T20 Policy Brief

G20 BRASIL 2024

T20 Brasil 2024 Let's rethink the world

Task Force 05

INCLUSIVE DIGITAL TRANSFORMATION

Enabling Social Inclusion through Human-centered Approaches to Cybersecurity

Jaimee Stuart, United Nations University, (Macau, SAR, China)

Mamello Thinyane, University of South Australia (Australia)

Keith Detros, Tech for Good Institute (Singapore)

TF05

Abstract

While asymmetries in digital access are decreasing globally, inequities in digital skills and opportunities are expected to increase, alongside exposure to cyber threats, cybercrime, and online violence. Even with growth in global cybersecurity investments seeking to protect the confidentiality, integrity, and availability of digital infrastructure and resources, individuals, businesses, and nation-states still face increasing cyber risks. There is a disproportionate prevalence of cyber insecurity and greater negative impacts of cyber threats on marginalized individuals and communities, particularly women and girls. These issues undermine social inclusion, reduce trust, and stymy economic growth and the lack of progress in attending to them. This alludes to inadequacies in our current efforts that are exacerbated by technocentric framing of cybersecurity.

To effectively support social and digital inclusion, a key theme in the G20 Digital Agenda, cybersecurity policy-making needs to move beyond a focus on the security of digital artifacts to centralize the protection of the rights and freedoms of individuals and communities. This human-centered approach focuses on the role human factors play in perpetrating, preventing, and responding to cyber risks and broadens our prevention and intervention efforts to reduce individual level harms to health and wellbeing and sociocultural harms such as exclusion and lack of trust. This policy brief extends the current narratives around cybersecurity and makes recommendations on ways for the G20 to effectively position humans (rather than technology) as the primary subjects of cybersecurity. Framing cybersecurity from this perspective harmonizes states' commitments and aspirations to respect human rights, to promote the development of the digital economy, and to reduce risks to international peace and security.

Keywords: Cybersecurity, Human-Centric, Human Rights.

Diagnosis of the issue

Digital transformation has resulted in much of economic and social life now being carried out in cyberspace, with most nations currently relying heavily on the digital sector. The exponential rise in the use of digital technologies has created challenges in cybersecurity including novel attack vectors for cybercriminals and hackers who are using increasingly sophisticated methods to target digital assets and infrastructures and threaten social stability. The World Economic Forum Global Risks Report (WEF, 2023) listed cybersecurity in the current and future top 10 risks and highlighted the increased interconnections and complexity among cybersecurity, societal, geopolitical, economic, and environmental future threats. The global importance of this issue is underscored by investments in the industry, which are estimated to be growing at 9% annually.

Despite the growth of the industry, cybercrime is increasing and is estimated to cost $10.5 trillion per year internationally by 2025. Beyond the economic impacts, cyber insecurity has wide-ranging harms; it degrades trust and social cohesion, causes reputational damage, undermines access to and availability of critical infrastructure and services (e.g., telecommunications, finance, and healthcare), and reduces individual and social well-being. The negative outcomes of cyber insecurity have disproportionate impacts on marginalized individuals and communities including women and girls, young people, and older populations. Given the importance and costs of this issue, there has been little headway made in mitigating cyber threats, suggesting that current approaches to cybersecurity may be insufficient in our contemporary global context.

Traditionally, cybersecurity has treated technology artifacts as the target of protection, thus aiming to ensure the confidentiality, integrity, and availability of digital resources (i.e., infrastructure, systems, software, and platforms) and the information contained

therein. This framing is limiting our ability to address existing and interconnected security issues resulting from the omnipresence of digital technologies and their integration with all aspects of life.

- Cybersecurity is predominantly treated as a technical issue due to its basis in computing and technical disciplines that are predominantly located in academic, business, or military installations, and as such expertise has also been siloed in these areas. However, digital transformation has resulted in a ubiquitous infrastructure that connects nearly all people and if disrupted impacts personal and societal functioning. While human and societal dimensions of cybersecurity are recognized, technical expertise and digital harms are still over-represented in policy discourse (e.g., national security and cybersecurity strategies).

