Barun ICT Global News

October 2021

YONSEI UNIVERSITY Barun ICT Research Center

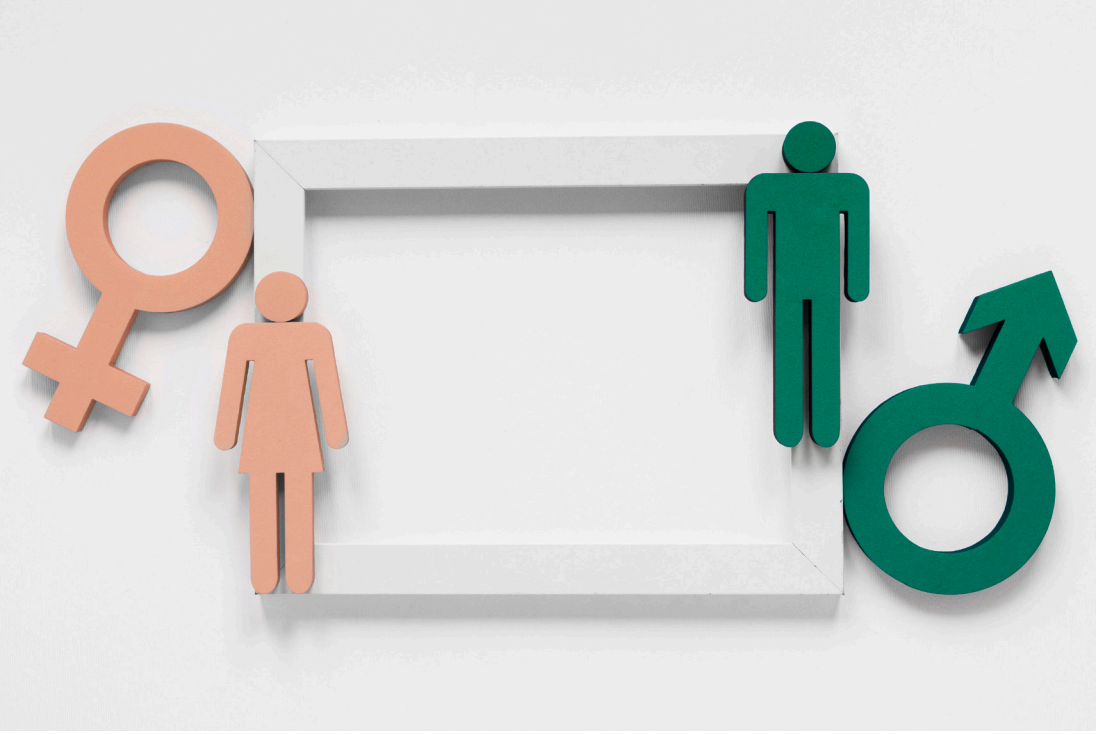
01

Closing the Gender Data Gap

Emily Qiyan Wu
Department of Economics, UIC, Yonsei University

The data gap, when data on a particular group is missing, has become a noteworthy issue in the context of reporting on minority groups [1]. The gender data gap, in particular, is a phenomenon to describe the biased collection process with data only pertaining to one gender. An example is how voice-recognition technology is often found to be less accurate for women than men simply because the algorithms used are trained based on male datasets [2]. There are subsequent implications for women having higher chances of being injured in car crashes as the algorithms are tested and designed based on male data. Thus, it becomes crucial to resolving the gender inequality in the world of big data.

There are several ways to go about addressing the gap. The WHO has decided to disaggregate global health statistics by sex in 2019 so that researchers can conduct intersectional gender analysis and apply appropriate resources to facilitate the health system with equal policies on both genders [3]. In fact, the



effort to fill such a gender gap is one of the core agendas in the 'data revolution', which refers to a set of actions or improvements in how the data should be used or collected and thereby closing the gap to minimize discrimination. Although it is typical that datasets or samples tend to cover more responses from males than females unless specifically reach out to the other gender group, data producers should always be aware of such a gap in the raw data in the first place and apply additional measures or analysis to counteract it.

