FISIP DEPARTMENT OF INTERNATIONAL RELATIONS

ISSN 2722-838X

IR-UI COMMENTARIES

IR-UI Commentaries is a platform for academics of the Department of International Relations, Universitas Indonesia (IR-UI) to share their thought on issues related to the study of international relations. The ideas are presented from the perspective of International Security, International Political-Economy, Transnational Society, or the multidimensional approaches across the three clusters. It is jointly published by the IR-UI and Centre for International Relations Studies (CIReS) - Faculty of Social and Political Sciences Universitas Indonesia. Analysis presented here represent the views of the author(s) and not the institutions they are affiliated with, the IR-UI and CIReS-UI.

vol. I / no. 09 | October 2020

Implementing Human Security Measures in the Cyberspace: Navigating through the Institutional and Regulatory Disarray

Authors: Darang S. Candra[1], Broto Wardoyo[2]

Summary[3]

Cyberspace is the newest realm of human interactions that bring human security issues within its existence. Traditional security approaches would not suffice in tackling the threats and problems in the cyberspace as even the definition, regulation, and institution on cybersecurity are unclear and full of quarrels. A move toward agreeable conceptual understanding, especially towards comprehensive and non-traditional point of view, among stakeholders and cross-sectoral cooperation between both state and non-state actors are needed to ensure human security measures are included in the discourse regarding the cyberspace.

Keywords: *Cyberspace, Artificial Intelligence, Individual Security, Cybersecurity*

[1] *Lecturer, Department of International Relations, Universitas Indonesia*

[2] *Senior Lecturer, Department of International Relations, Universitas Indonesia*

[3] *This edition is the output of 'DefiningNurani a Dialogue Series on Human Security' held by the IR-UI as part of its 35th Anniversary celebrations, and supported by its Alumnae Association (ILUNI HI-UI), series 08, titled: "Human Insecurity dalam Keamanan Siber", with Egalita Irfan (Speaker), Broto Wardoyo, Ph.D. (Discussant), and Darang S. Candra (Host).* http://tiny.cc/irui_dn08

Cyberspace as the New Frontier of Human Security

Technological advancement has led the 21st Century society's daily life to be embedded to the internet, creating a brand-new world known as cyberspace. The cyberspace is a realm teeming with a massive population. Facebook, one of the most important entities in today's cyberspace, even boasted 2.7 billion users in 2020 or more or less equal to the population of China and India combined. Nonetheless, while the cyberspace provided a gargantuan opportunity to the development of the humankind by removing the temporal and geographical barriers for communication and networking as well as providing mass proliferation of knowledge, it is not a utopia free of problems, conflicts, and horrors. As with any places where humanity resides, anarchy is the name of the game and the environment in cyberspace is especially daunting. As the realm exists in complex and often-confusing governance, simply replicating the traditional state-based institutions and regulations to protect the interests and security of people that use the cyberspace would bring further complications. Nonetheless, the world has no other option but to employ a state-centric approach in understanding cyberspace as state is the only organization which capable of creating binding-regulations and enforcing protection, including in the cyberspace. Furthermore, almost all facets of human security, be it political, social, environmental, economic, military, and cultural aspects, are extant in the cyberspace and can face threats from multitudes of directions. Analysing human security in the cyberspace also entails the need to include cybersecurity point of views along with its perks and quirkiness. With all of this information in mind, how do today's state and non-state actors fare in the inclusion of human security measures and concerns in cyberspace? The question becomes more important as state and non-state actors already have different ideas and interests regarding human security sans the cyberspace. Is there anything that we can do to ensure the cyberspace would not turn into a lawless frontier akin to the Wild West of olden times where human insecurity was the norm?

Confounding Institutional and Regulatory Landscape: The Limits of State-Centric Approach for Human Security in the Cyberspace

Before we delve too deep into the details, first we need to understand that human security and cybersecurity are both far-flung from the focus of traditional security studies. Both human security and cybersecurity place high regard to individuals as their main referent object. It is worth noting that Cyberwarfare, not cybersecurity, is the topic that authors in the traditional security studies tend to put more focus on. As both of these people-centred security concepts, particularly cybersecurity, are a relatively new addition to the field of security studies, finding a suitable definition that can be agreed upon might sometime feel like a Sisyphean task. Even the renowned Contemporary Security Policy, one of the major publications within the security studies, in its special 2020 issue on cybersecurity can only go so far to cover the debates and was unable to present concise agreements between security studies scholars regarding the concept.

The most prominent issue when it comes to analysing human security in cyberspace is the lack of clarity for its locus. As security is traditionally held within a state's domain, applying it to cyberspace, where geographical, legal, and institutional boundaries are blurred, can confuse who is responsible to react when a cyber-attack or other threats to human security manifested. A clear example can be seen in how Facebook created its community standard as the guideline to ensure the social media can act as a safe platform to express their thoughts and opinions while preventing abuses, hate speeches, bullying, harassment, and terrorism from freely proliferated in the platform. The issue that arose is that Facebook is the sole definer and regulator of the community standard which can be conflicting with how states view those standards as seen in how Facebook failed to prevent manipulative political ads, racist messages, and other false information that directly affected the American electoral process. In the past few years, several Facebook posts also contributed to or were used in real-life security issues, including riots and killings in India, mass shooting in New Zealand, and genocide in Myanmar, to name a few. Social media is a double-edged sword, however, as it also helped in propagate social reforms and revolutions such as in the case of Arab Spring, the Umbrella Movement in Hong Kong, and the Euromaidan pro-democracy revolution in Ukraine. It should be noted, however, that while Facebook might be able to set up norms or governance within their domain, consequences from violation to this established governance are not their hand but are at the hand of the state where the defendant to Facebook's governance reside.

