Ponder the Improbable since 1996

A NATIVE WPS AGENDA FOR ASEAN

SECURITY IN DIGITAL SPACE

Policy Report

February 2022

Tamara Nair

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

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Policy Report

A NATIVE WPS AGENDA FOR ASEAN
SECURITY IN DIGITAL SPACE

Tamara Nair

February 2022

TABLE OF CONTENTS

Executive Summary

Assuming gender neutrality in digital space does little for gender equality in digital space. This report suggests using the agenda of UN Security Council Resolution 1325 (UNSCR1325) on Women, Peace and Security (WPS) as a framework for addressing issues of gender inequality and violence against women (VAW) in the digital world and indigenising it for ASEAN. The application of this framework goes beyond its provenance in conflict and draws on its roots in human security. The gendered impacts of digital technology and their connection with peace and security are a serious policy blind spot. Adopting the WPS narrative as it stands, created and propagated by mostly North America and Europe, means it does not allow an indigenous interpretation, which might be what is necessary when it comes to ASEAN. Currently the agenda is bereft of a cultural context, which is vital to its realisation in other parts of the world. If ASEAN seeks to move the agenda forward, it has to start with WPS projects that have resonance with all member states, and the agenda should ideally be approached from a human security angle that is relevant to current times, especially in the areas of economic security, digital security and climate security. The year 2021 marked the 21st year of UNSCR1325 and it seems timely that the agenda itself should mature and move into new terrains to address gender equality in new spheres of operation. The digital space and the impending Web 3.0 are presented here as ideal environments for doing so.

Introduction

Gender inequality and gender-based violence in the digital world, as in the physical world, are indicators of more widespread social fractures and disruption. Yet we do not see much action in addressing this policy blind spot when we look at the digital security architecture and governance of the virtual space. Much like in the physical realm, the idea of women's equality in general, and their safety and well-being in particular, has been under-securitised in this new arena and there really is little movement in addressing this gap in policy discussions, despite the fact that we very much live digital lives today. Much of this has to do with the limited data on women's presence in, and usage of, the digital space.

Digital technologies have only served to intensify the tensions between national security and the security of individuals, and the policies or laws set in place to ensure such security in the digital ecosystem. The orientation of digital data — its indifference to people and places[1] — sheds light on the fragility of legal knowledge, which becomes "increasingly 'undone' by digital technologies and future-oriented security practices".[2] To address these rapid changes, policymakers have opted to explore areas of non-knowledge as they emerge in controversies of mass surveillance, fraud, harassment, and the like, as they would in the physical realm, through systems of governance that, once again, leave out groups of interest, be it women, sexual minorities or other minority groups. What is required is to advance more critical approaches to security, especially for the protection of women, and to engage with different areas of security studies, including assessing available international frameworks that can be used to add a level of buoyancy and longevity to digital security policies. While existing legal frameworks form the background to policy formulation, new areas of knowledge can act as the bare bones upon which to build what will undoubtedly be an organic construct, growing and expanding to keep up with the digital "Proteus".

This report provides a brief overview of gendered inequalities in the digital ecosystem and offers recommendations based on the four pillars of the WPS agenda. The pillars —prevention, protection, participation, and involvement in relief and recovery — provide a new framing through which the security of women might be ensured in digital space. Given the importance of digitalisation in the region, the impending Web 3.0, and the increasing uptake of the WPS agenda in ASEAN, the report aims to merge these interests to create a native WPS agenda that resonates with all ASEAN member states.

[1] Claudia Aradau, "Assembling (Non)Knowledge: Security, Law, and Surveillance in a Digital World", *International Political Sociology* 11 (2017): pp. 327–342

[2] Claudia Aradau, "Assembling (Non)Knowledge", p. 329

This report is based on a longer investigative piece on the WPS agenda in digital space written by the author for the upcoming edited volume, *Gender and Security in Digital Space: Hate Speech, Disinformation, and the Evolving Threat Landscape.*[3]

[3] Tamara Nair, "The Women, Peace and Security Agenda in Digital Space", in *Gender and Security in Digital Space: Hate Speech, Disinformation, and the Evolving Threat Landscape,* eds. Ang Benjamin, Gulizar Haciyakupoglu and Yasmine Wong (forthcoming).