The gender data gap is limited to not only the discrepancy between male and female but also other minorities including LGBTQ communities. A report from the National Academies of Sciences, Engineering, and Medicine has indicated that the lack of data on those non-traditional gender norms is one of the main reasons that the programmed services or products have failed to address their specific needs [4]. The report also urges the federal statistical agencies to adopt new measurement tools so that all kinds of gender or sexual diversity can be included in even smaller datasets. Overall, the task of filling the gender data gap should be prioritized by not only researchers but also product developers in general since they should also be aware of the issue when developing a new product or service.

Sources

[1] Giest, S., Samuels, A. (2020). 'For good measure': data gaps in a big data world. Policy Sciences, 53(4), 559–569.

[2] Perez, C. (2020). We need to close the gender data gap by including women in our algorithms. Time. https://time.com/collection/davos-2020/5764698/gender-data-gap/

[3] Closing data gaps in gender. World Health Organization. https://www.who.int/activities/closing-data-gaps-in-gender

[4] Lowry, M. (2020, Oct. 21). New Report Calls for More Comprehensive Data on LGBTQI+ Well-Being. The National Academies of Sciences Engineering Medicine. https://www.nationalacademies.org/news/2020/10/new-report-calls-for-more-comprehensive-data-on-lgbtqi-well-being

02

Who is the Winner of the 5G Competition, the U.S. or China?

Sangeun Lee

Department of Sustainable Development and Cooperation (SDC), Yonsei University

Competition in the field of 5G has become an important indicator of IT-related technology supremacy and the future trend of technology competition. The U.S. has tried to impede Huawei, the leading company of the 5G market, while also striving to improve its competitiveness by developing Open Radio Access Networks (ORANs), preparing for 6G, and working with its similarly minded global partners [2]. In the first half of 2020, a growing number of countries explicitly banned Huawei's 5G network equipment, indicating the U.S. focus on multilateralist-based international cooperation.

There are also opinions that the U.S. export restriction policy lacks consistency. The Trump administration had stopped issuing large-scale export licenses to China in 2019 but later issued temporary export licenses to companies exporting to Huawei. This shows the ambivalence in easing export restrictions to benefit some U.S. companies. Meanwhile, the Biden administration has been seeking cooperation by issuing

executive orders banning Americans from investing in Chinese companies, while continuing regulations on Huawei, including a 100-day supply chain review and restriction on parts supply [4].

In response, China has aimed to create its own 5G ecosystem while expanding its 5G technology. This process, however, is likely to deepen the conflict between the U.S. and China, as it inevitably embodies "national capitalism", in which government-business cooperation takes place. China is also setting a goal to cover 70% of Chinese semiconductors with domestic production in the near future, reducing its dependence on foreign countries in key technologies and high-tech industries to increase domestic self-sufficiency. In addition, China is attempting to build its 5G-based network ecosystem [3].

Some scholars fear China's increasing share in the domestic market to respond to U.S. sanctions and Chinese consumers' high loyalty to Chinese smartphones will cause U.S.-China decoupling, leading both countries to face reduced industrial size and increased production costs. In addition, the author expects the U.S. and China to pursue "strategic re-connection" in the future - expanding technology and production capabilities domestically and strengthening international cooperation to limit the influence of other countries [1]. The two countries are likely to reduce interdependence in areas that are sensitive to security and technology competition, such as technology and high-tech industries while reshuffling their economies around areas that are not.

This incident demonstrates the ambiguity of the technology. Considering the distinction between 'hard-power' and 'soft-power' proposed by Dr. Joseph Nye, cutting-edge technology can fall under the category of hard power as well as soft be both. As the nation's technology develops and becomes more sophisticated, the connection between technology and military and economic power is strengthened and the technological expansion of other countries is prevented. If the U.S. and China keep seeking a strategic re-connection"in the future, they should have constructive competition in terms of hard-power, while engaging in soft power style corporation.

Sources

[1] Allen, J., & Stewart, J. (2021). The Strategic Challenges of Decoupling. Harvard Business Review. https://hbr.org/2021/05/the-strategic-challenges-of-decoupling

[2] Brake, D. (2020). A U.S. National Strategy for 5G and Future Wireless Innovation. Information Technology & Innovation Foundation. https://itif.org/publications/2020/04/27/us-national-strategy-5g-and-future-wireless-innovation

[3] Cheng, T., & Lauly, L. (2021). U.S-China Tech War: Beijing's secret chipmaking champions. Financial Times. https://www.ft.com/content/795060b7-1932-4491-af6f-d983e3cffb50

[4] Karen, F. (2021). Biden administration adds new limits on Huawei's suppliers. Reuters. https://www.reuters.com/article/us-usa-huawei-tech-idUSKBN2B3336

03

What a Hack!