- Key voices are under-represented in cybersecurity decision-making. Although digital transformation and cybersecurity impact everyone, leadership in cybersecurity (e.g., governance, product design, digital strategies) is largely the purview of technologists. The lack of participation of key population groups (e.g., women and youth), leads to instrumental deficits, ineffective products and short-sighted strategies that may undermine commitments to social cohesion and equality. Furthermore, the cybersecurity discourse tends to be inaccessible and may be marginalizing due to the widespread masculinised norms that inform design, defence, and response practices in cybersecurity (Miller, Shires, & Tropina, 2021; Stuart, 2024).

- States and organizations are privileged over individuals as the referent objects of security which means that security goals are shaped to serve the interests of states, sometimes at the expense, or even in direct opposition to, human rights and freedoms. While balancing individual versus national security imperatives can be challenging, these goals are not mutually exclusive and can be reinforcing if both are valued and privileged.

- Risk management practices focus too narrowly on the prevention of known risks and miss opportunities for resilience. Efforts to prevent cyber incidents are critical but emerging technologies (i.e., Artificial Intelligence) create new vulnerabilities and novel attack vectors to bypass security systems and processes. Cyber-resilience, or the ability to resist, respond, and recover from cyber threats suggests that despite the probability of known or unknown risks, threats can be mitigated to minimise long-term negative effects, and potentially promote positive adaptation. The resilience perspective strengthens the capabilities for society's continuity and adaptation in a climate of persistent cyber risks (Detros, 2023).
- While the technocentric focus of cybersecurity may suffice for some elements of the ecosystem (e.g., critical infrastructure and operational technology), by including human-centric approaches that prioritize the protection of rights and freedoms, improve resilience, and recognize social functioning as the primary referents of cybersecurity, the G20 policymaking can become more future-focused.

Recommendations

This policy brief presents four key recommendations that highlight human-centric approaches as a critical way of improving cybersecurity investments, promoting cyber-resilience, and supporting social cohesion. Notably, human-centric approaches are intended to reorient and supplement, not supplant, technical cybersecurity efforts. They act to refocus existing work and recognise that cybersecurity goals, such as confidentiality, integrity, and availability, already centralise humans as critical agents of risk and protection.

- Reaffirm commitments to human-centred approaches to cyber-resilience through the G20 Brazil Declaration. The G20 New Delhi Declaration in 2023 included a commitment to creating safety, security, and resilience in the digital ecosystem. Building on this common vision, it is recommended that the G20 Declaration in Brazil reaffirm countries' commitments in 2024 by adopting a human-centred approach to cybersecurity, one that upholds human rights and freedoms for a digital future. The declaration is also an opportunity to elevate the discussions from cybersecurity to cyber-resilience. Traditionally cybersecurity has connoted mechanisms of prevention and protection, both of which are oriented towards known threats. In contrast, cyber-resilience suggests that in a constantly evolving threat landscape, the probability of facing adverse (often unknown) cyber events is high and that the best way of mitigating the resultant harms is to be adaptable. It is key to highlight that cyber-resilience not only concerns bouncing back, or recovering functionality after a cyber-attack, but also bouncing forward, or responding in a way means the target is better able to manage future events. This change in discourse facilitates a mindset shift among various stakeholders to continually pursue

capacity building, develop innovative frameworks, and leverage emerging technologies to keep pace with the increasing sophistication of cyber threats while also investing in baseline prevention and protection against known threats.

- Establish a G20 Cybersecurity Knowledge Hub. Cybersecurity discourse tends to be highly technical meaning that information, prevention, recovery, and resilience mechanisms are mainly accessible to cyber professionals. Digital transformation has created a context whereby technology is central to work and life and where personal and professional device use are inseparable, meaning that cybersecurity is the responsibility of all citizens. Therefore, it is important to democratize information and to empower people to take an active role in creating safe and secure digital environments. To create pathways by which citizens, especially those who are most marginalized, are empowered to protect their digital security, awareness needs to be raised and capacity-building opportunities resourced. It is recommended that the G20 create a publicly available knowledge hub for cybersecurity information supported by public and private partnerships where governments and industry can share evidence-based training materials, videos, reports, and data. This would be similar to the Global Infrastructure Hub, which is also a G20 Initiative, where resources to advance G20's infrastructure agenda are collated on a knowledge-sharing platform. A knowledge hub could be a general tool to support individuals and organizations but would also raise awareness and offer support mechanisms for those who face disproportionate cyber risks but who are often under-resourced. Notably, civil society organizations and non-profit organizations; women, girls, and those who advocate for them; human rights defenders and journalists (Stuart, 2024). Such a hub may also address the multi-dimensional gaps in the cyber workforce by encouraging skills development (Thinyane, Christine, & Detros, 2022).