Old Threats, New Spaces

Since the passing of UN Security Council Resolution 1325 (UNSCR1325) on Women, Peace and Security (WPS), the WPS agenda has been gaining traction.[4] The agenda is the most highly recognised, significant global framework for addressing "gender equality in military affairs, conflict resolution and security governance".[5] The agenda has its provenance in conflict in the 1990s, namely, but not isolated to, the Serbian and Rwandan wars' impacts on women and girls. There is massive literature surrounding the agenda over the two decades of its existence. However, the focus here is on, as Laura Shepherd writes, "the rather porous borders of the agenda and the extent to which the agenda must change to address new problems"[6] that affect already imbalanced gender relations. The 21st year of the agenda marks new and evolving threats to the security of women in a new space, but dragging along with it the old threats to one group, which, despite forming 50 per cent of the world's population, is seen as a minority interest in security planning.[7] But, given the maturity of the agenda, it now seems poised to take on these new challenges facing women — starting from harassment, exclusion, and downright threat to life — in the new digital space.

There are as many reports, blogs, articles, protests and even laws against threats to or harassment of women online as there are actual incidents of violence faced by women in the digital space. Yet we do not necessarily see an abatement of these unlawful and dangerous activities despite much-needed "noise" brought up by women's groups and human rights advocates. This is unfortunately evidenced by examples ranging from suicides of prominent female artistes as a result of cyberbullying[8] and cases of "revenge porn"[9] being spread online by

[4] Resolution 1325 (2000) introduces the WPS agenda, while the remaining resolutions modify/add on to it.

[5] Soumita Basu, Paul Kirby, and Laura J. Shepherd, "Women, Peace and Security: A Critical Cartography", in *New Directions in Women, Peace and Security*, eds. Soumita Basu, Paul Kirby and Laura J. Shepherd (Bristol University Press, 2020), p. 1

[6] Laura J Shepherd, "Knowing Women, Peace and Security: New Issues and New Modes of Encounter", *International Feminist Journal of Politics* 22, no. 5 (2020): pp. 625–628

[7] Abigail S. Post and Paromita Sen, "Why can't a woman be more like a man? Female leaders in crisis bargaining", *International Interactions* 46, no. 1 (2020): pp. 1–27.

[8] Hayden Marks, "Cyberbullying and the Tragedy of Hana Kimura", *The Diplomat*, 5 June 2020, https://thediplomat.com/2020/06/cyberbullying-and-the-tragedy-of-hana-kimura/ .

[9] Tahlee Mckinlay and Tiffany Lavis, "Why did she send it in the first place? Victim blame in the context of

disgruntled former or current intimate partners to death threats and hate speech,[10] with a particular feminist twist, directed at women who may be exercising their freedom to express opinions on a social media platform. Add to this how women are sometimes marginalised in online commerce or, worse, harassed, based on their activities or presence in e-commerce platforms.[11] Such behaviour can negatively affect a country's potential for economic growth and development. According to Plan International, if 600 million more women were connected to the internet, it would translate to a rise in global GDP of US$13–18 billion.[12] The online space then has become an extension of the physical world, where inequality and discrimination has diffused through the technological boundary.

We think of technology as being gender neutral but it is in fact highly gendered at its very inception. At a recent virtual dialogue held by *Foreign Policy* magazine in collaboration with the One Earth Future Foundation, which examined the WPS agenda for the digital age, one of the panellists noted that the creators of current digital technologies failed to create platforms where all individuals would be safe simply because they came from a world where their own safety was never threatened in similar ways.[13] The social context within which new technologies are created and later embedded is where misogynistic behaviour resides and, therefore, women continue to face old threats, now in new places. Suppression of one's freedom of speech and expression, "cyber-touch",[14] breach of dignity, and violation of privacy all constitute violence against women (VAW). Although 74 per cent of countries around the world have passed legislation on cybercrimes, they

[10] Jennifer Scott, "Misogyny: Why is it not a hate crime?" BBC News, 15 March 2021. https://www.bbc.com/news/uk-politics-56399862; Jennifer Piscopo, "Being a woman in politics shouldn't come with death threats", *Ms*, 12 February 2020, https://msmagazine.com/2020/12/02/violence-against-women-being-a-woman-in-politics-shouldnt-come-with-death-threats/