Simran Karki
Department of Business Administration, Yonsei University

Those of us who have watched or heard of the popular Netflix Series Black Mirror are aware of its theme - the deadly consequences of technology in a dystopian world. While each episode covers a unique tech-related issue, season 3 episode 3 is particularly interesting because of its striking relevance to current cybersecurity concerns. The episode, “Shut Up and Dance” presents a group of hackers who gain illegal access to cameras on people’s devices, which they then use to record and expose private and sensitive details. Hacking and cybersecurity crimes have become more common with the heightened exposure to technology. This article aims to shine a light on a particular cybercrime - ransomware.

With over 4.2 million mobile users falling victim to attacks solely in America in 2020, Ransomware

poses a huge threat to cybersecurity [1]. In layman's terms, ransomware is malevolent software that accesses and encrypts important data from a device. Usually, such hacks are time-sensitive and are resolved after the payment of a ransom to the hackers. According to the Cybersecurity and Infrastructure Security Agency, common methods of a ransomware attack are email phishing and susceptibility of RDP (Remote Desktop Protocol) or software. While big organizations and businesses remain the focus of ransomware attacks, it is a threat for all due to consequences such as economic loss, risk of damage to data, and reputational harm.

The Ashley Madison Data Breach is among the most memorable cases of a destructive ransomware attack. Just like in the Black Mirror episode, hackers calling themselves The Impact Team took control of Ashley Madison, an online platform that facilitated extramarital affairs. They threatened to release user data in return for the website to shut down. The incident was controversial because many praised the hackers due to the unethical of activities the website. Nevertheless, such a data breach showcases the tremendous power lying in the hands of a hacker. It is also a reminder that ransomware attacks can motives beyond money.

Amidst the uncertainty, you may be wondering how to stay safe from such cybercrimes. While there is no easy solution, individuals can adopt various steps for self-protection. For example, one can appear less perceptible to hackers while on public networks by using a VPN that encrypts data. Similarly, good cybersecurity habits such as backing up important data, multi-factor authentication, and frequently updating passwords can be useful. In addition, individuals must browse safely and avoid clicking on unknown links or responding to emails from strangers. Last, people must take initiative to educate themselves about cybersecurity crimes since they are ever evolving.

Cybercrimes such as ransomware are a growing concern. The digital transformation brought forward by COVID-19 has enabled hackers to find new and creative ways to scam people online. While the intention behind hacking may differ, the threat is indisputable. Cybercrimes can cause huge monetary, privacy, and reputational harm to both individuals and organizations. Therefore, one must remain aware of them and always remain cautious if they do not want to be in situations screaming 'What a hack!'

Sources

[1] Sobers, R. (2021, June 7). 81 Ransomware Statistics, Data, Trends and Facts for 2021. Varonis. https://www.varonis.com/blog/ransomware-statistics-2021/

[2] Ip, C. (2018, March 29). Ashley Madison attempts to regain the public's trust. Engadget. https://www.engadget.com/2018-03-29-ashley-madison-president-comeback-interview.html

[3] Techaeris. (2019, May 27). What does Black Mirror teach us about privacy and security? https://techaeris.com/2019/05/27/what-does-black-mirror-teach-us-about-privacy-and-security/

Barun ICT Global News

Publisher Beomsoo Kim
Editor-in-Chief Miyea Kim
Editor Seungyeon Won, Alexandra Stephenson
Translator Sumin Lee, Kyong Ju Yu, Yejin Juliet Yi
Designer Subin Lee

October 2021

** Please note that any external contributions to the Global News do not represent Barun ICT's official views.*

YONSEI UNIVERSITY

Barun ICT Research Center

Barun ICT Research Center, Yonsei University
50 Yonsei-ro, Seodaemun-gu, Seoul 03722, Korea
+82-2-2123-6694 | www.barunict.org

https://www.instagram.com/barunict/
https://www.facebook.com/barunict/