- Embed multistakeholder approaches in cybersecurity policymaking (e.g., national strategy formulation) in G20 countries. Creating learning opportunities and fostering awareness is a critical step in human-centric cybersecurity that has important flow-on effects on social inclusion. However, this is insufficient as there needs to be formal mechanisms for key population groups to meaningfully participate in the creation of national strategies and cybersecurity policies. By including a diversity of under-represented voices, the G20 will be able to develop a holistic understanding of safety and security within the global digital ecosystem. Also, this would ensure that policies are responsive to the needs of various stakeholders. As a best practice, the International Telecommunications Union's Guide to Developing National Cybersecurity Strategy (2021) highlights the importance of consulting a broad range of stakeholders to develop a shared vision of what a robust cybersecurity policy may look like. The guide itself is a product of collaborations from multiple stakeholders across the public sector, businesses, academia, thinktanks, civil society organisations, and international organisations. The G20 is recommended to implement similar and consistent approaches to consultation on cybersecurity where diverse and meaningful participation is centralised.

- Creation of a G20 toolkit to promote human-centric cybersecurity incident response. Cybersecurity incident response mechanisms tend to focus on the technical aspects of a cyber-attack, such as identifying the source, patching the systems, containing the threat, recovering data, and restoring functionality. While such responses are crucial, these need to be complemented by user-centric approaches that attend to the harms felt at the individual or social level. Aside from networks and data, people and communities are the primary victims of cyber incidents and may experience wide-ranging negative outcomes such as lost economic opportunities, reputational damage, loss of trust, and

poor mental health – none of which are the focus of traditional incident responses or recovery efforts (Stuart, 2024).

To facilitate the adoption of human-centric approaches to incident response, the G20 can develop a toolkit for response teams so that they can better help those affected by cyber incidents. Psychosocial support and assistance are also sorely needed to manage the emotional and psychological impacts of cyber threats. Gender and cultural sensitivity training among cyber professionals should also be considered as a best practice to ensure that fit-for-purpose responses are respectful and do not further marginalize vulnerable groups. A toolkit on human-centric cyber incident responses can preserve trust and cohesion among users in times when their vulnerabilities have been exploited and reduce the costs and losses of non-technical harms that follow from adverse cyber incidents.

These recommendations are high-level principles and shared values to commit to during the G20 Summit. The aim is for these recommendations to be adopted by G20 economies into country-specific policies, but also to be a part of a collaborative and cumulative effort to create more effective response mechanisms.

Scenario of outcomes

The rapid advancement of digital technologies, their potential for social and economic development, and the likelihood of being left behind in the ever-evolving digital landscape have meant that ICTs have become critical to the fabric of social and economic life. However, digital transformation is inextricably imbued with tensions for development, well-being, and inclusion. For example, social media enables connectivity among geographically dispersed groups and has allowed for the proliferation and democratization of media production. Yet, these media contribute to polarization, misinformation, and radicalization as well as create the conditions for online harassment, hate speech, and trolling (Stuart & Scott, 2020). Platform-mediated gig work has enabled efficiencies in service, transportation, and accommodation industries, but has also contributed to employment precarity, labor vulnerability, and privacy breaches. Generative artificial intelligence has enabled efficiencies across industries but has also contributed to job loss and increases in sophisticated cyber scams, deepfakes, and online violence. At the crux of these issues is the question of what societies choose to value and prioritize, as all areas of digital development also come with cyber risks and potential harm to individuals, businesses, and nations. This policy brief aims to orient to these issues and to encourage the G20 towards cybersecurity solutions that prioritize and privilege well-being and social inclusion.

As we become more reliant on, and our lives more interconnected with, digital technology the role of cybersecurity policies and strategies is more complex than ever. Policies must now articulate and reflect societies' desired digital future which, while supported by the protection of data, networks, and systems, primarily concerns the peace, security, and well-being of citizens. Policies and strategies must also guide and anchor

private sector innovations that are predominantly driven by business and profit motives to the detriment of individual, social, and environmental outcomes. Additionally, policies must set the framework for good citizenship behaviours within a global, digital public space.

