiences with market liberalisation, small forays into democratisation, elections that triggered immediate democratic backsliding and the seizing of telecommunications infrastructure to crush democratic opposition. The Belarus case illustrates that countries that pursue assertive modernisation of their IT sector, can still respond to political instability by resorting to physical violence and censorship, even if the internet shutdowns threaten the country’s economic strength and growing international status. With the lack of international censure, there is little reason for governments not to use Internet shutdowns.

Webinar Two: Gender, Disinformation, and Politics

18th May 2021

Prof Sun Sun Lim, Head, Humanities, Arts and Social Sciences, Singapore University of Technology and Design (SUTD)

Summary: Sun Sun Lim delivered opening remarks and moderated the second webinar. The online threats to national and individual security, including disinformation, algorithmic biases, toxic representation of women and others, cast a shadow on the benefits afforded by the Internet. Media literacy is an essential component of the solution process, and Internet users should not be expected to solve the problem alone.

- Disinformation plagues the health of the online sphere. It threatens national security and individual safety, curtailing the degree to which the online environment could benefit society.
- Internet users, particularly women, navigate various trends that jeopardise the safe and constructive use of the Internet. These include algorithmic biases, questions concerning the design of the platforms, and the extent of machine learning processes that learn discriminatory practices due to corrupted data entered into the system.
- There are also other troubling developments that require attention, such as the "bro-culture" in games that have raised questions on the toxic representation

of women, and memes on platforms such as Instagram and Reddit that disparage women under the disguise of humour, which, in some cases, help normalise misogyny.

- While many see media literacy as seen as a vital solution, Internet users should not shoulder the task alone. Women's participation in the technology industry, including their access to programmer, designer, and coder roles, is essential to build a fair and representative infrastructure.

Gender, Disinformation & Politics: Part of the spectrum of VAWP

Dr Gabrielle Bardall, Principal, Herizon Democracy LLC and Research Associate, Centre for International Policies, University of Ottawa.

Summary: "Gendered disinformation"[4] capitalises on and intensifies existing gender stereotypes in society. It contributes to sustaining patriarchy in the political sphere, and it can serve as an apparatus for state power and foreign influence. The responses to gendered disinformation and abuse have to differentiate between different types of violence and take the evolving tactics, tools, and vocabulary around violence against women into account.

[4] Gendered disinformation and misinformation are components of violence against women in politics, which is a broader concept that encapsulates a wide range of acts, such as political rape, assassination, and suppression of women.

- Gendered disinformation is used to sustain the "patriarchal control of the political space," deterring women from holding leadership positions and engaging in politics. It reinforces and intensifies existing gender biases in societies, allowing malicious actors to prey on these existing biases. Women are subject to non-physical and psychological violence, including defamation and sexualization, more often than men. However, men also face violence, particularly homophobic content, as part of attempts to sustain the "heteronormativity" of the political sphere.
- Various factors, such as candidate profile, the electoral system and quota design, influence online violence against women. While high profile candidates are central targets, online violence can impact women without a public profile. Yet, online violence against women, with its visibility in cyberspace, also raises awareness and invites change. Violence against women in politics plagues every country. However, there are gendered norms and approaches particular to each country that mirror culture-specific differences. For instance, violence against women could involve narratives referencing the historical roots of communism in Ukraine.
- Disinformation can function as "a tool for state power," with states leveraging on gendered disinformation in foreign interference attempts. Gendered disinformation fits into "broader authoritarian projects" and may erode democracy. As

such, it is essential to understand why some foreign states might want to impede women of another country from accessing power. Authoritarian governments, such as Russia and China, may exploit gender inequality as a tool as the exacerbation of gender inequality infringes on social cohesion, and instils fear of change and feelings of insecurity.

- In attempts to measure online violence against women with a comparative outlook, it is critical to distinguish between different types of violence and tailor responses accordingly. Examining the "content," "volume," "speed," "intensity," and the degree of harmfulness of different types of violence is of great importance. The responses have to understand the scale of the problem, actors involved, acts perpetrated, targets of the acts, the timing and impacts of the acts, and evolving tactics, tools and vocabulary around violence against women. The triangulation of this with interviews and focus groups can provide a view of the extent of the problem. Countermeasures also need to account for the differences in platforms where violence can occur, including the variance in the security of and command over the content, and the private versus public nature of the platform.
- Furthermore, while laws directly addressing this issue are limited, there are various legal actions that target intersecting areas, including pornography-related laws; privacy laws; and laws concerning harassment, including "sexual cyber harassment, aggravated harassment, cyberstalking". Some countries (e.g.,

Bolivia and Mexico) have introduced laws concerning political violence against women, but these unique laws have been "difficult to implement." Online violence against women expands beyond national borders, and hence, responses cannot be limited to a national jurisdiction.