In terms of the governance of the cyberspace, we can also look on how the state-based approach and its limitations. State-based approach is generally treading on a thin line when it comes to threats to human security in the cyberspace. While harassment or terrorism cases can be seen as intentionally created by individual or organized actors, there are also issues with the underlying technological cornerstone of the internet. How should a state react if the threats to human security are caused by a social media's algorithm, artificial intelligence, or other non-human causes? Regulations managing cyberspace vary widely across countries and not all lawmakers and legal professionals understand the topic in depth. There is also the issue of overlapping jurisdictions within the state. While traditional security issues are usually defined as being the military and the ministry or department responsible for defence or war, cybersecurity and specifically human security in cyberspace is prone to miscommunication and overlaps among different institutions including the intelligence agency, institutions responsible for censure or propaganda, and telecommunication agencies. In the Indonesian context, for example, the country still has problems in determining which institution should be responsible for providing cybersecurity guarantee, let alone human security, in the cyberspace. This institutional problem, which also exists in various parts within the state, is also made worse by the lack of human resources in the field, weak infrastructure to protect their citizens in the cyberspace, and the absurdity, for lack of better terms, of the regulatory basis and understanding regarding the issue.

How, then, should we ensure that human security concerns are appropriately taken into consideration in the cyberspace? Likewise, with the limits of state-centric regulatory and institutional approach in providing safeguards for human security in the cyberspace, what can other actors, most notably corporations and civil society organizations, do to fill in the oversight?

Chiding the Current Approaches: How to bring Human Security Back to the Table?

To ensure the inclusion of human security concerns to the governance of cyberspace, one of the possible methods is through cross-sectoral cooperation. Back to the Facebook example, their stakeholder engagement team stated that they have to consult international and country-level documents, discuss the terms with state-based institutions and gather inputs from the academics, NGOs, and expert sources. Compliance with national laws is another grey area for cross-sectoral cooperation. In general, states will always try to ensure their regime security and they can either negotiate or punish internet-based businesses that allow dissidents or anti-state activities in their operations. However, as the line between freedom of speech and criminal acts against the state might be blurred on multiple occasions, non-state and non-business actors should also participate in the foray to fight for the human security-first approach.

As human security calls for the protection of individuals, not merely state or businesses, all stakeholders must find a way for some kind of auditory system, whether AI-based or human-based or a combination of both, that can determine threats to individuals in the cyberspace and act quickly to remove the threat. The road to a clear definition of who to protect, who should be responsible, and how the safeguards are implemented will be long and winding. However, it is not impossible. Facebook's transparency measures, which detailed among others-governments' requests for user data, is an example of cross-sectoral cooperation to protect users from hate speech, criminal acts, terrorism, and other threats to human security while also having the ability to be scrutinized by the wider membership of the society.

Another issue that also arises when talking about ensuring human security in the cyberspace is how to prevent over-surveillance. Surveillance is still needed as it is one of the few ways to snuff threats. However, surveillance by the state and/or corporations to detect threats can rather become a threat to netizens' privacy and personal freedom. There are pros and cons from both sides of the aisle on how to navigate this particular problem. On the other hand, the Cybersecurity and Cyber Resilience Law in Indonesia are stuck in its draft form due to resistance from groups who are rightly worried that the government will use the law to instead dig too deep into citizens' privacy and personal lives.

Conclusion: The Need for Concise Understanding and Collective Cooperation

Alas, amidst the constant debates and disagreements among security studies scholars, government officials, corporate lawyers, and civil activists, threats to human security ("human insecurity") in cyberspace are real and already affecting the physical world as seen in cyberspace-based revolutions, riots, and terrorist acts. The contested nature on multiple perspectives of the issue needs to be discussed and all parties have to compromise to reach an agreeable understanding of the matter. It should be noted that the definition would not need to be an unchanged slab as it could evolve and be adjusted over time following the betterment of our understanding of the threats in cyberspace. Lastly, as cybersecurity issues always move at an extreme speed compared to how the traditional security establishments could respond, a collective work between all stakeholders is needed to catch up with the ever-changing threats. As the field of cybersecurity is relatively underexplored, the addition of human security dimensions would be helpful in broadening the focus away from mere technological jargons and ensuring the stakeholders to also take part in the much-needed discussion and cooperation to prevent human insecurity in the cyberspace.***

35 Tahun Hubungan Internasional Universitas Indonesia

Department of International Relations
Faculty of Social and Political Sciences Universitas Indonesia
☎ (+62 21)-7873-744 ✉ internationalrelations@ui.ac.id
www.ir.fisip.ui.ac.id @internationalrelationsui @ir_fisipui

9 772722 838001