At the political level, adopting human-centred approaches to cybersecurity within the G20 means that citizens must be engaged in decision-making processes, such as the formulation of national cybersecurity strategies. Citizens need to be able to meaningfully contribute to shaping cybersecurity strategies in ways that centralize human factors and outcomes, specifically prioritizing experiences and harms resulting from adverse cyber incidents. Furthermore, the discourse of cybersecurity must shift to make cyber protection, prevention, and resilience more accessible, empowering citizens to reduce vulnerabilities, mitigate threats and become more engaged in cybersecurity (e.g., in incident reporting). More importantly, such an approach must ensure that vulnerable and marginalized groups are included, thus stymying the effects of digital divides and exclusion.

Human-centred approaches to cybersecurity allow for a focus on enhancing the capabilities of people in ways that value and respect their agency and freedoms, effectively supporting secure behaviours, as opposed to treating humans as distrusted entities to be controlled, constrained, and restrained. Further, the burden of cybersecurity will be borne by those primarily responsible and capable of addressing the vulnerabilities, namely digital technology developers. This will encourage responsible digital technology development within the G20 where principles such as secure-by-design, privacy-by-design, and humane technology are adopted by technology developers. Failure to adopt human-centred approaches may mean the cybersecurity landscape continues to be shaped in ways that concentrate digital privileges and increase power asymmetries. This digital

power concentration is likely to contribute to the erosion of social cohesion, employment crises, and widespread cybercrime and may lead to increasing use of digital surveillance to oppress citizens and suppress digital rights and freedoms (WEF, 2023). Therefore, even if more investments are made in security digital infrastructure, less resourcing would be directed towards addressing socio-technical threats, digital safety initiatives, and capacity-building efforts.

This policy brief recommends that G20 countries adopt human-centred approaches to reduce the likelihood of these threats, to ensure digital peace and security, and to support sustainable development and human thriving in a digital future. By adopting the recommendations in this brief, the G20 countries will fundamentally reaffirm their commitment to human rights, recognizing their role as primarily duty bearers with obligations to respect, protect, promote, and fulfil this both in the offline world as well as within the extended spheres of social and economic life that now comprise cyberspace.

References

Christine, D., & Thinyane, M. (2020). Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies. United Nations University. https://collections.unu.edu/view/UNU:7760

Detros, K. (2023). Towards a Resilient Cyberspace in Southeast Asia. Tech for Good Institute. https://techforgoodinstitute.org/research/tfgi-reports/towards-a-resilient-cyberspace-in-southeast-asia/

International Telecommunications Unit (2021). Guide to Developing a National Cybersecurity Strategy Strategic Engagement in Cybersecurity 2nd Edition https://ncsguide.org/

Miller, K., Shires, J., & Tropina, T. (2021). Gender Approaches to Cybersecurity. United Nations Institute for Disarmament Research. https://unidir.org/publication/gender-approaches-to-cybersecurity/

Stuart, J. (2024). Cybersecurity Threats, Vulnerabilities and Resilience among Women Human Rights Defenders and Civil Society in Southeast Asia. Un Women Regional Office of Asia and the Pacific and United Nations University.

Stuart, J. & Scott, R. (2021). The Measure of Online Disinhibition (MOD): Assessing perceptions of reductions in restraint in the online environment. *Computers and Human Behavior.* https://doi.org/10.1016/j.chb.2020.106534

Thinyane, M., Christine, D., & Detros, K. (2022, October 21). Here's how to address the workforce gaps in cybersecurity. World Economic Forum. https://www.weforum.org/agenda/2022/10/cybersecurity-workforce-gaps-inclusive-approach-jobs/

Un, C., Thinyane, M., & Christine, D. (2021). Civil Society Organizations' Cyber Resilience—Leaving no civil society organization behind in cyber resilience. United Nations University. https://collections.unu.edu/view/UNU:8262

WEF. (2023). Global Risks Report 2023. World Economic Forum. https://www.weforum.org/publications/global-risks-report-2023/

G20 BRASIL 2024
BUILDING A JUST WORLD AND A SUSTAINABLE PLANET

T20 Brasil 2024
Let's rethink the world

Let's rethink the world

CEBRI Rethink Tank

FUNDAÇÃO ALEXANDRE DE GUSMÃO

ipea
Instituto de Pesquisa Econômica Aplicada