[11] Yasmin Ismail and Hiral Hirani, "Addressing the Gender Dimension of E-commerce: Towards a Holistic Analytical and Policy Framework", CUTS International, Geneva, 2021, https://www.cuts-geneva.org/pdf/KP2021-Study-Gender_Dimension_of_E-Commerce.pdf

[12] Plan International, "Bridging the Gender Divide", n.d., https://plan-international.org/education/bridging-the-digital-divide; and *Intel* Newsroom, " Intel announces ground breaking 'Women and the Web' report with UN Women and State Department", 10 January 2013, https://newsroom.intel.com/news-releases/intel-announces-groundbreaking-women-and-the-web-report-with-un-women-and-state-department/#gs.mt9vxh

[13] Kara Swisher, speaking at virtual dialogue on *Women, Peace and Security for the Digital Age: Putting Gender on the Tech Agenda,* Foreign Policy (magazine) in collaboration with Our Secure Future programme of One Earth Future, 6 May 2021, https://oursecurefuture.org/news/virtual-dialogue-women-peace-security-digital-age

[14] This is a term coined by the UN Broadband Commission for Digital Development. See Working Group on Broadband and Gender, UN Broadband Commission for Digital Development, "Cyber Violence Against Women and Girls: A Worldwide Wake-Up Call", Discussion Paper, 2015. https://www.broadbandcommission.org/Documents/reports/bb-wg-gender-discussionpaper2015-executive-summary.pdf

lack adequate mechanisms to effectively address online VAW, with concurrent failures in law enforcement.[15]

Women and Web 3.0

The seemingly most important technology of humankind — the internet — has seen two stages of evolution and we are now at the start of the third.[16] Based on its decentralised nature of content creation, ownership/servers and storage of data, the evolving stage, known as Web 3.0 or Dweb, is said to release users and governments from the power and influence of tech giants like Facebook, Google and Amazon that now have full access to user information. If authorities wish to regulate cyberspace in some form, Web 3.0, moving away from the powerful companies that now own and store people's data, might prove the liberal way of doing so. However, there are still serious concerns about the desirability of such a state.[17] The policing of cybercrimes such as hate speech, child pornography and online harassment, to name a few, will be difficult in Web 3.0, given its lack of central control and access to data at specific sites.[18] Web 2.0, a platform that enabled us to create content and participate in social networking and sharing sites, was created mostly by men with limited, if any, input from women and minority groups. Web 3.0, to be used and created by anyone in the world, cannot be left to be designed by a homogenous group, i.e., a male-dominated system. With concerns of online VAW already rampant now, we do not want to see a proliferation of sites and data in this burgeoning space that would perpetuate such attacks and abuse. This is all the more reason why the involvement of women should factor strongly in the creation of this new digital world.

[15] Anita Gurumurthy and Amrita Vasudevan, "Equality, dignity and privacy are cornerstone principles to tackle online VAW", Women, Peace and Security Blog, London School of Economics, 4 December 2017, https://blogs.lse.ac.uk/wps/2017/12/04/equality-dignity-and-privacy-are-cornerstone-principles-to-tackle-online-vaw/

[16] Charles Silver, "What is Web3.0?", *Forbes*, 6 January 2020, https://www.forbes.com/sites/forbestechcouncil/2020/01/06/what-is-web-3-0/?sh=75965c7c58df

[17] Edina Harbinja and Vasileios Karagiannopoulos, "Web 3.0: The decentralised web promises to make the internet free again", *The Conversation*, 12 March 2019, https://theconversation.com/web-3-0-the-decentralised-web-promises-to-make-the-internet-free-again-113139

[18] Edina Harbinja and Vasileios Karagiannopoulos, "Web 3.0".