Gendered Disinformation & Online Attacks Against Women in Politics

Lucina Di Meco, Co-Founder, #ShePersisted

Summary: Social media platforms accommodate gender biases and are culpable for the growth of gendered abuse and disinformation online. Perpetrators of online abuse and disinformation are often not held accountable while victims often have to bear the burden of reporting such acts. **"**Gendered disinformation"[5] damages democracy and human rights. It is essential for women to be outspoken on gendered disinformation and they need to be equipped with necessary tools to continue their fight. There is a need to introduce

[5] Gendered disinformation is the dissemination of false or deceptive information and visuals targeted at women political leaders, journalists and public figures. Gendered disinformation seeks to create a false impression that women are not fit for politics, often employing similar narratives like the labelling of women as liars, stupid, untrustworthy, weak, and too sexual or not sexual enough. Some even allege that the women in discussion are not really women. The disseminators of gendered disinformation include "strong men, political leaders, liberal actors, authoritarian figures," who utilise misogynist websites and blogs.

standards as standards do not contradict, but rather, complement freedom of speech.

- Gendered disinformation aims to change public opinion on women politicians for political gain, damaging democratic institutions and human rights. There are intersections among the aims and impact of gendered disinformation taking root in different countries, including the weaponisation of gendered disinformation to curb political opposition and deter women from engaging in politics. However, gendered disinformation also demonstrates contextual and cultural variances across countries and involves stereotypes observed in a particular context.
- Gendered disinformation often capitalizes on misogyny and gender stereotypes, and it can trigger online abuse and hate. Gendered disinformation targeting Italian politician Laura Boldrini, for example, painted her as a controversial figure, leading to an onslaught of hate speech and rape threats against her. Gendered disinformation has also been used to mask "politically motivated murders." For instance, disinformation circulated after the assassination of Marielle Franco, a councillor of Rio de Janeiro in Brazil, sought to justify "political murder […] in some ways." Details of her assassination in 2018 still lacks clarity.
- A study based on interviews with more than eighty-five women in thirty countries exposed gendered disinformation and abuse in digital space. The study raised awareness on the gendered social media environment and the plethora of disturbing materials

against women, highlighted the amount of time invested by women to safeguard themselves and their “reputation” online, questioned the lack of perpetrator liability in online acts, and suggested that the social media companies are emerging as part of, rather than a solution to, the problem. Social media platforms often facilitate the circulation of gendered disinformation, and their algorithms help amplify such content. More importantly, online harms have influenced women’s view of the world and dissuaded some from running for office.

- Speaking out about gendered disinformation may bring about change as it did in the case[6] of West Bengal Chief Minister Mamata Banerjee. In this year’s elections, where many women came out to vote, Banerjee received a large percentage of women's votes, contributing to her unprecedented victory in the elections. Some women voters cited the sexism in the campaign trail as a reason for voting for Mamata. Other women politicians have been more vocal on the online attacks targeting them, including the First Lady of Namibia, Monica Geingos, who shared her

[6] Mamate Banarjee faced a politically motivated, coordinated disinformation campaign targeting her and her party. Her party argued that the accounts of hundreds of their supporters were removed and alleged a connection with the ruling party. A guardian article revealed that Facebook halted a move to remove various fake accounts in India upon noticing the involvement of the ruling party. Mamata Banerjee was targeted with misogyny again during this year’s elections. Mamata Banerjee, journalist and civil society called out the “sexism in the campaign”.

experience with online attacks in a video released on International Women's Day. Also, a letter to Facebook penned by U.S. representative Jakie Speier and supported by other women in politics called attention to the online hate targeted at women and the amplification of "extreme and dangerous" content via algorithms.

- Freedom of speech and improved standards should not be considered contradictory, but complementary. There are several existing regulations that target illegal content, however content that does not contradict the law yet has adverse effects on women and their participation in politics have slipped through the cracks of regulation. As "many women do not feel free and do not feel safe enough to actually speak on social media," it is essential to have social media standards to "support and foster freedom of expression."
- #ShePersisted sees the need for a three-pronged approach to the problem of gendered disinformation:
    - It is essential to improve knowledge on and public awareness of gendered disinformation, particularly in the Global South, as it is currently an understudied area with scarcity of data, and as it "relate[s] to authoritarianism."
    - It is critical to support women leaders who are striving to combat disinformation and who press for "regulatory change." Women leaders have to be equipped with the necessary tools and vocabulary to assume an

offensive position against the issue of gendered disinformation. Speaking out is critical. However, women should not be expected to solve the problem alone and societal effort is necessary.

- Online platforms have to be persuaded to attend to gendered harms in their standards and policies. Women have to take the lead in the process as those previously designed by men lack a comprehensive view of the extent of the problem. Also, the public has to put pressure on politicians to engage with social media platforms and consider social media regulations.

Malign Creativity: How Gender, Sex, and Lies Are Weaponised Against Women Online

Nina Jankowicz, Disinformation Fellow, Wilson Center

Summary: "Gendered disinformation"[7] discourages women from engaging in politics and erodes democracy. The impediments to countering gendered disinformation include

[7] Gendered disinformation refers to information that is (a) false, (b) that seeks to discourage women from "participating in the public sphere," and (c) that involves a degree of coordination. Gendered and sexualised disinformation is a subset of gendered abuse. Gendered abuse can be defined as the "use of derogatory terms aimed at degrading or insulting women based on their gender, ranging from name-calling to sexually violent threats."

malign creativity, inadequacy of tools and political will to eradicate the problem, absence of gender-considerate approaches in platforms, lack of intersectional enforcement, and victims being burdened with reporting gendered disinformation and abuse. The responses to the issue need to include steps undertaken by social media companies, governments as well as employers.

- Gendered abuse and disinformation cause women to withdraw from public life, taking a toll on democracy by hampering women's democratic engagement and "equal representation in elected offices". They are national security concerns as mal-intended actors could exploit the gendered faultlines in a society.
- The Wilson Center conducted a study on gendered disinformation, based on data accumulated from six social media platforms on a group of thirteen politicians (and journalists) before the US elections (September 1 to November 9). While gendered abuse appeared more often than gendered disinformation in keyword frequency, most of the women studied faced gendered disinformation and almost all were targeted by gendered abuse. Older women were not affected as much, calling for a deeper understanding of age as a factor.
- The content studied involved "sexual, transphobic, and racist and racialized narratives," with a large portion of the sexualized narratives targeting Vice President Kamala Harris. Disinformation with transphobic undertones alleged that successful women have achieved success because they are

transgender. In addition, racialized and racist disinformation is also common, and they are often aimed at representative Ilhan Omar.

- There are various hurdles en route to fighting gendered abuse and disinformation on social media. These include:
    - Malign creativity[8];
    - Inadequacy of tools and political will to tackle the problem, including the absence of a comprehensive definition of harassment;
    - Lack of gendered perspectives in platforms “built by and for” men;
    - Absence of intersectional considerations, mean that women of colour, for example, are subject to greater threat than others;
    - The burden of reporting being placed on victims.
- The potential policy responses to the issue of gendered abuse and disinformation are multi-fold:
    - Social media companies can produce incident reports, which would help provide a context to content moderators. The platforms should also revise their AI classifiers regularly to

[8] Malign creativity is “the use of coded language, iterative, context-based visual and textual memes and other tactics to avoid detection.” Malign creativity impedes the identification of gendered disinformation and abuse in online spaces, as it has the potential to escape the classifiers used by the platforms in the detection process. Furthermore, platforms lack the “situational, cultural or sometimes […] linguistic knowledge” to catch malign creativity.

detect and tackle malign creativity. The participation of targets of gendered abuse and harassment in this process is desirable. Regarding social media regulation bills, instituting “transparency for reporting measures against these platforms” is necessary. This could allow for a view of the number of reports submitted, and actions implemented, especially those against the harassment of women and other marginalized groups on the platforms.

- Social media companies need to diversify their workforce, from engineers to content moderators. Working conditions of content moderators have to be improved and they have to be equipped with better knowledge on the subject and cultural contexts to comprehend intersectional contexts. Other employers also have a part to play in the response efforts, including the introduction of a support network for their employees facing the risk of gendered abuse and disinformation.
- The introduction of nudges and friction by some social media platforms have proven effective in some cases, and it is crucial to expand on these efforts. Introducing and enforcing proportionate penalties on repeat abusers is important, such as a “three strike policy” where the perpetrator is warned, and the account of the persistent abuser is

suspended for a few days after the first two incidents and banned after the third abusive act. It is also important to regularly review and amend the designation of targeted harassment.

Webinar Three: Fighting Gender-Based Hate Speech and Disinformation, and the Role of Social Innovation

25th May 2021

Humour Over Rumour

Audrey Tang, Digital Minister, Taiwan

Summary: Taiwan's Humour Over Rumour model is central to its battle against the infodemic. The use of digital space as a platform to educate, collaborate, crowdsource, and co-produce has been key to dispelling disinformation and establishing norms for pro-social interaction. The centrality of the role of the civic-tech community in Taiwan has allowed for the growth of digital democracy.

- Humour is an emotion that spreads faster than discrimination and vengefulness. Capitalising on the virality of humour is central to Taiwan's effective communication during the pandemic. This complements Taiwan's approach of "notice and public notice” over “notice and take down”, because of the latter’s proclivity for division. With a top-down takedown of information, the public might believe it to be a government conspiracy. Instead, Taiwan has opted for keeping disinformation online- labelling and correcting for disinformation within a frame that is humorous. Humour is also effective in countering geopolitical meta-narratives central to influence operations.

- The use of the Internet to facilitate crowdsourcing has been key to dispelling popular disinformation. Through inviting people to think collaboratively and engage in the remixing and dissemination of popular memes, disinformation is quickly corrected. Taiwan has also established a toll-free number for the public to report potential disinformation through call or text. Taiwan also relies on a community known as g0v which promotes community collaboration with members of the public equipped with media competency to contribute to fact-checking. To encourage collective intelligence, it is essential that the state builds its own platform. For example, the PTT Bulletin Board System does not have shareholders nor has it hosted advertisements, and is as such, not subject to marketing or stakeholder demands. Another example is the use of Pol.is- a pro-social conversation platform that Taiwan has used to crowdsource some of its laws and policies. It automatically highlights consensus rather than divisions, facilitating productive discourse rather than polarisation.

- To tackle the possibility of paying platforms to circumvent fact-checking apparatus, norms were developed such that all social media companies must offer advertisement for social and political issues to independent investigative journalists for analysis, in addition to a ban on foreign-sponsored propaganda on socio-political issues leading up to the election or referendum season.
- There are parallels in effective management of the pandemic and the infodemic. The infodemic can only be thwarted if people are granted access to universal broadband and media competency curriculum is considered a human right. It is essential to support research development and universal access to the production of "vaccines"- in the case of cyber space, social vaccines, by enlisting basic and lifelong education to allow participation in fact-checking. Lastly, there is a need to impose a strict quarantine rule for information, for example, during the election season such that fact-checkers are not overwhelmed.
- Beyond the pandemic, public service plays an important role in cultivating a vibrant civic-tech community and encouraging collaboration between the civic-tech community and the government. In the office of Taiwan's Digital Ministry, half of the staff is from career public service from more than 12 different ministries, with the other half being community civic technologists. This highlights the central role of citizens in policy making, and encourages innovation and collaboration from the drafting stage.

#Holdtheline

Maria Ressa, CEO and Executive Editor, Rappler

Summary: Technology has shifted globally, impacting information ecosystems and facilitating the exercise and retention of power through the control and manipulation of information. Facebook is now the world's largest distributor of news but lies laced with anger and hate spread faster and further than facts, and which means social media platforms deliver posts that are biased against facts and traditional journalism. Many journalists and activists find themselves targets of gendered disinformation and hate speech. Power today is often channelled through misogynistic and sexist discourse on the Internet, and although humour and memes on social media platforms can serve pro-social functions, it can also be used for disinformation and hate speech, with sexism and misogyny used as tactics.

- Online violence has real world impacts- online sexism and misogyny can translate to sexist gendered attacks:
    - A UNESCO report called "The Chilling: Global trends in online violence against women journalists" highlighted how Facebook was used to target Maria Ressa and Carol Cadwallider, the latter of whom broke the Cambridge Analytica story.

    - A recent study by the International Centre for Journalists (ICJ) in partnership with Rappler reveals that across more than 130 countries, 73% of female journalists reported experiencing online abuse, 25% received threats of physical violence, and 20% have been attacked or abused offline.
    - Focusing on Ressa as a case study, 60% of the online violence sought damage to Ressa's credibility as a journalist, including disinformation-laced attacks and false claims that she peddles "fake news". 40% of the attacks are classified as personal, featuring significant sexism, misogyny, and explicit language, including orchestrated attacks on physical appearance, skin colour and sexuality, manipulated images of her, and threats of rape and murder. The attacks increased following high-profile media appearances from Ressa, including International awards and court appearances, and Rappler's published investigative reports into the Duterte administration.
- Attacks against journalists in the Philippines often employ dehumanising narratives and they are often orchestrated by a network- two profiles belonging to this network have worked with the government. Mocha Uson, for example, is still a government official. The Hype Machine, a book by Sinan Aral, describes the new advertising- where posts on social media are gathered as data by the medium, and a

model of the individual is generated by machine intelligence, and the profile of the individual’s vulnerability to messaging will be sold to the highest bidder. The advertising-driven model has made social media platforms behaviour modification systems.

- Geopolitical power play is also mapped onto cyberspace in the form of influence operations. For example, Russian disinformation networks that attacked the U.S. were also active in the Philippines through the alt-right in Canada. In September last year, Facebook took down a Chinese influence operation that was targeting all of Southeast Asia and had seen particular success in the Philippines where it campaigned for the daughter of President Duterte for President.
- Rappler’s response to the problem is guided by three pillars- Technology, Journalism, and Community. Governments should put guard rails on technology, to prevent the insidious manipulation of its people, as well as to collaborate with and help independent journalism survive. Finally, community is critical but is susceptible to disinformation spread through online platforms, exemplified by the rise of Donald Trump and QAnon. This has lasting effects on society because if facts are debated, truth becomes elusive, which translates to a decline in trust. The lack of trust and a shared reality not only impacts democracy, but also makes it impossible to deal with larger existential problems (e.g., climate change, the COVID-19 pandemic). As such, the relationship between technology and development is mediated by

governments and their willingness to protect the facts and their commitment to building reliable institutions.

Examining the Impact of COVID-19 on Online Misogyny

Priyank Mathur, Founder and CEO, Mythos Labs

Summary: A report by Mythos Lab in collaboration with UN Women on the impact of COVID-19 on online misogyny revealed that the volume and engagement with misogynistic content increased during the pandemic, sexist organisations are spreading new COVID-related narratives, and misogynistic Twitter accounts are disproportionately affecting the attitudes of their followers. This highlights that the need to counter misogynistic narratives online is especially pertinent during the pandemic, and digital literacy, as well as humour, provide ways to counter online misogyny.

- The posts examined on public groups of self-proclaimed misogynist organisations reveal a three-fold increase in the amount of misogynistic Facebook posts in 2020 compared to 2020 (from about 400 posts to 1,200) across India, Sri Lanka, and Malaysia. The number of posts and engagements with them fluctuated with COVID-19 measures, peaking during the strictest phases of lockdown. Similar trends were observed on Twitter in India, Indonesia and Philippines (three of the biggest Twitter markets in Asia). Searches for misogynistic terms like “Feminazi” for example, a commonly used term amongst misogynist circles, also spiked during lockdown.

- A growing concern is the use of COVID-19 by misogynist organisations to spread new narratives, often through memes and social media posts. Some of the common narratives in Sri Lanka and Malaysia on Facebook feature COVID-19 as a conspiracy to antagonise men, men being the real victims of domestic violence, and how laws discriminate against men (because many divorced men could not see their children because of lockdown). Wives have been compared to the virus, and in India, online posts have called for men to be the targets of economic packages distributed by the government as the virus is "worse on men". This suggests the need to consider malicious online activities including trolling and misogyny when instituting lockdowns.
- The report also explored whether the rise in COVID-related misogynistic content has moved the needle on people's opinions. It was found that the average person in Indonesia was 25% more likely to develop misogynistic opinions after being exposed to the tweets of misogynists. In India, the statistic is 20%, and in the Philippines, 19%.
- Digital literacy is key to countering viral lies with viral truths and penetrating echo chambers. Besides building women's social media literacy and knowledge on how to report hate speech, Mythos Lab works with communities, local comedians, and local influencers to produce and disseminate videos that use humour unique to different contexts to counter gender stereotypes.

- On a policy level, whether its state of social media companies, it is important to recognise that misogynist hate speech is its own subcategory. The proper categorisation of hate speech directed at women as distinct will aid in the removal of such content. Providing an argument from capital interest, it is in social media companies' economic interest to safeguard its users against hate speech and disinformation to avoid a backlash from a public that is increasingly cognisant. There also has to be an awareness and caution when it comes to small encrypted private platforms because of the difficulty to regulate information in those spaces.

This Event Report on the webinar series will be followed by a policy report and an edited volume which share the same thematic thread centred on gender and security in cyberspace.