WPS in ASEAN — An Indigenising Methodology

The operationalising of the WPS agenda has seen a mixed bag of positive and not so positive responses, as it is realised in its conventional understanding. At the international level, there have been many rhetorical promises by various international agencies, not in the least the UN Security Council itself, which has committed itself to implementing the agenda in international security and peace-building through concrete action that includes the promotion of greater gender balance in UN military and police contingents.[19]

One particular way of assessing levels of acceptance and success has been the adoption of national action plans (NAPs) by countries. But this too has shown the width of interpretation of the agenda rather than some form of universal acceptance in terms of women's role in international security.[20] The lack of an NAP, however, should not discount the good that has been done in some ASEAN member states in the area of gender equality and women's rights. All member states have constitutional mechanisms to **protect** women and girls, allow for their free **participation** in social, political and economic lives, **prevent** VAW, and involve them in post-crisis **relief and recovery**. In fact, one could say, the pillars of the WPS agenda are being realised in the ASEAN countries, to varying extents, without actually engaging in the technical details. But the traditional (North American/European) understanding of the agenda limits its realisation in different parts of the world, including Southeast Asia. Its focus on countering violent extremism and armed conflict as well as peace negotiations and mediations, although vital to the stability and security of the region, will not easily resonate with all states, which is a pity because it prevents the agenda from moving beyond its original intent. The four foundational pillars should also be understood in the cultural contexts within which they will operate. Such a context is coloured by many factors in the region, including but not limited to: a colonial past and post-independence challenges, rapid export-led economic development, and of course the diverse cultures and religions that encapsulate lives.

VAW is often like the idiomatic canary in the coal mine for wider implications of unrest and conflict in society, regardless of whether that gender-based violence is in the physical or digital world. Increasingly, sophisticated

[19] Chantal Oudraat and Michael E. Brown, "Gender and Security: Framing the Agenda", in *The Gender and Security Agenda: Strategies for the 21st Century*, eds. Chantal Oudraat and Michael E. Brown, (Routledge, 2020), pp. 27.

[20] Chantal Oudraat and Michael E. Brown, "Gender and Security".

technologies have created new means of violence against, surveillance of, and squashing opposition from, women. While the WPS agenda has focused on conflict situations, its attention in the digital world is long overdue. Harm in the virtual world can be experienced in reality with severe consequences.[21] All of us, regardless of gender or socioeconomic status, live digital lives in some form or another. One common area of interest and advantage for ASEAN member states is the digital lives of the people of the region. Web 3.0 and its blockchain technology, with its links to cryptography, will be an area of both policy and academic interest. The new internet will require varied architects. A more diverse, inclusionary environment must be created, especially in light of potential security concerns. One way we can engage the WPS agenda in a unique way then is to incorporate it specifically into regional and national digital security policies, specifically when discussing Web 3.0.

The following are some recommended actions for ASEAN, structured along the four pillars of the WPS framework.

[21] Amnesty International, "Amnesty reveals alarming impact of online abuse against women", 20 November 2017, https://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

Recommendations

WPS Pillar: Prevention

1. Reassess digital security policies with the explicit intention of including "vulnerability" as an area of engagement in preventing online VAW.

   It would be in the best interest of both public and private security entities to review their current digital security policies for gaps in understanding how vulnerability manifests for women. In identifying these gaps, we will be better equipped to realise the shortcomings of existing methods of preventing forms of harassment and abuse against women. From this step, we can move on to creating more targeted responses to online VAW and also identifying groups that need to be consulted in policymaking.

WPS Pillar: Participation

2. Redefine/widen definitions of "security", "knowledge" and "vulnerability" with the explicit intention of including greater diversity in digital security policies.

   Effective and sustainable policies are ones that incorporate consultations with a broad base of participants to ensure diversity, and digital security policies should be no different. But before this can happen, we need to redefine traditional notions of what we mean by "acceptable" knowledge, how we see "vulnerability", and our reaction to it, and even the very notion of "security" itself, given that threats to a nation and its people no longer present themselves in the traditional manner of outright wars. By widening definitions, we realise that generic digital security policies cannot apply to all users if the intention is to keep everyone safe and able to exercise their right to participate in this public space. For example, the creation and governance of digital technologies as well as the securitising of digital space has been a very gendered affair — omitting women and non-binary groups. Hence, this particular pillar focuses not only on including women in discussions of digital security, but also on enabling them to direct conversations and shape the agenda. This will be vital in the Web 3.0 world.

WPS Pillar: Protection

3. Collect disaggregated data on harassment/violence against different groups of users of digital space.

   This will require an openness to accepting different forms of knowledge production as important in security dialogues. With this comes the appreciation of having diversity in data collection and analysis and in the different types of knowledge that will drive this endeavour. It is only through a broad capture of data and information that effective, evidence-based policies can be formulated. It is exactly such policies that are required for greater protection from VAW, both in the virtual and physical worlds. The usage of such data can be stored and regulated closely at decentralised levels in the new Web.

WPS Pillar: Relief and Recovery

4. Focus on women's participation and feedback/knowledge, especially in rebuilding efforts after crisis situations such as a global pandemic or a financial downturn.

   After a crisis, the usual pattern is to fall back on known and comfortable ways of acting and doing, rather than using the crisis as an impetus for change for the better. The relief and recovery pillar is often overlooked notwithstanding the importance of preventing VAW and continuously protecting women from VAW during relief and recovery operations. But it is this pillar that provides the most relevant information pertaining to harassment and abuse in both the digital and physical spheres because it speaks out of lived experiences, especially in the aftermath or at the tail end of an upheaval. This is especially so for the digital world, given people's ever-increasing presence in this arena and the move towards more decentralised usage under Web 3.0.

Conclusion

Violence against women is increasingly taking hold in the digital sphere and there is a vital need to address this policy blind spot. The safety and security of any user in the digital space should not be compromised because that would simply lead to the security of all users being compromised in time to come. What is needed is a conscious effort by policymakers, at all levels of governance, to be cognisant of that fact and to act in a manner that upholds the rights and dignity of all. The WPS agenda provides a framing that can help in this regard. Not only is it wise for ASEAN to use an established international instrument and be ahead of the curve in the new Web 3.0, but the grouping could also lead in prompting other nations and regions to adopt native plans for the agenda, thereby increasing its use, importance and relevance to today's security dilemmas and new digital space.

About the Author

Dr Tamara Nair is Research Fellow at the Centre for Non-Traditional Security Studies (NTS Centre) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University. She graduated from the National University of Singapore (NUS) with a Bachelor's Degree in Political Science and Geography and went on to train at the National Institute of Education (NIE). She obtained a Masters in Environmental Management, a Graduate Diploma in Arts Research and a PhD in Development Studies from the University of New South Wales in Sydney, Australia. She also possesses a Professional Certificate in Project Management by the Institute of Engineers, Singapore and Temasek Polytechnic. She is also the coordinator of centre publications and Research Integrity Officer for RSIS.

Dr Nair's current research focuses on issues of power and the biopolitics of labour and technology, movements of people in Southeast Asia, and the Women, Peace and Security (WPS) agenda in the region. She is Singapore's representative of the ASEAN Women for Peace Registry and has authored the 2018 Human Rights and Peace Education Report for Singapore. She is also the representative for Nanyang Technological University for the ASEAN University Network on Human Rights and Peace Education. She has published in Development Studies journals; writing on marginalised communities and sustainable development, issues of gender, and power and subject creation.

About the Centre for Non-Traditional Security Studies (NTS Centre)

The **S. Rajaratnam School of International Studies (RSIS)** is a think tank and professional graduate school of international affairs at the Nanyang Technological University, Singapore. An autonomous school, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. With the core functions of research, graduate education, and networking, it produces research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, Cybersecurity, Maritime Security and Terrorism Studies.

NTS Centre conducts research and produces policy-relevant analyses aimed at furthering awareness and building the capacity to address non-traditional security (NTS) issues and challenges in the Asia Pacific region and beyond. The Centre addresses knowledge gaps, facilitates discussions and analyses, engages policymakers, and contributes to building institutional capacity in Sustainable Security and Crises. The NTS Centre brings together myriad NTS stakeholders in regular workshops and roundtable discussions, as well as provides a networking platform for NTS research institutions in the Asia Pacific through the NTS-Asia Consortium.

For more details, please visit www.rsis.edu.sg and http://www.rsis.edu.sg/research/nts-centre. Join us at our social media channels at www.rsis.edu.sg/rsis-social-media-channels or scan the QR code.

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

Nanyang Technological University, Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg