GP - ORF Series

Digital Debates

CyFy Journal 2019

Edited by

Samir Saran
Arun Mohan Sukumar

CyFy 2019
technology. security. society.

Durham University

WILEY-BLACKWELL

Digital Debates

CyFy Journal Volume 06 (2019)

Authors:

Nikhil Pahwa, Paula Kift, Tanuj Bhojwani, Dennis Broeders, Anushka Kaushik, Arindrajit Basu, Lydia Kostopoulos, Terri Chapman, Mihir S. Sharma, Winston Ma, Aditi Kumar, Astha Kapoor, Sarayu Natarajan, Sean Kanuck, James Lewis, Philip Reiner

Editorial Team :

Trisha Ray, Akhil Deo, Meher Varma

Inside Design:

Artlab, Chennai

Printed by:

Times Press, New Delhi

Contents

Editors' Note

CyFy Journal 2019

Our 'Insecure' Tech Futures

Samir Saran and Arun Mohan Sukumar

2019 will sputter to an end with unresolved anxieties about the future of emerging technologies, and their relationship with our societies. Sean Kanuck, our distinguished colleague and fellow chair of CyFy, identifies four trends that appear to be reinforcing these anxieties: "insecurity, disinformation, anti-globalization, and un-enlightenment." As is wont for these times, Sean contributes a new phrase to define the zeitgeist: "indisantiun". They represent drivers of change that, by themselves, have little to do with the digital domain. Like their Biblical counterparts, these horsemen of the digital apocalypse represent malaises residual in 20th century global governance: economic and social exclusion, lack of transparency in the business of government, pervasive xenophobia, and a profoundly anti-elite, anti-intellectual tendency that is on the rise. These problems may have been seeded in the previous century, but attempts to resolve them using 20th century institutions, regimes and coalitions have come a cropper.

Kanuck's contribution to the Digital Debates is one amongst fifteen essays for this edition of Digital Debates that are divided equally between five animating themes: Individual, Livelihood, Society, Governance and Conflict. We chose these themes to allow authors to explore comprehensively, the implications of digital technologies from their own unique vantage points as scholars and practitioners. Many of our contributors shared Sean's assessment of a more insecure and anxious world. In fact, "Indisantiun" may well capture the inability of current global governance arrangements to respond to broader, technology-fuelled disruptions and their disquieting consequences.

We attempt here to tie these themes together, and to present (what we hope is) a coherent picture of the virtual world in 2019. As the most granular, and perhaps most consequential, unit of this world, it is fitting that the first set of essays address the anxieties haunting the individual. The platform-ization of the public sphere may have democratized expression — or atleast deepened it through encrypted communications — its by-product has been the creation of new infrastructure designed to extract data and expand surveillance. This has created a paradoxical situation for individuals: the more they interact with digital spaces, ostensibly to exercise their freedoms, the more vulnerable they are to rights abuses—by private actors, their own sovereign, or even a foreign one. This has created a new type of insecurity, one where individuals are "simultaneously under attack and being weaponized" – as Nikhil Pahwa argues — by the influence of digital technologies on their social lives. Tanuj Bhojwani offers a provocative rebuttal to Pahwa, suggesting the notion of unfettered individual agency over digital networks is nothing but a "techno-utopia". However, he agrees that the framing of platforms as "mere marketplaces" is problematic.

Concurrently, digital technologies have also altered the relationship between labour, capital and productivity. For much of the past century, a nation's Gross Domestic Product — the sum total of goods and services produced — was considered an accurate picture of its economic, indeed political, health. This will not be a reliable metric for the digital economy, which will likely be characterized by incremental or marginal innovation, diffused supply chains and the "gig" economy that runs on shared resources — all, in turn, fuelled by the aggregation of data. There is great uncertainty about how to quantify the relationship between these independent variables, how they will affect development outcomes and what this implies for livelihoods in advanced and emerging markets. The essays under the theme of 'Livelihood' capture perfectly the nuances of this debate. While Winston Ma's piece speaks to the potential of digital technologies in bridging 20th century development divides, Aditi Kumar responds by clinically dissecting the inequities inherent in digital workforces of the 21st century. Astha Kapoor and Sarayu Natarajan argue India in particular is becoming a "hot bed for micro-tasks" in the digital economy — especially in areas like data labelling — which could 'invisibilize' labour and further exclude those at the margin. They too emphasise a shift away from "static notions" of productivity and a more rounded view of "well-being".

Whatever be the causal pathways, personal, political and economic insecurity has created a backlash against established forms of governance in domestic regimes. The dynamic between the individual, private platforms and the state is constantly in flux, prompting institutions of government to play catch-up. The social contract between the citizen and state is being usurped by private, digital platforms, who through their privacy policies confer on the individual rights that governments are reluctant to endorse. Conversely, they have begun to exercise "eminent domain" over the property of the individual in the digital age: data. In short, there is wide overlap between the functions of a platform and the state—of regulating speech, providing social protections, creating employment opportunities and ensuring national security. Rules and norms to govern these interactions are yet to fully mature, leading to uncertainty in the social contract and, as James Lewis points out, a crisis in the legitimacy of domestic norms and institutions.

The flux in domestic regimes is reflective of the churn in the international order. Connectivity between nations and mutual gains from trade, according to conventional wisdom, was expected to heighten the stakes for war or even limited conflict. Digital connectivity, however, has created a new set of tensions. Digital spaces are effectively a "system of systems", from cell towers and routers, to platforms and applications. Taken together, they reflect the digital interactions of entire nations, sans the neat segregation of boundaries which has been the edifice of 20th century politics. This infrastructure is not neutral; instead, as Arindrajit Basu argues, it is political. Cyberspace is not merely a reflection of geopolitics in the "offline" world but has rendered it even more chaotic by adding vectors of political contest: 5G, influence operations, the Dark Net...the list is long. Isolation is no longer a feasible strategy. Dennis Broeders refers to our times as an era of "unpeace"— a time of both messy interdependence, and of friction and conflict. To be sure, history offers precedents — think of continental Europe before the first World War — but the arena is different this time and poses a new set of challenges. Anushka Kaushik's lucid exposition of the attribution dilemma in cyberspace exemplifies the problem: without actors to blame, who is responsible for the malaises of the digital age?

Our authors seem secularly skeptical of prospects to navigate these problems. Nevertheless, we remain optimists. The faultlines emerging today across communities and states are not a factor of digital technologies, but of problems that predate their global popularity. As Philip Reiner notes, "insecurity always has, and always will persist, in varying degrees of flux." Disruptions exacerbated by digital technologies are an opportunity to re-conceive and adopt templates for domestic and international governance that are responsive and agile — but also rooted in ideas that were paid lip service in the last century: equity and sustainable development.

'Digital Debates' is an attempt to do just this—to highlight perspectives, diagnoses and solutions for the future of our digital world that are not necessarily rooted in technology. We are grateful to our authors for having fulfilled their mandates splendidly. By design or sheer circumstance, contributors to Digital Debates this year have not only dwelled on the many tensions agitating cyberspace, they have also argued that the political, social or economic realignments triggered by this medium may ultimately settle into a new normal.

Perhaps the most important of these realignments is the coming to terms of democracies with the introduction of digital technologies in our public sphere. We have, in a manner of speaking, entered a post-internet world. Previous evolutions in media and production technologies(such as the radio or the steam engine) dramatically altered the demands and methods of governance. It is not unexpected that a similar moment is upon us today. Despite present concerns around polarization and inequality, it was comforting for us to see that each of our pieces on the theme 'society' were unanimous in their belief that our democracies possessed the ability to self-correct. Mihir S. Sharma argues that the problems plaguing digital governance has to be treated on its own merit. Whether the management of digital spaces is democratic is, he writes, a separate question from whether they promote democracy. Terri Chapman responds to that poser, calling for greater "explainability" in algorithmic decision-making.

A course correction is indeed being embraced by or forced upon technology platforms. Whether it is protests against military contracts with governments, allegations of bias and partisanship, or disquiet at their sheer monopolistic power, the governance and ethics of technology platforms are being questioned more severely than ever before. Paula Kift recognizes that this new backlash stems from an "internal rift" (irreconcilable, perhaps?) between ideals and business practices. Consequently, we see boardrooms responding to popular concerns. New ethics and oversight practices, institutional cooperation with the state, and new user controls are all evolving to create — or at least, attempt to — accountable and transparent regimes for the technology industry.

Processes and conduits of globalization are also under pressure to respond more effectively to local communities or interests. In the 20th century, economic connectivity was a process moulded by a small set of state and private actors. Digital spaces have undermined this monopoly, allowing individuals and communities to agitate for representative global economic decision making. Civil society coalitions that challenged the provisions of the Trans-Pacific Partnership, and its negotiation in secrecy, were lent a fillip by the internet, lending them instant access to allies and like-minded partners in distant lands. Most crucially, we see such digital disruption playing out in the development sector—where innovations from Asia and Africa are creating platform-based solutions for the next six billion. Their technological pathways to development and policy frameworks will be digital-first by design, and

perhaps capable of providing the templates the world so desperately needs.

And finally, our contributors also recognized the character of our international community has changed in the digital world. Lydia Kostopoulous reminds us of the complexity of this new moment: where digital spaces are pervasive, but also interact with and operate within sovereign boundaries, each with their own political contexts. Resolving this contradiction will require efforts that are capable of bridging the disconnect between 19th century Westphalian understandings and the realities of a 21st century digital world. It is our hope that CyFy will be a platform to discover such solutions. We express our sincere thanks to contributors to this volume for setting the stage for the two days of debates and discussions that follow.

01.
Individual

Individuals' Rights at Risk in the Digital Age

Nikhil Pahwa
Founder, Medianama

The true benefit of the digital space lies in the fact that it enables billions of creators. It awards individuals agency, along with the opportunity and the space to express themselves with more freedom than ever before. It enables them to find work and to learn through the free flow of information and societal interactions global scale, without prescriptive local restrictions. However, such freedoms have also brought forward multiple challenges for individual rights.

The trends defining the state of the individual and her rights over the past few years are as follows:

First, and most importantly, we've lost control over our data.

Individuals have effectively lost control over their own data, and how they consume content and services. Data is being collected en masse, and used by marketers to profile users, which is used to drive engagement, clicks and time-spent on applications. Individuals have little knowledge or understanding of how they're being profiled and targeted, and have few options to prevent or restrict this targeting, since this data is being collected from multiple sources, across applications and services. Consent frameworks have largely failed to restrict data collection and profiling, owing to verbose agreements and consent fatigue. Application stores with broad permissions tend to act more as enablers of data collection, rather than provide users agency. Apps and advertising networks have malware which compromise user privacy.

Secondly, the centralization of the Internet into significantly large businesses with over a billion users each has led to a reduction in the individual's reduced to negotiate its terms of engagement.

Platforms are in the business of increasing fragmentation and monetizing aggregation. The Internet allows for aggregation of factors of production on a global scale, thus providing a global customer/user base with a never-before diversity of content and services. For creators and service providers, there is the opportunity to be an entrepreneur, and/or get disproportionately high revenue, or build a loyal fan/customer base. Some platforms - taxi aggregators, for example - end up providing debt and high revenue to incentivize participation on the platform, while also increasing their dependence on the platform itself. However, as more and more participants are added to platforms, the exertion of control by the platform, over discovery through personalization, reduces the negotiating ability of each individual producer. Tweaks to algorithms or revenue shares can destroy all that they have built.

Unionization and cartelization among individual producers are possible responses to this outcome. For example, this could involve key content creators going off YouTube, or drivers protesting or boycotting Uber. However, while the Internet offers creators with alternatives, the winner-takes-all nature of competition in the platform business, the utility of the network effects, the dependence of users on discovery, and the financial heft of platforms means that signing out is often not an option for individual creators/service providers. While entrepreneurship and agency for individuals was once enabled by platforms, now they're often stuck without a choice.

Thirdly, free speech is highly dependent on a few platforms, and is being restricted by hecklers getting the veto.

The centralization of Internet usage around a few platforms has made them critical as carriers of free speech. For users, these large platforms – with their network of friends, family and colleagues — are primary avenues for expression: the dependence on such platforms to maintain and allow their speech is high. However, restrictions to speech are now being attempted via these platforms. Governments do this, for example, through amendments to safe harbor protections; in India, in the name of automating censorship, pro-active monitoring and automated takedowns of content is being considered. Secondly, the same platforms are being used by organized trolls, who are often paid to overwhelm users and platforms with hateful content – this has a chilling effect on speech. While organic critiques and pushback against comments made on the Internet have been around for decades, these organized pushbacks have now become the norm.

Fourth, data is being viewed as a factor of production and a national asset, as opposed to an individual right. Governments are profiling citizens.

'Data is the new oil', is a popular catchphrase in business and government circles. Both individual and analysed data are being viewed as critical to the development of a region/nation. The claim is that data belonging to a community of individuals belongs to the nation state, or needs to be controlled by the state directly, or via national corporations. Digital National IDs are in vogue, and in India, silos between various datasets are being made obsolete, as they are now connected by a single unique identifier, which is being used to profile citizens. Currently, large government datasets are being created: for example, a public credit registry will hold transaction and credit information for individual citizens. Pitted against statutory power, individual citizens have little choice but to part with their data. Consent frameworks enable the sharing of this data with private enterprises, and are faced with a potential denial of service sans the data-sharing; it is clear that individuals have little choice. Data collection is being positioned as critical for growth of an artificial intelligence ecosystem, without critical analysis of whether collecting more data actually helps the system. In all of this, the individual is particularly helpless and often without choice.

Fifth, usage of biometrics and facial recognition systems for authentication is becoming shockingly popular.

Biometric systems are being seen as a solution to fraud. Cameras and data storage have become cheaper, and biometric authentication software — especially on mobile devices — have become common. In addition, facial recognition in public places, such as in airports, on the streets, and via CCTV cameras, is becoming more pervasive. These developments pose new risks for individuals: firstly, biometrics are

permanent and seen as irrefutable, despite the fact that they can be cloned and misused. The usage of polymer resin to clone fingerprints is possible, as is cloning via high resolution photographs. Secondly, biometrics are often seen as a single factor of authentication, and a corresponding second factor is often missing. Thus, given the inaccuracy of authentication, especially when it is a one-to-many comparison with a database, the chances of false positives and false negatives is high. When facial recognition systems meet citizen profiling and social credit systems, individual liberty is at particular risk.

Sixth, individuals are being attacked and weaponized.

Our behavior is constantly being gamified: marketers and product developers are using the dopamine effect to drive addiction to applications, services and purchases using targeted communication and pattern recognition on a planetary scale. And, that's not where it ends: content is being created to instill and entrench bias; this is amplified using algorithmic filter bubbles and granular personalization. With behavioral targeting of individuals, and an instillation of deep bias, indviduals are being manipulated and weaponized to target communities, democratic processes and countries. We have already seen how messages on social media have been used to manipulate elections, and create misinformation; online videos have driven mobs to kill people.

Seven, speech is being restricted via internet shutdowns, content regulation and online mobs.

With the pervasiveness of misinformation, and its impact on inciting mob violence, governments are choosing to shut down all access to the Internet: this is a disproportionate act of censorship, which punishes everyone for the actions of a few. In India, court cases have been filed for regulating content on the Internet, especially on video streaming platforms, on grounds of obscenity, being hurtful towards religious sentiments, violence etc. On social media, the Indian government is seeking proactive monitoring and the takedown of content. Several Indian ISPs already block porn sites. In addition, co-ordinated mobs attack particular accounts for their comments, especially on Twitter and Facebook, with doxxing, and death and rape threats being par for the course.

Eight, surveillance is the new normal.

The demand for government monitoring of all communications is high, and there's a significant threat to end-to-end encryption. The privatization of surveillance manifests in two major ways: firstly, with private companies providing technological support to governments for enabling their surveillance systems. Second, it manifests with private companies collecting data on users, which in turn may be accessed by governments. The profiling of citizens, and the breaking down of silos between disparate databases, using unique identifiers like mobile numbers and national IDs is becoming normalized.

While threats to individual rights continue to grow with rapid digitization and centralization, these issues are compounded by a lack of user awareness, the understanding of the implications of certain practices, and in some instances, the lack of user agency. Work needs to be done to create structures to reduce the usage of digital technologies to harm individual rights.

The Turning Tide of the Platform Revolution – Current Trends and Future Developments

Paula Kift
Civil Liberties Engineer, Palantir Technologies

From vehicles to vacations, retail to restaurants, networking to news – we live in the age of platforms. Uber and Lyft transformed the taxi business by enabling regular drivers to connect with potential passengers and offer their services online. AirBnB transformed the hotel business by enabling local residents to welcome strangers on vacation into their homes. Facebook and Twitter users have transformed the traditional media business by acting as both consumers as well as on-the-ground producers and real-time commentators of news. None of these companies provide their own physical infrastructure to provide these services, or even provide these services themselves.

Platforms are popular for good reason: by turning traditional pipeline exchanges between producers and consumers into multi-way dynamic exchanges, value can be generated and consumed by market participants on all sides.[1] Products can better be tailored to individual needs. Service providers, in turn, can participate in the market flexibly, without the need for special training, or having to subject themselves to working hours dictated from above.

Platforms often portray themselves as neutral intermediaries: they enable us to connect without forcing us into a hierarchy. They present themselves as technical rather than political.[2] They are private rather than public: we can choose to accept their terms or not.[3] At the same time, the platform revolution[4] also harbors significant risks: for our right to privacy and informational self-determination on one hand, and to our labor protections and social welfare on the other hand.

At an individual level, both sellers and consumers of goods on digital platforms are subject to extensive surveillance and control. Uber drivers and riders alike are subjected to ratings, which, if not at a near-perfect level, prevent them from offering and making use of services on the platform in the future.[5] The same applies to AirBnB. Social networks such as Facebook collect granular data about their users in order to tailor posts to individual preferences: a model which might work well at an economic level ("if you like this, then you also like") but becomes problematic at a social level ("if you believe this, then you'll also believe"). This further narrows the space for meaningful dialogue across the socioeconomic and political divides.

At a socioeconomic level, the devaluation of professional training – as is the case for taxis with ride-sharing services such as Uber or Lyft, or the hospitality industry through the rise of AirBnB – also leads to a devaluation of professions themselves, threatening livelihoods and sparking protests worldwide.[6] Amateur drivers, along with other workers in the on-demand economy, do not enjoy the same benefits as regular full-time employees. This is particularly true in the case of traditional service industries that have waged long and protracted battles for unionization in the past. AirBnB, while promoting tourism, also contributes to property speculations and rising rents, as local residents can no longer afford to live in their own neighborhoods. Finally, by subjecting traditional news outlets to the need of having to generate the most clicks in order to remain relevant, social media also force them into writing the most attention-grabbing headlines, further sensationalizing an often already polarized political reality.

But the tide of the platform revolution seems to be turning, as public and political pressure to reign in some of the most egregious consequences is mounting. Uber – the app itself or select subservices thereof – has been banned in several locations across Europe and abroad.[7] Ride-sharing services are also increasingly facing regulatory scrutiny in the United States as jurisdictions such as New York and California passed bills limiting the number of drivers, imposing minimum wages and demanding that contract workers, which include ride-hailing drivers, be classified as regular employees.[8] AirBnB is confronted with large-scale protests in popular tourist destinations like Barcelona, where the platform has contributed to transforming even traditionally residential neighborhoods into transitory spaces, best characterized by the sound of hand luggage suitcases clattering down cobblestone streets.[9] Other cities such as Amsterdam, Berlin and London are experimenting with different ways to balance a thriving sharing economy with protecting the integrity of urban spaces that an explosion of short-term rentals risks undermining. Facebook continues to struggle with the aftermath of Cambridge Analytica that triggered investigations and regulatory actions by the Information Commissioner's Office (ICO) in the UK,[10] the Standing Committee on Access to Information, Privacy and Ethics in Canada,[11] and the Italian Data Protection Authority,[12] among others.

Meanwhile Silicon Valley, an industry that has long prided itself as a source of good ("transportation as reliable as running water, everywhere for everyone," "making the world more open and connected"), is facing an internal reckoning based on the discrepancy between declared ideals and actual business practices.[13] Uber changed its leadership in response to mounting scandals, ranging from sexism and sexual harassment in the workplace,[14] to violating user privacy by enabling employees to track rides for the purpose of personal entertainment.[15] AirBnB released a so-called policy tool chest for improving cooperation with the cities in which it operates, including on issues such as tax collection and promoting more sustainable tourism.[16] Mark Zuckerberg has redefined the company mission to focus more on privacy-protective services and offerings, such as encryption, deletion and secure data storage.[17] An open question remains as to the extent to which these changes are compatible with the original business models, ranging from an open disregard for rules and regulations ("move fast and break things") to the detailed segmentation and monetization of users' personal data.[18] While some early pioneers of the platform model such as Apple actively advertise their emphasis on user privacy today,[19] not everyone, on neither the demand nor supply side, will be able to afford the premium price tag associated with offering luxury products, assuming tangible products are sold to begin with.

Increasingly, platforms are not only under political (and psychological) but also economic pressure. When Uber went public in May this year, its stock price dwindled.[20] WeWork, a platform that specializes in shared working spaces, withdrew from its initial public offering after it failed to convince bankers to buy its shares.[21] The appetite for investing in companies that aggressively push into markets, with little regard for toxic internal cultures and a potentially devastating social footprint, while at the same time accumulating reckless costs combined with an unclear path toward long-term profitability, seems to be waning. Does this mean the platform revolution failed?

Perhaps not. It depends on what we consider to be a successful revolution. If we think of the revolutionary waves that swept across Europe in 1848, some may consider these a failure as liberal and republican forces ultimately failed to topple the monarchies against which their uprisings were targeted. But while these political movements may not have succeeded in overthrowing the prevailing system of government in the short term, they did pave the way for fundamental structural sociopolitical changes in the long term.[22] Similarly the most important near-term impact of the platform revolution might not be to displace traditional industries, but to force them to fundamentally rethink their operating model in light of the real benefits of flexibility and efficiency that platform models do provide. Among others, BMW and Daimler – otherwise competitors in the market for luxury cars – have teamed up to shape the future of mobility, including a joint venture on car sharing and a network of charging points for more eco-friendly electric vehicles. [23] Marriott International, one of the most dominant players in the hospitality industry, now also includes home sharing in its portfolio in an attempt to offer well-endowed travelers a more boutique experience.[24] Most importantly, traditional market players are not only ahead at the level of infrastructure but also social welfare; the hope being that traditional industries will take the positive learnings of the platform model to heart, while avoiding its worst impacts on employment security and social welfare.[25]

We can again look to the revolutions of 1848 for inspiration: on a positive note, in order to take the wind out of the sails of the socialist forces gaining traction around him, Bismarck implemented a series of social reforms, including in the areas of health, accident and disability insurance as well as workplace safety that constituted the basis for the German welfare state today. On a more cautious note, widespread unemployment and rising inequality across Europe were incorporated into an increasingly nationalized narrative, contributing to the formation of nation states in the late nineteenth century, but perhaps also previewing the excesses of nationalism in the mid-twentieth century. As the preeminent historian Christopher Clark aptly put it, “in their swarming multitudinousness, in the unpredictable interaction of so many forces, the upheavals of the mid-19th century resembled the chaotic upheavals of our own day, in which clearly defined end-points are hard to come by.”[26]

On a final note, the platform revolution is far from over, as infrastructure itself is now being transformed into a service with the cloud. The extent to which in-house solutions from traditional telecommunications providers such as Deutsche Telekom will be able to compete with the likes of Amazon AWS, Microsoft Azure and Alibaba remains to be seen. One competitive advantage the former still have over the latter is in the area of security and privacy – an advantage not be underestimated, particularly in the long run. After all, if there is one lesson to be learned from the history of platforms (and revolutions), it is that trust is the one currency neither our companies, our economies, nor our societies can afford to lose.

Endnotes

1 Van Alstyne, Marshall W., Geoffrey G. Parker, and Sangeet Paul Choudary, "Pipelines, Platforms, and the New Rules of Strategy," Harvard Business Review, April 2016 https://hbr.org/2016/04/pipelines-platforms-and-the-new-rules-of-strategy.

2 For a critical take on this convenient self-portrayal, see Tarleton Gillespie, "The politics of 'platforms,'" new media & society 12(3): 347-364.

3 For an analysis of the extent to which it actually remains possible not to participate in such platforms, see Evgeny Morozov, "Every Little Byte Counts," New York Times, May 16, 2014, https://www.nytimes.com/2014/05/18/books/review/the-naked-future-and-social-physics.html.

4 Parker, Geoffrey G., Marshall W. Van Alstyne, and Sangeet Paul Choudary, Platform Revolution: How Networked Markets Are Transforming the Economy – and How to Make Them Work for You, New York, NY: W.W. Norton Company, 2016.

5 Rosenblat, Alex and Luke Stark, "Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers," International Journal of Communication 10, 2016: 3766.

6 Smith, Noah, "Uber Strikes Could Be the Start of Something Bigger," Business Insider, May 7, 2019, https://www.bloomberg.com/opinion/articles/2019-05-07/uber-strikes-could-be-the-start-of-something-bigger.

7 Asenjo, Alba and Ruqayya Moynihan, "Driver protests, bans and fighting with the competition: how Uber and other ride-hailing apps are holding up around the world," Business Insider, May 10, 2019, https://www.businessinsider.com/how-uber-and-other-ride-hailing-apps-are-holding-up-around-the-world-2019-5?r=US&IR=T.

8 Conger, Kate and Noam Scheiber, "California Bill Makes App-Based Companies Treat Workers as Employees," New York Times, September 11, 2019, https://www.nytimes.com/2019/09/11/technology/california-gig-economy-bill.html?action=click&module=inline&pgtype=Homepage&section=Business.

9 Mead, Rebecca, "The AirBnB Invasion of Barcelona," New Yorker, April 29, 2019, https://www.newyorker.com/magazine/2019/04/29/the-airbnb-invasion-of-barcelona?reload=true.

10 Information Commissioner's Office, "Investigation into the use of data analytics in political campaigns: A report to Parliament," November 6, 2018, https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

11 Zimmer, Bob, "Democracy under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly: Report of the Standing Committee on Access to Information, Privacy and Ethics," House of Commons, December 2018, https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf.

12 Garante per la protezione dei dati personali, "Cambridge Analytica: il Garante privacy multa Facebook per 1 milione di euro," June 28, 2019, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9121352.

13 Marantz, Andrew, "Silicon Valley's Crisis of Conscience," New Yorker, August 19, 2019, https://www.newyorker.com/magazine/2019/08/26/silicon-valleys-crisis-of-conscience.

14 Isaac, Mike, "Uber Founder Travis Kalanick Resigns as C.E.O.," New York Times, June 21, 2017, https://www.nytimes.com/2017/06/21/technology/uber-ceo-travis-kalanick.html.

15 Hill, Kashmir, "'God View': Uber Allegedly Stalked Users For Party-Goers' Viewing Pleasure (Updated)," Forbes, October 3, 2014, https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/#156f896b3141.

16 AirBnB, “Home sharing policy approaches that are working around the world,” May 17, 2017, https://press.airbnb.com/home-sharing-policy-approaches-that-are-working-around-the-world/.

17 Zuckerberg, Mark, “A Privacy-Focused Vision for Social Networking,” Facebook, March 6, 2019,https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/.

18 Thompson, Nicholas, “Mark Zuckerberg on Facebook’s Future and What Scares Him Most,” Wired, June 3, 2019 , https://www.wired.com/story/mark-zuckerberg-facebook-interview-privacy-pivot/.

19 Apple, “Apple products are designed to protect your privacy,” last accessed on September 30, 2019, https://www.apple.com/lae/privacy/.

20 Isaac, Mike, “Uber’s Stock Disappoints, Capping a Rocky Path to Its I.P.O,” New York Times, May 10, 2019, https://www.nytimes.com/2019/05/10/technology/uber-stock-price-ipo.html.

21 Eavis, Peter and Michael J. de la Merced, “WeWork I.P.O. Is Withdrawn as Investors Grow Wary,” New York Times, September 30, 2019, https://www.nytimes.com/2019/09/30/business/wework-ipo.html.

22 Clark, Christopher, “Why should we think about the Revolutions of 1848 now?,” London Review of Books, March 7, 2019, https://www.lrb.co.uk/v41/n05/christopher-clark/why-should-we-think-about-the-revolutions-of-1848-now.

23 Ewing, Jack, “BMW and Daimler, Once Rivals, Join Forces to Fend Off Silicon Valley,” New York Times, March 28, 2018, https://www.nytimes.com/2018/03/28/business/daimler-bmw-car-sharing.html.

24 Glusac, Elaine, “A New Marriott Division Goes Head-to-Head With Airbnb,” New York Times, April 29, 2019, https://www.nytimes.com/2019/04/29/travel/marriott-airbnb-homeshare-luxury.html.

25 Irwin, Neil, “Maybe We’re Not All Going to Be Gig Economy Workers After All,” New York Times, September 15, 2019, https://www.nytimes.com/2019/09/15/upshot/gig-economy-limits-labor-market-uber-california.html.

26 Clark, Christopher, “Why should we think about the Revolutions of 1848 now?,” London Review of Books, March 7, 2019, https://www.lrb.co.uk/v41/n05/christopher-clark/why-should-we-think-about-the-revolutions-of-1848-now.

The Internet is Not on Fire

Tanuj Bhojwani
Fellow, iSPIRT Foundation

Critiques of the internet often point to the techno-utopian promises of its early days. The "free-flow" of information and glorious, unrestricted connectedness were supposed to change the world for the better. However, what they have done falls somewhat short of the ideal. It remains prudent to believe that new technology can generally make things better for individuals. Simultaneously, it is foolhardy to believe it would solve all our problems and lead to utopia. It is always likelier that this connectedness would do what any other technological transformation has always done: resolve some of the old trade-offs, but also introduce entirely new trade-offs.

It takes some time to fully understand the cost of progress. Things are not as bleak as framed in the eight trends outlined below. Moreover, some of these are a case of "*damned if you do and damned if you don't*"- i.e. either choice can and will be criticized by someone. For example, we simultaneously want an internet that promotes free speech where anyone has a voice, yet we protest when people on the fringe express their voices. The nature of democratic dialogue is that any amount of censorship will be criticised by someone, including no censorship at all. Therefore, the question is not whether there should or should not be censorship, but rather how much censorship is too much, or too little.

The internet is, ultimately, no more or no less than any other messy human project built by multiple, uncoordinated actors. We are merely figuring out how to find a new balance between newfound freedoms and age-old responsibilities. This response tries to add nuance to the eight trends as framed by the discussant, while grouping them into four related themes. The bold text in quotations is text from the framing proposition, which this piece responds to.

Theme 1: Data & Network Effects

"Firstly, and most importantly, we have lost control over our data.

Secondly, the centralization of the internet into significantly large businesses with over a billion users each has led to a reduction in the negotiating ability of individual users."

We have not *lost* control over our data; we never had any. If anything, the real trend is that we get more control over our data with every passing day. Today, the number of choices we have to make and their complex, intersecting effects leads to bounded

rationality. The problem with consent is not philosophical; it is practical. The choices are overwhelming, but we undeniably have more choice and more protections than we did in the early days of the internet.

Privacy policies and clicking for consent are simple tools that worked when the internet was a much smaller place. The number of digital services we interact with today means that no user can be rationally expected to choose options that best protect their privacy. Even if companies are mandated to disclose their data relationships transparently, most people will not read those disclosures. One can argue that harms-based policing is also unlikely to be very helpful. The threat of being sued is not going to stop companies armed to the teeth with lawyers. We saw Facebook announce an anticipated $5Bn FTC fine, and then saw its stock price go up! Regulations such as GDPR only entrench those who can pay for large compliance teams like the Googles of the world, while making life harder for upstarts.

One hopeful trend is that we see the rise of more privacy-oriented data-sharing technologies such as federated learning. The inventor of the web, Tim Berners-Lee, is building personal data-stores with agents that negotiate data sharing with applications. We see cryptography-based decentralised alternatives to centralised systems. If any of these systems go mainstream, it would mean a world of more control over more of our data! I believe that our ability to granularly control our data will only increase, and we are going to have automated or human intermediaries who will negotiate these complex choices for us.

The unionization of workers has been under threat even before the internet. There are also examples of how employees have come together politically in ways that they could not have done as effectively before the internet. Take the example of the Google walkout, where tens of thousands of employees across the world were able to organise a protest that resulted in a change in policies. Though this is admittedly a rare event, the overall story does look like the fortunes of many internet corporations are built by stepping on the backs of vulnerable workers.

Algorithms do make for lousy bosses. The gig economy works off of two clever arbitrages. It is in fixing these arbitrages that we have the hope of protecting individual rights. The first is a regulatory arbitrage: by positioning themselves as mere marketplaces, these organizations can shirk many responsibilities like benefits and a minimum wage, not afforded to their analogue counterparts. This claim of being “merely a marketplace” is bewildering because they typically control pricing and incentives, unlike a real marketplace like the stock exchange which would allow for both parties to discover a price that works mutually.

The second is a risk capital arbitrage: the private market capital afforded to a “tech startup” to enter traditional markets comes at a massive discount compared to those typically available to public market funded analogue competitors. For example, WeWork’s astronomical valuation for being a rent middleman is unavailable to any other real estate company.

This arbitrage is the golden tap: this is the real fuel that feeds blitzscaling and reduces the negotiating ability of workers in a marketplace model. This golden tap allows these companies to build a honeytrap for their workers with high incentives that disappear once they are sufficiently entrenched. Promises of quick and easy money have always lured humans. False promotion of incentives should be punished as false advertising.

These companies lured users to join by simultaneously selling services cheap while paying more to their creators. Individual rights are under risk from this completely legal behaviour. This dumping of capital needs regulation from an antitrust lens that breaks away from the Bork school of thought. Is this risk capital arbitrage crowding out competitors that would create a fairer (albeit costlier) choice? Many would claim yes, but the legal tools available do not allow us to control this behaviour.

Theme 2: Data as an Asset of the State.

"Fourth, data is being viewed as a factor of production and a national asset, as opposed to an individual right. Governments are profiling citizens.

Sixth, individuals are being attacked and weaponized."

Data is a factor of production! That does not legitimize profiling citizens or peering into their personal lives. However, think about sufficiently anonymised data sets. Merely counting the number of passengers passing through an airport at all times can help understand the economic outlook for a region. The GSTN dataset, stripped of all business identifiers while retaining HSN codes can help policymakers understand what parts of the economy are under distress. Whom does this data belong too? Whom does it hurt if released stripped of identifiers?

It is misleading to say that pitted against statutory power, individuals have no choice to part with their data. None of the recent developments has changed what data one had to share with the state to avail a service. If one is applying for a loan, the data stored about them in a public credit registry (PCR) is not different from what existing credit bureaus already have. The creation of the PCR makes it affordable to serve the excluded.

The use of unique identifiers like digital national IDs may help consolidate disparate records, but it does not mean that consolidation is impossible without them. Real names, birthdates and other details also lead to a fairly accurate match. Simultaneously, giving the same unique identifier in multiple databases, does not automatically imply consolidation. We provide our phone numbers in many, many more databases than we provide our Aadhaar number. The consolidation of large datasets, without the user's knowledge or consent, should be illegal. The problem is not the choice of the identifier; the problem is the intent of those combining these datasets, and those acquiescing to it.

India has taken a bold step, in providing tokenization by default, and virtualisation of the identifier in the Aadhaar. If one could, the safest thing to do would be to share the tokenised ID from Aadhaar, and not our phone number which is stored in plain text. Apple --whose primary business model is hardware, not advertising -- has recently added this feature to its repertoire with "Sign in with Apple". Fundamentally, this comes down to whom the user trusts: Big Tech or democratic institutions.

Theme 3: Internet and Free Speech

"Sixth, individuals are being attacked and weaponized."

"Thirdly, free speech highly dependent on a few platforms, and is being restricted by hecklers getting the veto"

"Seven, speech is being restricted via internet shutdowns, content regulation and online mobs."

In 2017, the Nobel prize in economics went to Richard Thaler for effectively manipulating people into doing things better for them in the long run. An example was discovering people's laziness in opting-out of retirement savings instead of opting-in. The internet has long known this trick of manipulating human tendencies, or "bugs" in the "rational actor" model. However, this knowledge is not necessarily always used for good.

There is truth to the fact that the internet allows any motivated individuals or organizations to spread their message far and wide, and precisely to the kind of people who would agree with it. Alternatively, the same tools could be used to target and overwhelm those who would disagree. This is a feature of the internet – it is not a bug.

As described by the framing proposition this is an instance of how people "learn through the free-flow of information and societal interactions at a global scale, without prescriptive local restrictions." That does not make it automatically acceptable in all scenarios, but it does reinforce a point from the opening argument.

An internet with absolute protection for free speech is not necessarily a great objective to have. It can cause as many harms as it prevents. When audiences are manipulated to promote generally accepted pro-social values, it is considered a *nudge*. When used to aggressively market to the individual, or promote opposing political views, it is *weaponizing the individual*. It is hard to tell them apart, especially when those "*weaponizing*" maybe equally earnest in their intention as those "*nudging*".

Defining the boundaries of free speech is not a new problem. Platforms such as Facebook adopted real-name policies precisely to moderate and increase the quality of conversation, compared to the vitriol that spewed on darker corners of the internet. Censorship is a classic case of "*damned if you do, damned if you don't*". Our real problem is not censorship, but who has the authority to censor and how fair are they.

The government, which has classically held that authority is now wrestling with platforms to have that power once again. Usually, the attitude to government censorship in these large companies is hostile. Where governments cannot participate in that decision, they choose more forceful tools like internet shutdowns. The hopeful trend is to relegate censorship to ombudsmen that we can all agree are diverse, representative and fair. Both Facebook and Google have shown precedent in moving towards such a model, and it is easy to see why.

Theme 4: Use of technology for surveillance

"Fifth, the usage of biometrics and facial recognition systems for authentication is becoming shockingly popular."

"Eight, surveillance is the new normal."

In the Indian context, biometrics are shockingly popular because shockingly, many people still cannot read or write. Ideas like passwords and OTPS are harder than merely showing up and scanning a fingerprint. In and of themselves, the use

of biometrics for authentication is not bad or evil. Many willingly use fingerprint scanners on smartphones for their convenience. The fingerprints are locally stored and never shared.

What makes the use of biometrics dangerous are using biometrics for identification (one-to-many match) and lack of a second (or more) factor(s). One-to-one matching of biometrics such as fingerprints or face with a previously recorded image does not compromise privacy by itself. However, if there is potential to use the same data for one-to-many matching, the system will soon become a tool for surveillance. This is a trickier problem but is not entirely impossible to manage.

Most solutions involve trusting an intermediary, and it is at this point that an important question comes up: who do you trust to save your biometrics but not abuse the information? Some prefer their government, some prefer private players, and some prefer not having to share it with anyone at all.

The lack of a second (or more) factor is much easier to control. Anyone who is designing a system that uses biometrics should realise that biometrics can be compromised (such as cloning of fingerprints) and build adequate safeguards and fallbacks. Almost all new biometric scanners have liveness detection and other protections.

We see a more hopeful trend. The quick adoption of biometrics also means that people are now learning about potential ways in which biometrics fail and how they can be secured. Just like in the early days of databases, most were vulnerable to SQL injection attacks. This did not mean we needed to eliminate databases; instead, we fixed how that attack could be carried out and educated developers.

Should we phase out fingerprints in favour of something harder to clone like vein prints? The answer seems like an obvious yes, but the problem is simply affordability. The point of biometrics in ID systems was too provide a low-cost method of authentication. One can argue that technology X(or Y or Z) is safer, but to make authentication useful, one has to make it *affordable as well*.

The temptation for surveillance will always remain a corrupting force. A government intent on surveillance, with a convincing narrative about a terrifying enemy, backed by a jingoist majority, is incredibly hard to stop. The only known effective technology system to control surveillance is something like Estonia's X-Road. X-Road allows citizens to see how their records were accessed and by whom. To do this requires, ironically, combining user data with a unique identifier which some argue makes surveillance *easier*. That is a tricky choice for anyone to make.

This last point dovetails into my final argument: policymakers and corporations face ridiculously hard trade-offs. It is easy for anyone with no skin in the game to criticise any idea in a vacuum and call it a worrying trend, when one does not have to make that decision. The nature of news is that we ignore ongoing, mundane tragedies to worry about future, possible tragedies bought on by new developments. What rarely gets talked about is the cost of doing nothing. The cost of doing nothing in a country like India is that hundreds of millions of people continue to remain poor, uncounted, and outside of the progress narrative. The internet is a powerful tool in empowering those individuals. They deserve the opportunities it creates for them. While we need to be cautious in our progress, let us not rob hundreds of millions of a better life now, because of the extreme apprehensions of a few.

02.
Governance

Mutually Assured Diplomacy: Governance, 'unpeace' and diplomacy in cyberspace

Dennis Broeders
Senior Fellow of The Hague Program for Cyber Norms

Introduction

Internet governance steered clear of geopolitics for quite some time. The internet's rise to global dominance really took off after the invention of the World Wide Web which coincided with the end of the cold war in the 1990s and a period of limited global strife. Geopolitics is now centre stage again with implications for internet governance and the stability of cyberspace. The stakes are much higher – engrained as the internet is in everyday life – and international tensions are growing. In this short essay I highlight three developments that are vital for the development for the international debate about internet governance and cyber diplomacy (thus also side-lining many other relevant developments): the politicisation of technical internet governance, the mismatch between the state of 'unpeace'[1] in cyberspace and the legal frameworks that aim to bring stability, and, the parallel diplomatic future for 'responsible state behaviour in cyberspace' of the UN GGE and OEWG processes.

The politics of infrastructure

For a long time, the governance of the technical infrastructure of the internet was something that happened while governments were busy making other plans. The internet expanded in scope and size, grew exponentially in terms of numbers of users and the formats of information it could support (text, audio, video) and with the rise of IoT the number of connected devices is set to grow in mindboggling numbers. For much of its existence the technical internet was relatively untouched by geopolitics. However, both geopolitics and the global internet are changing. As the internet became more engrained within our societies and economies and therefore vital for everyday life, governments began to take more notice. Moreover, different countries had different concerns. Early points of contention in internet governance focused on ICANN and the IANA transition. This was more about international political legitimacy than about the question whether the naming and numbering of the internet was adequately expanded and administered by ICANN. As the weight of the global user base of the internet shifted from its original transatlantic axis to both the East and the South of the globe, the political aspects of this specific institutional setup became contested. The fact that naming and numbering was under nominal control of the US government and the prospect of settling disputes in a Californian court was challenged by many states, even though actual disputes have been scarce.

The IANA transition was a dispute about how global internet resources could be de-Americanized, in light of geographical shifts on the internet. Now, geopolitical strife between the USA and China also follows the path of mounting technological competition. Against a background of general great power competition over global dominance and the US-Sino trade war, Artificial Intelligence (AI) has become an area of fierce and open competition between the two superpowers. While Kai-Fu Lee maintains that the US holds the better cards for finding a new qualitative leap in the evolution of AI, he maintains that we are now in an age of AI implementation for which China is much better placed.[2] As AI will be a pervasive technology – that will be integrated into many other systems from the mundane to the military – it will have infrastructural qualities and will lead to new and politicised governance questions.

With the advent of 5G networking, the securitization of the technical internet infrastructure has entered the main global stage. With the all-out resistance of the US against Huawei providing the global infrastructure for 5G internet, the technical infrastructure – and with it technical internet governance – has become thoroughly politicised. The US is worried about the security aspects of having the 5G infrastructure provided by Huawei and has been trying – with varying success – to convince allies and others to shun the Chinese bid to provide new crucial aspects of the internet's infrastructure. Again, it is no so much the quality of the technological hardware but rather the security implications as a result of the suspected privileged access of the Chinese state (espionage) to Chinese soft- and hardware – which of course echoes the earlier episode of privileged access of the American state that was revealed by Snowden.

The chances for depoliticization of technical internet governance in this era of geopolitical strife are slim. However, all countries still depend on the global internet infrastructure to function and support their digital economies, societies and governments, suggesting that there must be something of a lowest common denominator that serves the interests of most, if not all, states. For example, the call to protect the public core of the internet[3], has been gaining traction and is now part of the 2018 French initiative of the *Paris Call for Trust and Security in Cyberspace*[4] – signed by over 60 states and many companies and NGOs – and the *EU Cybersecurity Act* adopted in 2019[5]. If possible, technical internet governance should be as depoliticised as possible and be something that largely happens while states are busy making other plans again.

The state of 'unpeace' in cyberspace

States are not blind to the fact that stability in cyberspace would benefit their digital economy and would mitigate the risks of escalation of conflict. However, agreeing on core aspects of responsible behaviour in cyberspace is, and has been a cumbersome process. While the fear of the weaponization of cyberspace has been the underlying rationale for the UN GGE process, which is now in its sixth iteration, the possible strategic and military advantages that cyberspace opens up to states may stand in the way of taking big diplomatic steps in this domain. Most states are reluctant to give up possible (military) capabilities by restraining themselves when they cannot be sure that other states will do the same. The result has often been framed as a militarization of cyberspace, which in turn has facilitated an ongoing debate about if and how International Humanitarian Law applies to cyberspace, both in UN and regional diplomatic fora and through non-state initiatives such as the Tallinn process.

The question is whether the frame of militarization fits the reality at this moment. Even though many states have in recent years founded military Cyber Commands in varying degrees of professionalism and readiness, the main cyber operations the world worries about are the so-called 'below-the-threshold operations' – i.e. they do not add up to 'war'- and are mostly executed by (military) intelligence agencies or proxies.[6] The first are not in any direct sense regulated by international law, while the second per definition operate outside of international law. The cyber operations of intelligence agencies – rather than militaries – and proxy actors have created a state of permanent 'unpeace' with an intensity that sits well below the threshold that would qualify it as a military conflict. Some countries thrive in this permanent state of digital unrest and are able to project power far beyond their 'physical' means. There is debate on the question whether or not – and under which conditions - these low-level conflicts are prone to escalation of conflict, but tensions surely have been rising.[7] Moreover, this is not just the domain of espionage and cyber sabotage anymore, but with the increase of mis- and disinformation operations it is also, and increasingly, the domain of the integrity of our information environment, which influences the nature and the quality of the domestic political debate. Cyber operations now also reach the heart of the domestic political process.

Crucially, however, if the nature of cyber conflict is not (yet) military in nature, we may be barking up the wrong legal tree when it comes to the international debate about international humanitarian law as a means to promote responsible state behaviour.[8] Intelligence agencies are the proverbial elephants in the diplomatic room: everyone knows they are there, but all states are unwilling to discuss their operations, let alone regulate them by international law. Formal public attribution now seems the main way of addressing these rising tensions, but that is largely a 'western affair' (i.e. most formal attributions have been made by western states) and comes with its own difficulties. However, if much of the international diplomatic effort – in the UN GGE and in other fora – is poured into defining the applicability of the Law of Armed Conflict, the world may end up ignoring the conflicts and 'unpeace' – and the actors behind it - that most states seem to worry about most. Herein lies another challenge for the political governance of cyberspace.

Mutually Assured Diplomacy

After the 2017 round of the UN GGE failed to produce a consensus report many declared the UN track for discussing responsible state behaviour in cyberspace dead. However, the reports of the GGE's death seem to have been greatly exaggerated, as the sixth round of the process is to start in December of 2019. The fact that 25 UN member states will meet to discuss the application of international law to the cyber domain and cyber norms again is in itself not a guarantee for success, although sources say that the 2017 round found quite a lot of common ground as well as the disputes that eventually blocked consensus. But when in November 2018, the General Assembly of the UN voted through the American resolution that installed a new UN GGE[9] it thickened the diplomatic cyber plot by also voting through the Russian resolution that called for the installation of an Open-Ended Working Group (OEWG) on the same issues.[10] So there are now two parallel diplomatic tracks looking at roughly the same issues. Russia has claimed the moral high ground and played the card of international political legitimacy. The Russian delegation built its case for the OEWG on the principle that it is open to the participation of all states and renounced the UN GGE as "the practice of club agreements that should be sent into the annals of history".[11] As one of the permanent members of the Security Council

Russia is also assured of a seat in the UN GGE club, but given their sponsorship of the OEWG resolution the stakes are high. The parallel tracks have ushered in a state of Mutually Assured Diplomacy: it is more than likely that either both processes yield a result or that both will fail. If one fails on account of one political camp, the other camp is likely to respond in kind and derail the other process. This will complicate an already difficult process. Getting agreement on *how* existing international law applies to cyberspace - generally agreed to be the stumbling block of the 2017 GGE round - now has to be navigated in two processes that are at once separate and joined at the hip. Add in the new geopolitics of technical internet governance and rising tensions about the permanent state of 'unpeace' in cyberspace and those working on the diplomatic challenges of cyberspace stability and internet governance have their work cut out for them.

Endnotes

1 Lucas Kello (2017) The Virtual Weapon and International Order. New Haven and London: Yale University Press.

2 Kai-Fu Lee (2018) AI Superpowers. China, Silicon Valley and the New World Order. Boston: Houghton Mifflin Harcourt

3 See Dennis Broeders (2015) The Public Core of the Internet. An International Agenda for Internet Governance. Amsterdam: Amsterdam University Press and the 2017 Call to Protect the Public core of the Internet of the Global Commission on the Stability of Cyberspace.

4 The Paris Call for Trust and Security in Cyberspace, 12 November 2018

5 The EU Cyber security Act, 17 April 2019. See paragraph 23 and Article 5.3

6 Sergei Boeke and Dennis Broeders (2018) The Demilitarisation of Cyber Conflict', Survival, Vol. 60 (6): 73-90; Tim Maurer (2018) Cyber Mercenaries. The State, Hackers and Power. Cambridge: Cambridge University Press.

7 Jason Healey, The implications of persistent (and permanent) engagement in cyberspace, Journal of Cybersecurity, Volume 5, Issue 1, 2019, tyz008, https://doi.org/10.1093/cybsec/tyz008

8 Sergei Boeke and Dennis Broeders (2018) The Demilitarisation of Cyber Conflict', Survival, Vol. 60 (6): 73-90

9 https://undocs.org/A/C.1/73/L.37

10 https://undocs.org/A/C.1/73/L.27/Rev.1

11 Statement of the Russian delegation to the UN General Assembly First Committee, 8 November 2019, Cited in Xymena Kurowska (2019) The politics of cyber norms: Beyond norm construction towards strategic narrative Contestation. EU Cyber Direct: Research in Focus, p. 9.

"Politics by other means": Fostering positive contestation and charting 'red lines' through global governance in cyberspace

Arindrajit Basu
Senior Policy Officer, The Centre for Internet and Society

The past year has been a busy one for the fermentation of global governance efforts in cyberspace[1] with multiple actors-states, industry, and civil society spearheading a variety of initiatives. Given the multiplicity of actors, ideologies, and vested interests at play in this ecosystem, any governance initiative will be, by default, political, and desirably so.

There is no silver bullet that will magically result in universally acknowledged rules of the road. Instead, through consistent probing and prodding, the global community must create inclusive processes to galvanize consensus to ensure that individuals across the world can repose trust and confidence in their use of global digital infrastructure.[2]This includes both 'red lines' applicable to clearly prohibited acts of cyberspace and softer norms for responsible state behaviour in cyberspace, that arise from an application of the tenets of International Law to cyberspace.

Infrastructure is political

Networked infrastructures typically originate when a series of technological systems with varying technical standards converge, or when a technological system achieves dominance over other self-contained technologies.[3] Through this process of convergence, networked infrastructures must adapt to a variety of differing political conditions, legal regulations and governance practices.[4] Internet infrastructure was never self-contained technology, but an amalgamation of systems, protocols, standards and hardware along with the standards bodies, private actors and states that define it.[5] The architecture has always been deeply socio-technical[6] and any attempt to severe the technology from the politics of internet governance would be a fool's errand.

Politics catalyzed the development of the technological infrastructure that lead to the creation of the internet. During the heyday of nuclear brinkmanship between the USA and USSR, Paul Baran, an engineer with the US Department of Defense think tank RAND Corporation was tasked with building a means of communication that could continue running even if some parts were to be knocked out by a nuclear war.[7]

As Baran's 'Bomb proof network' morphed into the US Department of Defense-funded ARPANET, it was initially apparent that it was not meant for either mass or commercial use, but instead saw its nurturing in the US as a tool of strategic defense.[8]

This enabled the US to retain a disproportionate -- and till the 1990s, relatively uncontested -- influence on internet governance. As the internet rapidly expanded across the globe, various actors found that single state control over an invaluable global resource was unjust.[9] Others ([9]which included US Senator Ted Cruz), argued that the internet would be safer in the hands of the United States than an international forum whose processes could be reduced to stalemate as a result of politicized conflict between democratic and non-democratic states who seek to use online spaces as an instrument of suppression.[10] The ICANN and IANA transitions were therefore not rooted in technical considerations but much-needed geopolitical pressure from states and actors who felt 'disregarded'[11] in the governance of the internet. An inclusive multi-stakeholder process fueled by inclusive geopolitical contestation is far more effective in the long run, and has the potential of respecting the rights of 'disregarded' communities all across the globe far more than a unilateral process that ignores any voices of opposition.

It is now clear that despite its continued outsized influence, the United States is no longer the only major state player in global cyber governance. China has propelled itself as a major political and economic challenger to the United States across several regimes[12], including in the cyber domain. China's export of the 'information sovereignty'[13] doctrine at various cyber norms proliferation fora, including at the United Nations-Group of Governmental Experts (GGE), and regional forums like the Shanghai Co-operation (SCO), is an example of its desire to impose its ideological clout on global conceptions of the internet.

As a rising power, China's aspirations in global internet governance are not limited to ideology. China is at an 'innovation imperative', where it needs to develop new technologies to retain its status and fuel long-term growth.[14] This locks it into direct economic, and therefore strategic competition with the United States that seeks to retain control over the same supply chains and continues to assert its economic and military superiority.

China has dominated the 5G space in an unprecedented way, and has been a product of a concerted 'whole of government' effort. [15] Beijing charted out an industrial policy that enabled the deployment of 5G networks as a key national priority.[16]China has also successfully weaponized global technical standard-setting efforts to promote its geo-economic interests.[17] Reeling from the failure of its domestic 3G standard that was ignored globally, China realised the importance of the 'first-movers' advantage' in setting standards for companies and businesses.[18] Through an aggressive strategic push at a number of international bodies such as the International Telecommunications Union, China's diplomatic pivot has allowed it to push standards established domestically with little external input, thereby giving Chinese companies the upper hand globally.[19]

Politics continues to frame the technical solutions that enable cybersecurity.[19] Following Snowden's revelations, some stakeholders in the global community have shaped their politics to frame the problem as one of protecting individuals' data from governments and private companies looking to extract and exploit it. The technical solutions developed in this frame are encryption standards and privacy-

enhancing technologies. However, intelligence agencies continue to frame the problem differently: they see it as an issue of collecting and aggregating data in order to identify malicious actors and threat vectors. The technical solutions they devise are increased surveillance and data analysis -- problems the first framing intended to solve. The techno-political gap, both in academic scholarship and global norms proliferation efforts continues to jeopardize attempts at framing cybersecurity governance.[20] Instead of artificially depoliticizing technology, it is imperative that we ferment political contestation in a manner that holistically promulgates the perception that internet infrastructure can be trusted and utilised by individuals and communities around the world.

Fostering 'red lines' and diffusing 'unpeace' in cyber-space

'Unpeace' in cyberspace continues to ferment through 'below the threshold' operations that do not amount to the 'use of force' as per Article 2(4), or an 'armed attack' triggering the right of self-defense under Article 51 of the United Nations Charter. This makes the application of *jus ad bellum* ('right to war') inapplicable to most cyber operations.[21] However, the application of 'jus in bello' (law that governs the way in which warfare is conducted) or International Humanitarian Law (IHL) does not require armed force to be of a specific intensity but seeks to protect civilians and prevent unnecessary suffering. Therefore the principles of IHL that have evolved in The Geneva Conventions should be used as red lines that limit collateral damage as a result of cyber operations.[22] No state should conduct cyber operations that intend to harm civilians, and should us all means at its disposal to avoid this harm to civilians. It should act in line with the principles of necessity[23] and proportionality.[24]

Cultivating 'red lines' is easier said than done. The debate around the applicability of IHL to cyberspace was one of the reasons for the breakdown of the fifth UN-GGE in 2017.[25] States have also been reluctant to state their positions on the rules developed by the International Group of Experts (IGE) in the Tallinn Manual.[26] This is due to two main reasons. First, not endorsing the rules may allow them to retain operational advantages in cyberspace where they continue engaging in cyber operations without censure.Second, even those states who wish to apply and adhere to the rules hesitate to do so in the absence of effective processes that censure states that do not comply with the rules.

Both these issues stem from the difficulties in attributing a cyber attack to a state as cyber attacks are multi-stage, multi-step and multi-jurisdictional, which makes the attacker several degrees removed from the victim.[27] Technical challenges to attribution, however should not take away from international efforts that adopt an integrated and multi-disciplinary approach to attribution which must be seen as a political process working in conjunction with robust technical efforts.[28] The Cyber Peace Institute, which was set up earlier in September 2019, and adopts an ecosystem approach to studying cyber attacks, thereby improving global attribution standards may institutionally serve this function.[29] As attribution processes become clearer and hold greater political weight, an increasing number of states are likely to show their cards and abandon their policy of silence and ambiguity -- a process that has already commenced with a handful of states releasing clear statements on the applicability of international law in cyberspace.[30]

Below the threshold operations are likely to continue. However, the process of contestation should result in the international community drawing out norms that ensure that public trust and confidence in the security of global digital infrastructure is not eroded. This would include norms such as protecting electoral infrastructure or a prohibition on coercing private corporations to aid intelligence agencies in extraterritorial surveillance[29] The development of these norms will take time and repeated prodding. However, given the entangled and interdependent nature of the global digital economy, protracted effort may result in universal consensus in some time.

The Future of Cyber Diplomacy

The recently rejuvenated UN driven norms formulation processes are examples of this protracted effort. Both the Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG) processes are pushing states towards publicly declaring their positions on multiple questions of cyber governance, which will only further certainty and predictability in this space. The GGE requires all member states to clearly chart out their position on the applicability of various questions of International Law, which will be included as an Annex to the final report and is definitely a step in the right direction.

There are multiple lessons from parliamentary diplomacy culminating in past global governance regimes that negotiators in these processes can borrow from.[31] As in the past, the tenets of international law can influence collective expectations and serve as a facilitative mechanism for chalking out bargaining points, and driving the negotiations within an inclusive, efficient and understandable framework.[32]

Both processes will be politicized as before with states seeking to use these as fora for furthering national interests. However, this is not necessarily a bad thing. Protracted contestation is preferable to unilateralism where a select group of states decides the future of cyber governance. The inclusive, public format of the OEWG running in parallel to the closed door deliberations at the GGE enables concerted dialogue to continue. Most countries had voted for the resolutions setting up both these processes and while the end-game is unknown, it appears that states remain interested in cultivating cyber norms.

Of course, the USA and its NATO allies had voted against the resolution setting up the OEWG and Russia, China and the SCO allies had voted against the resolution resurrecting the GGE. However, given the economic interests of all states in a relatively stable cyberspace,it is clear that both these blocks desire global consensus on some rules of the road for responsible behaviour in cyberspace. This means that both processes may arrive at certain similar outcomes. These outcomes might over time evolve into norms or even crystallise into rules of customary international law if they are representative of the interests of a large number of states.

However, sole reliance on state-centric mechanisms to achieve a stable governance regime may be misplaced. As seen with Dupont's contribution to the Montreal Protocol that banned the global use of Chloro-Fluoro-Carbons (CFCs)[33] or the International Committee of the Red Cross's concerted efforts in rallying states to sign the Additional Protocols to the Geneva Conventions[34], norm-entrepreneurship and the mantle of leadership in norm-entrepreneurship need not be limited to state

actors. Non-state actors often have the gifts of flexibility and strategic neutrality that make them a better fit for this role than states. Microsoft's leadership and its ascent to this leadership mantle in the cyber governance space must therefore be taken heed off. The key role it played in charting out the CyberSecurity Tech Accords, Paris Call for Trust and Security in Cyberspace and its most recent initiative, the Cyber Peace Institute, must be commended. However, the success of its entrepreneurship relies on how well it can work both with multilateral mechanisms under the aegis of the United Nations and multi-stakeholder fora such as the Global Commission on Stability in Cyberspace. This will lead to a cohesive set of rules that adequately govern the conduct of both state and non-state actors in cyberspace.

It is unfortunate, however,that most governance efforts in cyberspace are driven by the United States or China or their allies. For example, only UK[35], France[36], Germany,[37] Estonia[38],Cuba[39] (backed by China and Russia), and the USA[40] have all engaged in public posturing advocating their ideological position on the applicability of International Law in cyberspace in varying degrees of detail with other countries largely remaining silent.Other emerging economies need to get into the game to make the process more representative and equitable.

More recently, India has begun to take a leadership role in the global debate on cross-border data transfers, spurred largely by their domestic political and policy ecosystem championing 'digital nationalism.' At the G20 summit in Osaka in July this year, India, alongside the BRICS grouping emphasized the development dimensions of data for emerging economies and pushed the notion of 'data sovereignty'-broadly understood as the sovereign right of nations to govern data within their territories/ jurisdiction in the national interest and for the welfare of its people.[41]Resisting calls from Western allies including the United States to get on board Japan's initiative promoting the free flow of data across borders, Vijay Gokhale also mentioned that discussions on data flows must not take place at plurilateral forums outside the World Trade Organization as this would prevent inclusive discussions.[42]This form of posturing should be sustained by emerging economies like India and extended to the security domain as well through which the hegemony that a few powerful actors retain over the contours of cyber governance can be reduced.

To paraphrase Clausewitz, technological governance is the conduct of politics by other means. Internet infrastructure has become so deeply intertwined with the political ethos of most countries that it has become the latest front for geo-political contestation among state and non-state actors alike. Politicizing cyber governance prevents a deracinated approach to the process that ignores simmering inequalities, power asymmetries and tensions that a limited technical lens prevents us from viewing.

The question is, not *if* but *how* cyber governance will be politicized. Will it be a *politics of inclusion* that protects the rights of the disregarded and adequately represents their voices in line with the requirements of International Law, or will it be a *politics of convenience* through which states and non-state actors utilise cyber governance for reaping strategic dividends? The global cyber policy ecosystem must continue the battle to ensure that the former remains essential.

Endnotes

1 Arindrajit Basu and Elonnai Hickok (2018) " Cyberspace and External Affairs: A memorandum for India" https://cis-india.org/internet-governance/files/cyberspace-and-external-affairs, 8-13.

2 In its draft definition of cyber stability,The Global Commission on the Stability of Cyberspace has adopted a bottom up user centric definition of Cyber Stability where individuals can be confident in the stability of cyberspace as opposed to an objective top-down determination of cybersecurity metrics. https://cyberstability.org/news/request-for-consultation-definition-of-stability-of-cyberspace/

3 PN Edwards, GC Bowker Jackson SJ, R Williams 2009. Introduction: an agenda for infrastructure studies.J. Assoc. Inf. Syst.10(5):364–74

4 Brian Larkin, " The Politics and Poetics of Infrastructure" Annual Rev. Anthropol 2013,42:327-43

5 Ibid.

6 Kieron O'Hara and Wendy Hall, " Four Internets: The Geopolitics of Digital Governance" CIGI Report No.208, December2018,https://www.cigionline.org/sites/default/files/documents/Paper%20no.206web.pdf

7 Cade Metz, "Paul Baran, the link between nuclear war and the internet" Wired, 4th Sept, 2012,https://www.wired.co.uk/article/h-bomb-and-the-internet

8 Kal Raustila (2016) "Governing the Internet" American Journal of International Law 110:3,491

9 Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine & Mark Raymond, The Emergence of Contention in Global Internet Governance 3 (Global Comm'n on Internet Governance, Paper Series No. 17, July 2015), at https://www.cigionline.org/sites/default/files/no17.pdf.

10 Klint Finley," The Internet Finally Belongs to Everyone", Wired, March 18th, 2016,https://www.wired.com/2016/10/internet-finally-belongs-everyone/

11 Richard Stewart (2014),Remedying Disregard in Global Regulatory Governance:Accountability, Participation and Responsiveness" AJIL 108:2

12 Tarun Chhabra, Rush Doshi, Ryan Hass and Emilie Kimball, "Global China: Domains of strategic competition and domestic drivers" Brookings Institution, September 2019,https://www.brookings.edu/research/global-china-domains-of-strategic-competition-and-domestic-drivers/

13 According to this view, a state can manage and define its 'network frontiers; through domestic legislation or state policy and patrol information at it state borders in any way it deems fit. Yuan Yi,. "网络空间的国界在哪 " [Where Are the National Borders of cyberspace]? 学习时报.May 19, 2016. <http://www.studytimes.cn/zydx/KJJS/JUNSZL/2016-05-19/5690.html>

14 Anthea Roberts, Henrique Choer Moraes and Victor Ferguson (2019), "Toward a Geoeconomic Order in International Trade and Investment" (May 16, 2019) https://ssrn.com/abstract=3389163

15 Eurasia Group (2018), "The Geopolitics of 5G" <https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf>

16 Ibid.(In 2013, the Ministry of Industry and Information Technology (MIIT), the National Development and Reform Commission (NDRC) and the Ministry of Science and technology (MOST) established the IMT-2020 5G Promotion Group to push for a government all-industry alliance on 5G.)

17 Bjorn Fagersten&Tim Ruhlig (2019)," China's standard power and it's geopolitical implications for Europe" Swedish Institute for International Affairs,https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2019/ui-brief-no.-2-2019.pdf

18 Alan Beattie, " Technology: how the US, EU and China compete to set industry standards" Financial Times,Jul 14th,2019 <https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271>

19 Laura Fitchner, Walter Pieters.,&Andre Herdero Texeira(2016). Cybersecurity as a Politikum: Implications ofSecurity Discourses for Infrastructures. In Proceedings of the 2016 New Security Paradigms Workshop (36-48). New York: Association for Computing Machinery (ACM

20 Michael Crosston," Phreak the Speak: The Flawed Communications within cyber intelligentsia" in Jan-Frederik Kremer and Benedikt Muller,"Cyberspace and International Relations: Theory, Prospects and Challenges (2013,Springer) 253.

21 "Fundamental Principles of International Humanitarian Law",https://casebook.icrc.org/glossary/fundamental-principles-ihl

22 Veronique Christory " Cyber warfare: IHL provides an additional layer of protection" 10 Sept,2019,https://casebook.icrc.org/glossary/fundamental-principles-ihl

23 See https://casebook.icrc.org/glossary/military-necessity (The "principle of military necessity" permits measures which are actually necessary to accomplish a legitimate military purpose and are not otherwise prohibited by international humanitarian law. In the case of an armed conflict the only legitimate military purpose is to weaken the military capacity of the other parties to the conflict.

24 See https://casebook.icrc.org/glossary/proportionality The principle of proportionality prohibits attacks against military objectives which are "expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated"

25 Declaration by Miguel Rodriguez, Representative of Cuba, At the final session of group of governmental experts on developments in the field of information and telecommunications in the context of international security (June 23 2017), at <https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf

26 Dan Efrony and Yuval Shany (2018), " A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice" AJIL 112:4

27 David Clark and Susan Landau. "Untangling Attribution." Harvard National Security Journal (Harvard University) 2 (2011

28 Davis, John S., Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern and Michael S. Chase. Stateless Attribution: Toward International Accountability in Cyberspace. Santa Monica, CA: RAND Corporation, (2017). At <https://www.rand.org/pubs/research_reports/RR2081.html.>

29 See "CyberPeace Institute to Support Victims Harmed by Escalating Conflicts in Cyberspace"https://cyberpeaceinstitute.org/latest-insights/2019-09-26-cyberpeace-institute-to-lead-global-action-against-cyberattacks

30 Dan Efrony and Yuval Shany (2018), " A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice" AJIL 112:4

31 Arindrajit Basu and Elonnai Hickok (2018), "Conceptualizing an International Security architecture for cyberspace" https://cis-india.org/internet-governance/files/gcsc-research-advisory-group.pdf

32 Monica Hakimi (2017), "The Work of International Law," Harvard International Law Journal 58 : 1.

33 James Maxwell and Forrest Briscoe (2007)," There's money in the air: The CFC Ban and Dupont's Regulatory Strategy" Business Strategy and the Environment 6, 276-286.

34 Francis Buignon (2004). "The International Committee of the Red Cross and the development of international humanitarian law." Chi. J. Int'l L.5: 191

35 Jeremy Wright, "Cyber and International Law in the 21st Century" Gov.UK https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

36 Michael Schmitt, "France's Major Statement on International Law and Cyber: An Assessment"Just Security, September16th,2019,https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/

37 Nele Achten," Germany's Position on International Law in Cyberspace," Lawfare, Oct 2,2018,https://www.lawfareblog.com/germanys-position-international-law-cyberspace

38 Michael Schmitt, "Estonia Speaks out on Key Rules for Cyberspace" Just Security,June 10,2019,https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/

39 https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf

40 https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf

41 Justin Sherman and Arindrajit Basu," Fostering Strategic Convergence in US-India Tech Relations: 5G and Beyond," The Diplomat,Jul 03,2019,https://thediplomat.com/2019/07/fostering-strategic-convergence-in-us-india-tech-relations-5g-and-beyond/

42 Aditi Agrawal," India and Tech Policy at the G20 Summit," Medianama, Jul 1,2019,https://www.medianama.com/2019/07/223-india-and-tech-policy-at-the-g20-summit/

Public Attribution and its Scope and Efficacy as a Policy Tool in Cyberspace

Anushka Kaushik
Research Fellow, Globsec

Introduction

The quest for stability in cyberspace has seen governments try and test various policy tools and processes with little success. Even as countries come together under the aegis of the United Nations – in the form of the sixth iteration of the UN Group of Governmental Experts (UNGGE) and the newly formed Open Ended Working Group -to arrive at a consensus on cyber norms, there are definitional disagreements on what constitutes 'stability'. Usual suspects like China and Russia have continued to stress their approach to regulation and governance which stems more from information control and less from securing networks, which is unlikely to change in the near future. The need to develop global norms that should guide governments' behaviour in cyberspace, however, has never been stronger. Due to the ubiquity of digital networks and the Internet, cyberspace is undeniably a domain to carry out targeted attacks that seek to destabilise a country's services and infrastructure. Calls of 'cyber war' and a 'Digital Pearl Harbour' may be exaggerated and/or problematic but there's no denying that there's a dire need to revisit the old rule book – or publish a new one altogether – to monitor and regulate unlawful activities in cyberspace. Over the past few years, a number of cyber-attacks made global headlines owing not only to the sheer scale of financial and infrastructural loss but because they were attributed to nation-states or groups with direct affiliations to governments. WannaCry, a ransomware attack that impacted almost one hundred and fifty countries in 2017 resulting in the loss of billions of dollars, was publicly attributed to North Korea by the governments of the United Kingdom and the United States.

Public attribution of a cyber-attack is increasingly being used as a tool by governments to draw red lines of what constitutes acceptable state behavior in cyberspace. The rationale of calling out malicious behavior is simple enough but as this paper argues, is grossly limited in its application and the ultimate goal of ensuing stability in cyberspace. It's important to note that public attribution is not a tool used only by states. One of the most significant and possibly game-changing trends in the field of attribution – and politics of cyberspace governance by extension – has been the level of involvement of private sector firms in attributing cyber-attacks to governments and non-state actors. According to the Cyber Operations Tracker created by the Council on Foreign Relations, 85% of cyber-attacks resulted in some

form of public attribution between 2016 and 2018, where 15% of those were carried out by governments. The countries to which attacks were most commonly attributed were China, Russia, North Korea, and Iran[1]

Why public attribution?

Attribution in cyberspace is notoriously difficult. It is a mix of behavioral patterns, technical forensics, errors made, style and methodology of an intrusion, geopolitical circumstances, and historical relationships. Attribution goes beyond the simple action of finding out who's responsible behind aggressive behavior online[2]. It typically involves analysis at three levels; the technical (how), the operational (what), and the strategic (who and why)[3]. To deem a state responsible for a cyber-attack, however, is a complex process not least because there is no universal source of international law regulating principles of state responsibility and malicious behavior. Currently, a confluence of secondary sources and bilateral agreements provides suggestions to maneuver international humanitarian law in the context of cyber incidents. As instances of state-directed cyber intrusions have increased significantly, numerous governments have also set up Cyber Commands in the hope to thwart attacks and mitigate consequences. The use of a proxy in cyberspace, defined as "an intermediary that conducts or directly contributes to an offensive *cyber* operation that is enabled knowingly, actively or passively, by a beneficiary who gains advantage from its effect", by states has tremendous consequences for the attribution process as well as the formulation of global norms[4].

Public attribution of cyber-attacks is regarded as an important policy tool in cyberspace governance and regulation. There are several arguments made in favor of the naming and shaming doctrine – which is a common method used to deter bad conduct of other nations[5]. These range from its use as a deterrent to its abilities in rallying several countries towards a coordinated response against malicious behavior. In October 2018, the governments of The Netherlands, UK and the US publicly accused Russia's intelligence authority GRU of orchestrating a cyber- attack on the Organisation for the Prohibition of Chemical Weapons (OPCW) where investigations were being undertaken on the attempted assassination of Sergei Skripal[6]. Dutch Defense Minister Ank Bijleveld stated that this kind of public attribution was "intended as an unambiguous message that the Russian Federation must refrain from such actions"[7]. This somewhat coordinated international response harshly condemning Russia's actions could contribute to the norms-building process and delineating what constitutes irresponsible behavior in cyberspace, as more countries establish red-lines.

Public attribution of state attacks is used as one of the tools of deterrence within cyberspace[8]. The rationale is simple; exposure of a government's malicious activities with credible and verifiable evidence will deter them from continuing bad behavior. Increased involvement of private sector firms – some notable examples include CrowdStrike and FireEye – has prompted many to call for a more proactive role by governments in public attribution. The gist of the argument is that firms are guided by commercial interests and to ultimately sell their services and thus, should not be the primary actors attributing malicious activities to nation-states[9]. Furthermore, attribution of cyber-attacks to governments can be seen as interference with a country's foreign policy, possibly disincentivizing firms to publicly share information[10].

A final case in favor of public attribution by governments is premised on the sheer lack of regulatory and arbitration processes to address malicious behavior in cyberspace. While countries deliberate on applying Law of Armed Conflict or International Humanitarian Law to cyberspace activities and the twin UN processes get underway, there is complete uncertainty whether a single source for cyberspace regulation can be developed or if such a regulation is even necessary. With no recourse to international law and mounting state-directed cyber-attacks including the increased use of cyber proxies, public attribution becomes one of the very few ways of responding to state aggression.

Limited efficacy of public attribution

How successful has public attribution of cyber-attacks proven to be? Citing involvement of limited actors, failure of consensus-building to impose strict measures, and its narrow scope as a deterrent, I argue that we shouldn't exaggerate its efficacy as a policy tool.

Involvement of few states

Looking at past cyber incidents, one can safely say that the theatre of public attribution only has a few actors. The Five Eyes – US, UK, Canada, France, New Zealand, and Australia – and The Netherlands have been far more active in public denouncements of state aggression in cyberspace. This is a small number given the magnitude of suspected state-directed cyber intrusions. In 2018, the White House National Cyber Strategy stated the importance of "working in concert with a broad coalition of like-minded states" towards cyber deterrence however this coalition has hitherto remained limited[11]. There can be several reasons why more states aren't participating in denouncements. Public attribution is a decision guided primarily by geopolitical considerations and foreign policy objectives. Governments could have compelling evidence against a nation-state and still choose not to publicly accuse a state given strategic, political, or even domestic factors. Further, while technical attribution abilities are improving, the risk of misattribution is still quite high especially with the use of false flags, as seen in the South Korean Winter Olympics in 2018[12]. Attribution to a nation-state must have a high degree of credibility and transparency for it to be an effective tool and public denouncement might not be a risk worth taking for many victim governments. If public attribution is exercised only by a handful of governments, its efficacy in both norms-building and as a deterrent is severely limited.

Failure of consensus-building in imposing strict measures

Without imposing real costs and measures, publicly denouncing a government – especially repeat offenders – can end up being a futile exercise. However, building consensus for imposing sanctions among members of the European Union, for example, has been tricky. While the implementing guidelines outlined in the EU Cyber Diplomacy Toolkit have listed restrictive measures like sanctions, the EU has generally neither attributed cyber-attacks nor taken measures against states which have been identified as perpetrators[13]. In the case of the OPCW cyber-attack on the headquarters in The Hague, very few EU member-states publicly voiced their support to The Netherlands in condemning the Russian Federation. Getting twenty-eight member-states of the EU to unanimously agree on restrictive measures on a

state accused of perpetrating a cyber-attack is not likely. In addition to geopolitical considerations that may sway decisions of certain member-states against restrictive measures, differing technical capabilities and threat assessment indicators are also factors in opting out of public denouncements even within the aegis of the EU. Similarly, even as NATO Secretary-General Stoltenberg stated that the collective defense doctrine is applicable to cyberspace, the expectation that allies with differing intelligence capabilities and technical wherewithal will be on the same page in cyber attribution processes seems problematic. If the likelihood of public attribution being followed by concrete measures is low, denouncements alone might be ineffectual in the long-run.

Narrow scope as a deterrent

For public attribution to be an effective deterrent, it has to be credible and evidence-based. Unsurprisingly, states have been reluctant to reveal too many details about their attribution processes and how they reached certain conclusions, which are usually arrived at through a mix of technical, operational, and strategic factors. While there are obvious incentives for this decision, not providing substantial proof hurts the credibility of the government attributing an attack as well as allows a certain level of plausible deniability to the accused state. Further, according to the 2015 UNGGE report, countries must substantiate claims of international wrongdoings by states. In the case of the WannaCry attribution in October 2018, the US provided almost no public evidence that led them to believe it was North Korea and did not reveal plans for retaliatory measures, arguing that the aim was to increase accountability. Almost a year later, in September 2019, the US Department of the Treasury announced sanctions targeting Lazarus and two other hacking groups, believed to be affiliated with the North Korean military. The Catch-22 at play – where governments cannot reveal their attribution processes but need to show credible proof for effective cyber deterrence - renders the abilities of public attribution as a deterrent limited especially if it's neither followed by concrete measures nor supported by additional states.

Conclusion

Given that there's currently no regulatory mechanism or consensus on what constitutes appropriate behavior in cyberspace, there are limited options at the disposal of policymakers to address rapidly growing tensions precipitated by state-sponsored cyber aggression. As cyber-attacks increase both in number and scale, some countries have used public denouncements of accused governments as a way to enforce accountability and deter future attacks. This strategy can be useful and plays an important role in affirming culpability of malicious behavior. However, its application is limited for three reasons; the involvement of only a few states, the failure of consensus-building to impose strict measures, and its narrow scope as a deterrent.

The credibility of attribution still remains a challenge, more so since states are constrained by how much their intelligence authorities can actually reveal while communicating to the public. Alternative mechanisms like stateless attribution by the RAND Corporation, for example, which calls for a Consortium that would provide an independent investigation of major cyber incidents and would ideally exclude the formal representation of nation-states, have potential to introduce a greater level of credibility[14]. Additionally, companies like Microsoft have previously

suggested an international body for peer-reviewed technical attribution for major cyber-attacks. While it's difficult to predict how viable such a model will be, working on standardizing and framing attribution could improve the process considerably.

Endnotes

1 "Cyber Operations Tracker", Council on Foreign Relations, last modified July 1, 2019, https://www.cfr.org/interactive/cyber-operations

2 Kaushik, Anushka, "Attribution in Cyberspace: Beyond the 'Whodunnit'". GLOBSEC. May 2018.

3 Rid, T & Ben Buchanan. "Attributing cyber-attacks" Journal of Strategic Studies, 38, no. 1-2. December 2014

4 Maurer, Tim. "Of Brokers and Proxies". In Cyber Mercenaries: The State, Hackers, and Power, 1-68. Cambridge: Cambridge University Press 2018

5 Baker, Stewart, "The Attribution Revolution". Foreign Policy. 17 June 2013

6 Crerar, Pippa., Jon Henley and Patrick Wintour. "Russia accused of cyber-attack on chemical weapons watchdog". The Guardian. 4 October 2018.

7 Sanders-Zakre, Alicia. "Russia charged with OPCW hacking attempt" Arms Control Today. November 2018.

8 Painter, Chris. "Deterrence in Cyberspace". Australian Strategic Policy Institute, June 2018.

9 Rich, William. "The US leans on private firms to expose foreign hackers". The Wired. 29 October 2018.

10 There are several arguments furthered in favour of the increased involvement of private sector firms including sophisticated technical attribution capabilities, credible and evidence-based deterrence, which are not within the purview of this paper.

11 National Cyber Strategy of the United States of America. September 2018

12 Greenberg, Andy. "Hackers have already targeted the Winter Olympics – and may not be done". 1 February 2018.

13 Ivan, Paul. "Responding to Cyber Attacks: Prospects for the EU Cyber Diplomacy Toolbox". European Policy Centre. March 2019.

14 Davis, John S. II, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, and Michael S. Chase, Stateless Attribution: Toward International Accountability in Cyberspace. Santa Monica, CA: RAND Corporation, 2017.

03.
Society

Interrogating the future of digital democracies

Dr. Lydia Kostopoulos
Disruptive Technology Educator and Consultant

Democratic governance is one of the oldest forms of political governance, dating back to 507 B.C.E. in Ancient Greece. Most people believe that since then, democracy has only flourished. The reality is that 'ancient democracy' collapsed; first into anarchy and then into dictatorship, heralding the medieval period, also known as the dark ages. When the United States of America declared itself a sovereign nation in 1776 (1776-1789) and ratified its new government, it was the first 'modern democracy'. Near simultaneously on the other side of the Atlantic, the French revolution overthrew the monarchy to establish a republic with liberal democratic values. Both countries experienced violent political periods a few decades after becoming democracies and have grown into their form of governance over the centuries since their forming.

Today, the United States and France are liberal democracies that continue to uphold democratic values, human rights and maintain their commitment to the political freedom of their citizens. This is not without struggle, because democracy is messy and it is a constant dialogue between citizens and their elected leaders. Citizens demand that their many voices be heard, that actions be taken in support of different interest groups, and that elected leaders be held accountable. Democracy is naturally messy because it is meant to represent an entire nation of people who think differently and want different policies from their leaders. Liberal democracies are the preferred choice of government for those who wish to elect their leaders and, no matter the outcome, experience a peaceful transition of power. It is the preferred choice for those who wish to be able to live free from prosecution because of the gender they love, the god they pray to (or don't believe in), as well as for women to freely have access to civic liberties (and have a space to defend them) such as the pursuit of independence in all its forms (economic freedom, political participation, professional choice, reproductive rights and sexual consent).

Over 2,500 years after the birth of democracy in Ancient Greece, and just a few hundred years after its resurgence at the end of the medieval times, we are transitioning into a 'digital democracy'. We are toddlers in this new period, learning how to walk in the digital spaces of an intangible territorial sovereignty, where the digital borders are blurry but play a role on the democratic infrastructure inside physical borders.

What does it mean if most of a nation's time is spent in digital spaces? Their mind and attention is in these digital spaces, while their physical bodies are in the territorial sovereignty of a nation's government. Digital spaces for work, love, shopping, hobbies, and religion can all be found online. Over the years, the platforms that facilitate these

exchanges reached across borders to become the glue for social and professional networking, they have provided access to business markets for a new wave of digital 'mom and pop' shops, and have documented our lives in ways that generations of royalty have never experienced.

These digital technologies, combined with the pervasiveness of corporate algorithms, have created a social and economic infrastructure that has increasingly taken power away from government as more citizens sign onto terms and conditions of the platforms they *digitally* inhabit. While this has taken away layers of bureaucracy in some aspects, it has brought more power to individuals to deliver their messages to broader audiences, sell their products to larger markets, learn new skills for free through many digital mediums, enjoy more forms of digital entertainment and connect with like-minded people across the world.

However, as the spaces we inhabit (with our attention) have shifted from physical to digital, we have entered the sovereignty of those digital spaces, and their respective algorithms, which have increasingly become the mediators of our lives. They suggest who to date, what job to apply to, what home appliance to buy and which political candidate to vote for.

In this sense, the algorithmic mediators of our lives have taken agency away from citizens, with several consequences, one being that the thoughts in our minds may not have necessarily come from there. It is unrealistic to argue that individuals should simply 'leave' these platforms. The costs of leaving are too high for those who rely on them for market viability and economic sustenance. Some say it is convenience, but these platforms are also a form of liberation (for revival of 'mom and pop shops' on Instagram and Etsy and Uber). They are also a form of entrapment when there aren't other platform options. Opting out can have financial, professional and social consequences. In this space, unelected leadership and corporate policies are the de facto form of civil law online.

How do liberal democracies around the world exercise their authority inside their physical territory, when the hearts and minds of their citizens residing in that same soil are living digital lives (for the most part of their day) under another leadership's terms and rules. If liberal democracies are meant to be "for the people, by the people", then the corporate jurisdictions in which we inhabit most of our digital lives are "for the corporation (and its shareholders), by the founders, mediated by a small group of engineers and defined by lawyers protecting corporate interests". None of these people are democratically accountable to the citizens of any nation because they have never been elected in democratic elections.

While citizens vote in elections to determine who will govern them in the physical space, unelected leaders govern the digital spaces we spend time in, and they are playing an important role in the new fabric of our digital governance. Does democracy exist in the digital world if no one elected those who govern it? Does democracy exist in the digital world if no one elected those who control the main platforms of our digital lives, or write the algorithms that play a role in our fate? What does that mean for the role of those who are democratically elected in the physical spaces we inhabit? What does it mean to have an "informed" civic debate in these circumstances? When democratic representation in the physical world does not apply to the digital world, the laws as they stand are not fit for purpose.

Digital Democracy: Old Problems on New Devices?

Terri Chapman
Non-Resident Fellow, Observer Research Foundation

There is widespread belief that the internet and social media strengthen individuals' voices and have a democratizing effect. This paper looks at four potential threats to liberal democracy in the context of digitization. First, the poser for this paper suggests that digital technologies and the pervasiveness of corporate algorithms have led to a shift in power away from states. Yet many states are leveraging digital tools to exert increasing control. Second, as large technology companies gain unprecedented market and political power, they are also becoming dominant conduits for the flow of information while having little to no responsibility for the content that they host. Third, the echo chambers resulting from platform structures are threatening to deepen social fissures, replicating and creating self-affirming communities shielded from opposing views. Finally, the algorithms increasingly used in public and private sector decision making are opaque, with little transparency of their inner workings or accountability for their outcomes.

A rising number of countries are exercising extreme control over the flow of information. This takes place through bans and the disruption of internet and website access, the denial of digital anonymity, restrictions on and the manipulation of content, or the spread of disinformation and propaganda. Ensuring a free and open internet is critical for realizing its democratizing and emancipatory benefits. In 2018, there were an estimated 196 internet shutdowns in 25 countries. This number is on the rise, from 75 in 2016 and 106 in 2017.[1] The official justifications for shutdowns in 2018 were overwhelmingly cited as safety, followed by national security, action against fake news and hate speech, and school exams.[2] The countries that used this measure most in 2018 include India, Pakistan, Yemen, Iraq and Ethiopia. India's shutdown of the internet in Kashmir in August 2019 was the 51st shutdown in the country this year.[3] Besides the significant social impacts of such internet blackouts, the economic impacts are estimated to have cost the economy 3 billion US Dollars between 2012 and 2017.[4]

In addition to access to the internet, anonymity online is critical for protecting individual freedom of expression and the right to privacy. Globally, states are implementing measures that weaken anonymity including bans on the use and dissemination of encryption technologies. Pakistan, for instance, implemented the *2016 Prevention of Electronic Crimes Act*, which prohibits the use of encryption tools that provide anonymity.[5] Some countries are introducing licensing and registration requirements. Examples include Vietnam, which in 2015 established the *Law on*

Network Information Security requiring companies trading in civil encryption goods to obtain special business licenses.[6] Similarly, Malawi introduced a registration requirement for companies providing encryption services, as well as a requirement of disclosing the technical details of the encryption technologies.[7] Further, several countries including the United States, the United Kingdom and Australia are attempting to weaken encryption tools through the creation of 'backdoors'. Several countries mandate the localization of personal data, and the local storage of encryption keys.[8] The debate around encryption and the dichotomy between privacy and security remain unresolved. Encryption policies must strike a balance between national security and individual freedoms.

Disinformation campaigns and content manipulation by state and non-state actors are increasing. State propaganda is often fabricated and disseminated using paid content contributors and bots.[9] 32 of the countries studied in the Freedom House 2018 report were found to have pro-government commentators manipulating online discussions[10] China is believed to have hired nearly 2 million 'pseudo-writers' to contribute deceptive content to social media sites. A recent study estimates that these authors fabricate and publish nearly 500 million comments a year.[11] Their main objective is to strategically distract social media users from contentious topics.[12]

Influence campaigns across borders by both state and non-state actors are threatening the legitimacy and trust in democratic systems. State-sanctioned influence campaigns include efforts such as defamation (delegitimizing public figures), public persuasion (trying to influence public opinion), and polarization (leveraging social and political divides, and undermining confidence in democratic institutions).[13] Recent research identified 53 foreign influence efforts (FIEs) in 24 target countries between 2013 and 2018.[14] More than half of the identified efforts were by Russia. The Russian online influence campaign during the American presidential election in 2016 is one example of this. Most of the remaining efforts were by China, Iran, and Saudi Arabia.[15] Popular social media platforms such as Facebook and Twitter have repeatedly been used in such efforts.

While technology equips states with new levers of control, technology companies such as Facebook, Google, Apple and Amazon are also gaining political and market power, and regulators are struggling to keep pace. Large technology companies have become prominent arbiters of the flow of information. Two thirds of Americans get at least part of their news from Facebook.[16] Technology companies have largely been able to eschew liability for the content that they host. The business models of big technology companies rely on targeted advertisements, which require the collection of unprecedented amounts of information about their users. This model favours content that spreads quickly, in many instances this is malicious, false and harmful content. According to a recent study of 126,000 news stories on Twitter posted between 2006 and 2017, it took true tweets six times as long to reach 1,500 people as false tweets.[17] The study found that human behaviour was the leading cause of the spread of false information.[18]

New policies aimed at holding platforms liable for the content on their sites are a step in the right direction. France's *Rapid Response Law*, which requires technology platforms to cooperate with law enforcement in the removal of false information. Germany's *Network Enforcement Law* mandates companies with 2 million or more users to remove content that is deemed to be against German law within 24 hours.[19] Moreover, the U.K.'s *Mandatory Duty of Care* legislation will hold firms accountable for hosting harmful content.[20] Fake-news legislation introduced in a number of

countries including Malaysia have been used to silence dissent. Care must be taken that new legislation is aimed at improving the flow of true information online, while protecting individual freedoms. Such efforts must also address the human behaviour aspects of the spread of misinformation online.

Individualized advertising and the network structure of social media risk creating echo chambers. Technology companies and social media platforms filter content that they believe a user does not want to see. Users are therefore exposed primarily to opinions that they agree with.[21] While this keeps users engaged on a site, it also poses the risk of polarization, particularly around political issues. Individuals are organizing around likeminded people online, shielded from opposing perspectives.[22] This contradicts the open discourse between different opinions which lies at the heart of democracy. It remains unknown, however, to what extent these echo chambers are replicating offline communities. If we want to break through these virtual echo chambers, we need greater awareness of how to engage with opposing viewpoints online.

It is believed that the internet has empowered individuals by creating more avenues for political participation and political voice. A critical part of political voice is being heard.[23] The complex network of links and search engine algorithms mean that online traffic coalesces around a few dominant sources, not unlike traditional media.[24] While people can write blogs to express their political views online, that does not mean that they are being read.[25] Importantly, not everyone has the needed skills to participate in online discussions, let alone shape democratic discourse.

The space for free speech online and offline is under threat everywhere by both the left and the right. Alarmingly, 61 percent of college students in the United States report that their campus climate prevents people from speaking freely. Further, 37 percent of respondents report thinking it is okay to shout down people with opposing views, and even more worryingly 10 percent of respondents report that using violence to do so is acceptable.[26] The tendency of the extreme left and right in the United States to prevent voices that they find offensive from being heard is counterproductive. In many instances, differing views are not only seen as wrong, but increasingly they are seen as 'evil'.[27] Open dialogue and debate is needed and a minimalist approach to regulating speech should be taken, with the exception of the incitement of violence.[28]

As individuals generate ever increasing amounts of data online, machine learning is enabling the processing of vast amounts of information. Algorithms are permeating new areas of our lives and are increasingly being used in decision-making processes. In the public sector, algorithms are used to make decisions such as tuition and financial aid, criminal justice, and public housing eligibility. In the private sector, examples of algorithmic decision-making include assessment of insurance and loan eligibility. The outcomes of such decisions have significant implications for individuals, organizations and communities.

Algorithmic decision-making is often favoured for its supposed objectivity, efficiency and reliability. Yet, the knowledge fed into these systems, the assumptions and values embedded in the data through collection, and the models risk replicating human bias.[29] Machine learning decision systems modelled on historic data also risk re-enforcing discriminatory biases.[30] Greater transparency and accountability are needed when it comes to the application of algorithms.[31] A pertinent example is the use of algorithm-based risk assessment tools in the United States criminal justice

system. COMPAS - Correctional Offender Management Profiling for Alternative Sanctions - has been used in assessing the risk of criminal recidivism and thus for determining eligibility for parole. Research shows that COMPAS correctly predicted the rate of recidivism just 61 percent of the time.[32] Researchers also found that COMPAS calculated a higher false positive rate of re-offence for black people. The opposite was true of whites, who were more likely to be labelled as low risk and then go on to commit another crime.[33]

The implications of algorithmic bias on individual lives and society are significant. The use of algorithms and machine learning are on the rise in the private and public sectors. This means that our lives, our opportunities, and risks are increasingly impacted by algorithms which the general population does not understand. Therefore, greater transparency and accountability for the bases of algorithmic decision-making is crucial. This will require greater explainability, validation and monitoring, legislative change, and increased public debate.[34] It might mean greater disclosure of human involvement in algorithmic design to expose inbuilt assumptions, as well as create more individual accountability. Transparency and monitoring of data would mean providing information on the accuracy, completeness, timeliness, representativeness, uncertainty and limitations of data used.[35] Finally, inferences drawn from the outcomes such as the margin of error, the rate of false positives and false negatives, and the confidence values can and should be disclosed.[36]

Democracy is not only about individual voice or decision-making by majority, it is just as much about the rule of law, representative democracy, limiting the power of individuals, and protection of minority rights. With that in mind, we must continue to assess the impacts of digital transformations on multiple aspects of democracy and democratic processes. This paper looked at four such challenges, including the exploitation of digital tools by states, the rising power of technology companies, the isolationist impacts of individualized social-media and news feeds, and the applications of algorithmic decision-making. Finally, we must consider the challenges that the digital domain presents for liberal democracy as both unique, and as extensions and replications of existing issues.

Endnotes

1 "The State of Internet Shutdowns." Access Now. July 209. https://www.accessnow.org/the-state-of-internet-shutdowns-in-2018/

2 Ibid

3 Ibid

4 Rajat Kathuria, Mansi Kedia, Gangesh Varma, Kaushambi Bagchi and Richa Sekhani. "The Anatomy of a Blackout: Measuring the Economic Impact of Internet Shutdowns in India." Indian Council for Research on International Economic Relations. 2018. 10. https://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf

5 "Encryption and Anonymity Follow-up Report. United Nations Human Rights Special Procedures. Research Paper 1. 2018. 5. https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

6 Ibid

7 Ibid

8 Ibid, 8.

9 Susan Morgan. "Fake news, Disinformation, Manipulation Tactics to Undermine Democracy. Journal of Cyber Policy 3 No. 1. 2018. https://www.tandfonline.com/doi/full/10.1080/23738871.2018.1462395

10 Freedom of the Net: The Rise of Digital Authoritarianism Report. Freedom House. 2018. 22.

11 Soroush Vosoughi, Deb Roy and Sinan Aral. " The Spread of True and False News Online." Science 359. March 2018. 3. DOI: 10.1126/science.aap9559

12 Gary King, Jennifer Pan, and Margaret E. Roberts. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument." Harvard University. April 2017.

13 Soroush Vosoughi, Deb Roy and Sinan Aral. " The Spread of True and False News Online." Science 359. March 2018. 3. DOI: 10.1126/science.aap9559

14 Diego A. Martin and Jacob N. Shapiro. "Trends in Online Foreign Influence Efforts. Princeton University. 2019. 3. https://scholar.princeton.edu/sites/default/files/jns/files/trends_in_foreign_influence_efforts_2019jul08_0.pdf

15 Ibid

16 Elisa Shearer and Jefrey Gottfried. "News Use Across Social Media Platforms 2017." Pew Research Centre. September 7, 2017. https://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/

17 Soroush Vosoughi, Deb Roy and Sinan Aral. "The Spread of True and False News Online." Science 359. March 2018. 3. DOI: 10.1126/science.aap9559

18 Ibid

19 Soraya Sarhaddi Nelson. "With Huge Fines, German Law Pushes Social Networks to Delete Abusive Posts." Morning Edition: National Public Radio. Oct 2017. https://www.npr.org/sections/parallels/2017/10/31/561024666/with-huge-fines-german-law-pushes-social-networks-to-delete-abusive-posts

20 Press Release. “UK to Introduce World First Online Safety Laws.” Department for Digital, Culture, Media & Sport, Home Office. April 9, 2018. https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws#targetText=This%20will%20include%20a%20mandatory,harmful%20activity%20on%20their%20services.&targetText=We%20have%20listened%20to%20campaigners,companies%20to%20keep%20people%20safe.

21 Kiran Garimella, Aristides Gionis, Gianmarco De Francisci Morales and Michael Mathioudakis. “Political Discourse on Social Media: Echo Chambers, Gatekeepers, and the price of Bipartisanship.” 2018. 913. 10.1145/3178876.3186139.

22 Nick Funnell. “ Bubble Trouble: How Internet Echo Chambers Disrupt Society.” The Economist. Year Unknown.http://shapingthefuture.economist.com/bubble-trouble-internet-echo-chambers-disrupt-society/

23 Mathew Hindman, The Myth of Digital Democracy. Princeton University Press. 2009. 13.

24 Ibid, 17.

25 Ibid, 16.

26 Jeffrey M. Jones “More U.S. College Students Say Campus Climate Deters Speech.” Gallup. March 2018. https://news.gallup.com/poll/229085/college-students-say-campus-climate-deters-speech.aspx

27 “The Global Gag on Free Speech is Tightening.” The Economist. August 17, 2019. https://www.economist.com/international/2019/08/17/the-global-gag-on-free-speech-is-tightening

28 “The Global Gag on Free Speech is Tightening.” The Economist. August 17, 2019. https://www.economist.com/international/2019/08/17/the-global-gag-on-free-speech-is-tightening

29 Reuben Binns. “Algorithmic Accountability and Public Reason.” Philosophy and Technology. 31, Issue 4. 2018. 546.

30 Ibid

31 Ansgar Koene et al., “A Governance Framework for Algorithmic Accountability and Transparency.” European Parliamentary Research. PE625.262. April, 2019. 1. http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf

32 Angwin J et al., “Machine bias: There’s Software Used Across the Country to Predict Future Criminals and it’s Biased Against Blacks.” ProPublica. May 23, 2016 https://www.ProPublica.org/article/machine-bias-riskassessments-in-criminal-sentencing accessed 12 September 2019.

33 Tom Douglas. “Biased Algorithms: Heres a More Radical Approach to Creating Fairness.” The Conversation. 2019.https://theconversation.com/biased-algorithms-heres-a-more-radical-approach-to-creating-fairness-109748

34 “Understanding Algorithmic Decision-Making: Opportunities and Challenges.” Panel for the Future of Science and Technology, European Parliamentary Research Service. March 2019. http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf

35 Nicholas Diakopoulos. “Accountability and Transparency in Algorithmic Decision Making.” Computations of the ACM. 59, No. 2 February 2016. 60. DOI:10.1145/2844110

36 Ibid

Don't Panic: Democracy and the Digital Transition

Mihir S Sharma
Senior Fellow and Head, Economy and Growth Programme, Observer Research Foundation

Does digital transition threaten democracy? Or does it deepen it?

In order to answer this question, it is necessary first to understand what it is that we are worried about. Few can claim that there is an existential threat to democracy itself; the concern is that the quality and nature of democratic deliberation and choice has been radically altered by the power of online debate and the ubiquity of online platforms.

The line between democracy and tyranny is thin. Majorities, even super-majorities, do not always choose wisely or well. This is why it has been more than two millennia since our first recorded experiments with democratic government: the form of democracy that has demonstrated longevity and strength is a diluted version. What we are now called on to defend is not democracy itself, but 'liberal democracy,' which constrains majority power, and representative democracy, which restricts voters' options.

In its most basic form, the digital revolution cannot but be "democratic" in the simplest sense of the world. The internet connects people. It reduces the cost of conveying information from one person to another. This means that we could theoretically replicate the Agora of ancient Athens on millions of smartphones daily. This is a seductive vision: somewhere within us all is the assumption that direct democracy is the first and purest form of the model. Digital technology takes us closer to this ideal of universal voice and constant accountability. It seems impossible that these things can be bad.

However, unmediated voice is unsuited to today's world. One merely has to look at the problematic recent consequences of direct democracy: the Brexit referendum, for example. The people can demand something through direct democracy that the complex modern world can simply fail to provide in any rational form. Representative democracy is in crisis in Britain today, thanks to the pull of direct democracy. This is in many ways analogous to the larger crisis that the digital age has forced on liberal institutions and deliberative dialogue.

Liberal institutions work only because they constrain the 'will of the people'. They say to voters: no, you cannot make that choice, because it infringes something we

consider basic to the functioning of society. Or they say, "no, you may want that now, but you did not in the past and you may not in the future, so you must be patient and prove you need it." Representative democracy works by muffling the voice of the people. You choose someone who understands your interests to sit in a room with other people and work out a deal, and then you live with the consequences — which may not be exactly what you want.

Digital technology renders both these tasks more difficult. It amplifies the voice of 'the people' and deafens it. It renders their will overpowering. When this change meets the structures of liberal democracy, the consequence is division; paralysis, stalemate. What happens when 'their people' feel their will is being frustrated? The same society that gave us the word 'democracy' also gave us the word 'demagogue'. The global rise of populists who claim to embody the will of the people today is not so hard to explain. It is an inevitable consequence of digitalised democracy. Most of them claim that through digital technology they can speak unfiltered, and express popular, subterranean views that elites have long sought to suppress. This claim depends, of course, on the conceit that the structure of the digital world does not by itself privilege certain kinds of speech, or certain majoritarian viewpoints.

It is, however, not obvious that this is necessarily a lasting trend. Since the earliest days of the internet, it has been understood that it introduces the 'many-to-many' form of information transmission, which may be mediated by social media or Wikipedia. This is distinct from 'one-to-one', like in a letter, or 'one-to-many', like in a newspaper. Sustained control of information transmission under these circumstances — crucial to the maintenance of autocratic power — is not easy. Nature abhors a vacuum, and the internet abhors consensus. In recent years, the fundamentally democratic nature of the digital transformation has been subverted to the service of majoritarian power. However, it is too soon to suppose that basic democratic character will not re-assert itself. The question of whether the digital world is democratic in its essential form must be answered separately from the question of whether it promotes democratic deliberation.

04.
Conflict

Future Conflict: The Nays Have it!

Sean Kanuck
Distinguished Fellow, Observer Research Foundation and Co-Chair of CyFy

CyFy 2019 will advance the global discussion on technology, security, and society through six pillars encompassing public policy, government regulation, virtual communities, reactionary regimes, democratic processes, and digital platforms. The notion of disruptive innovation will undoubtedly permeate each of those dialogues, and the reality of human conflict (military, political, economic, social, religious etc.) will inevitably contribute to re-defining the relationship between technology and society. This essay offers a framework for understanding the macroscopic trends that will shape the future of conflict and its manifestation through war and other means.

Four macro-trends are currently driving international affairs, and each is decidedly negative in nature: (1) **in**security, (2) **dis**information, (3) **anti**-globalization, and (4) **un**enlightenment. Those negative factors are not only mutually reinforcing with one another, but they are also all destabilizing at the systemic level. This framing essay coins the term "**indisantiun**" (a conjunction of the relevant prefixes "in-", "dis-", "anti-", and "un-") to collectively refer to those four first-order phenomena, the synergistic interplay among them, and the broader strategic implications of their confluence. *Indisantiun* is partially a by-product of disruptive information technologies and is fast becoming the defining characteristic of modern conflict.

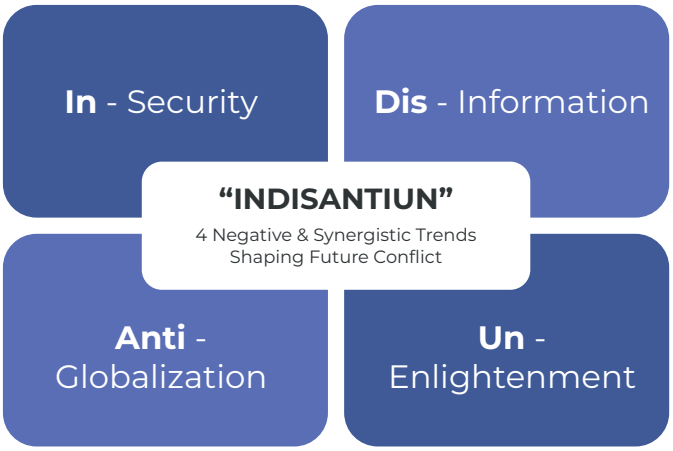

Figure 1 : Conceptual Bases of Future Conflict

In-Security

Both international conflicts and domestic strife are often engendered by politico-economic competition between ethnic and/or social interest groups within a society (including global "society" writ large). Technological development is having profound impacts on the labor force and the re-distribution of wealth, or more appropriately, the accretion of massive wealth in the hands of fewer and fewer individuals.[1] That redistribution of value is jeopardizing many individuals' sense of economic security and fueling populist movements, as illustrated by President Trump's political base in the United States and the "Brexit" supporters in the United Kingdom.

In the context of finite commodities (like gold or oil) and shared resources (like freshwater aquifers than span national boundaries), even the perception of zero-sum competition can lead to insecurity and efforts to preserve or expand one's own advantage. At the personal level, fear of unemployment due to automation or competitive pressure from immigrants in the workplace also breeds insecurity. As the world approaches the third decade of the 21st Century, information and communication technologies ("ICT") are transforming the global economy and displacing many long-standing parochial interests. In turn, insecurity is pervading the national political discourse in many countries.

This first contributing factor to indisantiun is equally apparent in military affairs, including at the tactical, operational, and strategic levels. First, the evolution of precision guided munitions and unmanned vehicles (e.g. aerial or maritime drones) are radically altering the experience of "combat" for aviators and sailors in advanced militaries while simultaneously increasing the risk of battlefield casualty for combatants from less developed nations.[2] Second, the introduction of artificial intelligence ("AI") and lethal autonomous weapons systems ("LAWS") mandates the reconsideration of operational doctrines and procurement policies because large, expensive military platforms that aggregate immense value within a limited physical area are increasingly becoming vulnerabilities rather than assets.[3] Third, the potential threat of cyber-attacks to nuclear command and control ("C2") systems is creating a source of strategic instability.

At all three levels, insecurity driven by new technologies will define the future of war. Moreover, cyber operations and other measures are increasingly being used by adversaries to hold each other's critical infrastructures at risk in order to coerce or to exact concessions.[4] This is a highly disturbing trend because many of those targets in the financial, media, transportation, and health sectors are civilian in nature. That shift in focus from attacking an adversary's military to undermining its civilian infrastructures is a serious and radical departure from 20th Century legal and diplomatic efforts – as embodied in the Geneva Conventions – to insulate civilians from the dangers of international armed conflicts. At CyFy 2017, I suggested that future conflicts would become safer for soldiers and more dangerous for civilians, and that trend is indeed proving to define modern conflict and spread insecurity across populations.[5]

Dis-Information

The second element of indisantiun – disinformation – has gained wide public notoriety through Russian-sponsored interference in recent Western elections, such as the 2016 US presidential election, the 2017 French presidential election, the 2016 Brexit referendum, and the 2017 Catalan secession debate.[6] However, similar methods are being utilized by many state and non-state actors to protect regime stability, disparage political opponents, and challenge the legitimacy of foreign government institutions to gain advantages on the world stage. Disinformation offers belligerents the opportunity to coerce and destabilize their adversaries without crossing the legal line of kinetic armed conflict. In fact, the strategic doctrine of multiple countries now identifies hybrid warfare methodologies as important components of military operations (e.g. the "Gerasimov doctrine" from Russia).[7]

Just as with insecurity, disinformation can have tactical, operational, and strategic applications. It could be employed to influence specific voters or investors, to alter the situational awareness of military commanders, or to undermine the very legitimacy of a political regime or form of government. AI will further empower offensive activities over defensive activities in the near term (i.e. the next 3 to 5 years) because automated algorithms will be able to generate and disseminate falsified information at a much faster rate than humans or competing algorithms will be able to detect, assess, and countermand such disinformation. The most difficult cases will involve falsified components that are included within otherwise accurate documents or accounts. Furthermore, public officials of limited credibility who are confronted with the release of compromising private information will likely not be successful in confessing that certain aspects of the leaked data may indeed be true but that some of the more egregious aspects are disinformation nefariously fabricated and included by their opponents.

The emergent threat of deep fakes (i.e. falsified documents, digital pictures, audio files, or videos) that are essentially indistinguishable from true productions – and therefore highly impactful on unsuspecting audiences – profoundly challenges the notion of objective reality.[8] The world will soon be without definitive sources of uncontestable evidence or "proof" of what is true.[9] Without recourse to a collective reality or definitive truth, future conflicts – whether international confrontations or domestic unrest – are likely to be much easier to instigate and much more difficult to dissipate.

Disinformation both stems from and reinforces other elements of indisantiun. Insecurity induces actors to employ disinformation against their competitors, and polarizing content only exacerbates anti-globalist tendencies – usually in both the perpetrator and target of such influence campaigns. The absence of agreed-upon epistemological principles or common evidentiary processes for establishing factual reality and objective truth is the antithesis of Enlightenment ideology. Postmodernist and relativist tendencies may also permit individuals' experiences or biases to drive their perceptions, thereby creating uncertainty. In turn, anti-globalism and unenlightenment complete a recursive cycle by making populations even more susceptible to disinformation and feelings of insecurity.

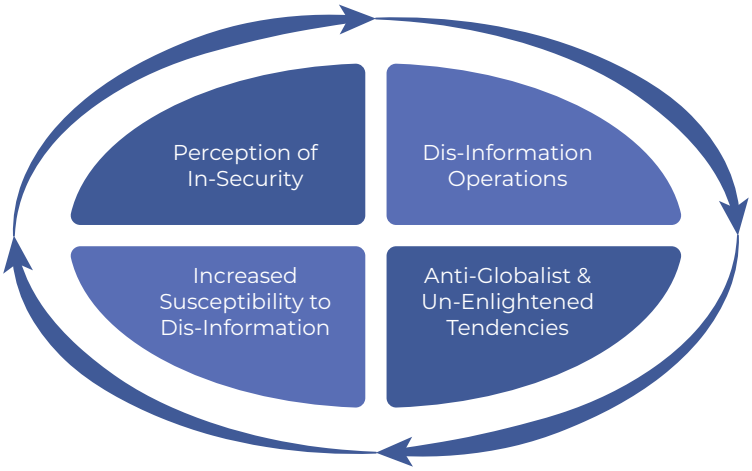

Figure 2 : Negative Feedback Cycle of Mutually Reinforcing Factors

Anti-Globalization

Insecurity fosters xenophobia, nationalism, and even radicalization. Moderate examples of such inclinations can be observed among the electorates that supported President Trump's campaign and the Brexit referendum. In both of those cases, politicians converted public fears of zero-sum competition into populist movements favoring national advantage over global integration. The most egregious examples of anti-globalization include increased tariffs between China and the United States, violent protests against international trade agreements, recent support for ultra-right-wing political parties in Europe, periodic skirmishes on the India-Pakistan border, and even terrorist acts by certain Islamic extremists.[10]

Under the indisantiun conceptual framework, future conflicts become more societal than military in nature. Sovereigns compete with information in addition to weapons. Moreover, they strive to directly impact their adversary's populace without necessarily engaging that country's military forces.[11] In essence, it becomes an indirect intervention whereby one state leverages another state's constituents to challenge their own government and necessitate the target state's public officials and institutions to focus inwardly at the expense of contesting foreign adversaries on the world stage. Social media platforms have already been exploited by foreign influence campaigns designed to distract and/or destabilize target countries. They have also been exploited to spread disinformation aimed at fomenting sectarian violence within societies.[12]

In the political and social context, anti-globalization is often accompanied by intolerance, censorship, and disinformation. Disinformation is the modus operandi that enables a government to delegitimize its opponents and degrade their situational awareness, thereby reducing their capacity to supplant the existing regime. Whether at the international or domestic level, disinformation is utilized to reinforce rifts between social groups, discourage mutual understanding, and thwart political compromise.

In the technology sector, anti-globalization manifests itself in a competitive arms race that prevents robust information sharing and joint research and development ("R&D") initiatives that could be economically beneficial. We currently see such competitive – rather than cooperative – R&D in the areas of cyber security and AI.[13] Other examples of technology-based anti-globalization are: data localization regimes, efforts at the extraterritorial application of content restrictions, and segregated national "intranets" that can be disconnected from the global Internet.[14] Unfortunately, advancements in ICT are both a causal factor and an implementing methodology for indisantiun.

Anti-globalization is the center point of a negative reinforcement cycle whereby disinformation is used to simultaneously destabilize competitors and insulate one's own adherents from external voices. However, the paradoxical result is that the censorship and disinformation that are bred by insecurity make one even more susceptible to manipulation and coercion by both truth and foreign disinformation … which in turn breeds even greater insecurity. Indisantiun is a conjunction of self-realizing and compounding phenomena.

Un-Enlightenment

The three negative and synergistic trends that have already been identified above operate in opposition to nearly three hundred years of Enlightenment learning that favors rational thought, objectivity, and tolerance. Taken collectively, the fear of insecurity, the creation and dissemination of false information, and anti-globalist policies relegate individuals, communities, and societies to parochial relativism. Indisantiun rejects the existence of common interests and undermines the desire for common understanding. Without those commonalities, there can be no shared human experience.

At a recent Stanford University event, Herb Lin described unenlightenment as the lack of a shared rationality.[15] Enlightenment values include: acceptance of alternative cultures and religions, recognition of empirical evidence and a scientific method for evaluating propositions, and a reliance on reason (vice mysticism or dictatorial fiat) as a governing principle for human endeavor. Future conflicts will stem from entities that not only disagree with one another, but which also do not even see the value in seeking any agreement. ICTs now permit people to interact almost exclusively with like-minded persons who share the same insecurities and subscribe to the same disinformation (e.g. fake news).

Paradoxically, some of the most militarily aggressive empires in history espoused pragmatic tolerance regarding selected issues, even while they engaged in oppressive colonialism and slavery. The Roman, Mongol, and British empires all permitted certain cultural and religious freedoms, provided that their subjects gave unwavering political and economic fealty. Conquest afforded these administrative systems expanding resources, so the insecurity attendant to zero-sum competition was not determinative.

However, such tolerance withers when heightened competition between and within societies manifests itself. Rather than the universal rights and entitlements that the Enlightenment ascribed equally to all human beings, indisantiun ignores absolute truths and preoccupies itself with obtaining relative advantages and entitlements. Insecurity, disinformation, and anti-globalization all pierce the Rawlsian "veil of ignorance" that demands rational thought unfettered by personal circumstance.

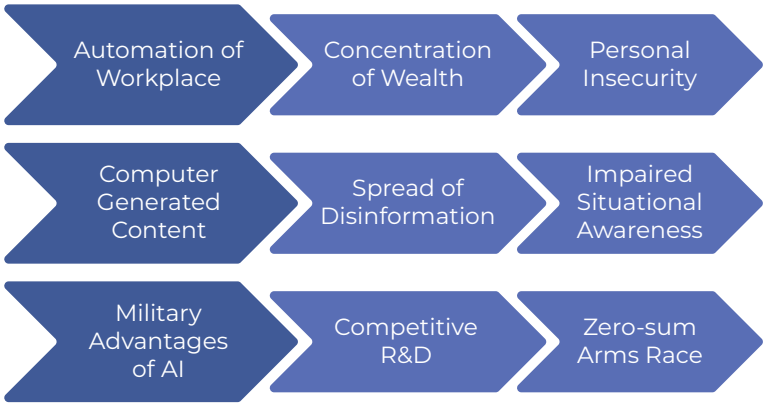

Figure 3 : Destabilizing Implications of Technological Advances

It is highly ironic that ICTs are effectively used to divide interest groups instead of encouraging engagement and mutual understanding. Furthermore, it is ironic that ICTs and AI are now being utilized to delegitimize evidentiary standards and established processes of rational inquiry. Without the ability to reach factual consensus, conflicts – and escalation of those conflicts – are more likely. Finally, perhaps most disturbing is the increasing adoption of indisantiun beliefs, policies, and strategies by liberal, democratic societies. What will be the result if adherence to Enlightenment values is not deemed to be a viable strategy in today's competitive geo-political environment? Do technological development and the historical dialectic favor liberalism or authoritarianism?

Conclusion

This framing essay posits that the future may experience more conflict, but of a qualitatively different nature. So, where would a teleology of indisantiun lead? Future conflict would be passive aggressive. Reliance on innovative (and uncertain) technology would be the primary catalyst of that conflict as well as its primary resultant. Adversaries would indirectly exploit civilians to harm themselves and their polities. Local advantage and personal entitlement would be paramount motivators. Truth and tolerance would become casualties of future conflicts, but those Enlightenment ideals would no longer be held in such esteem by the vast majority.

In order to prove the "naysayers" of insecurity, disinformation, anti-globalization, and unenlightenment wrong, the world community must recognize the implications of ICT for political economy. Second, analysts must examine the evolution of strategic incentives and conflict dynamics to identify opportunities to exit the recursive cycle of indisantiun.

Hopefully, CyFy 2019 will provide a vibrant forum to explore these topics in a collective environment that reflects a broad array of backgrounds, interests, and perspectives. It should come as no surprise that the motivation for preparing this essay for the CyFy journal Digital Debates is specifically to counter unenlightenment, anti-globalist tendencies, and the deleterious practice of disinformation. Common understanding is vital to alleviating insecurity and reducing conflict.

Endnotes

1 See e.g., "Outrageous fortune"; The Economist; 5 October 2019, page 82 (citing a University of California, Berkeley study that found 0.1 percent of taxpayers in the United States accounted for approximately 20 percent of America's wealth in 2012).

2 See generally, Amy Zegart, "Cheap flights, credible threats: The future of armed drones and coercion"; Journal of Strategic Studies; 28 February 2018.

3 Massed infantry has for some time been regarded as a liability vis-à-vis artillery or aerial bombardment, but in the face of hundreds or thousands of "swarming" drones even warships and other major combat platforms could soon become indefensible targets. For example, this very subject was discussed aboard the Royal Navy's new aircraft carrier HMS Queen Elizabeth during the Atlantic Future Forum in New York City harbor on 22 October 2018.

4 The December 2015 and 2016 cyber-attacks against Ukraine's energy grid can certainly be viewed as such actions. See e.g., Andy Greenberg, "New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction"; Wired; 12 September 2019; available at https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.

5 Sean Kanuck; panel presentation entitled "The Big Questions: Technology, Security and Society" at CyFy 2017; Observer Research Foundation; available at https://www.youtube.com/watch?v=vYNVuMDOw0E.

6 See e.g., Grand Jury indictment in the United States District Court for the District of Columbia (Case 1:18-cr-00215-ABJ); United States Department of Justice; 13 July 2018; available at https://www.justice.gov/file/1080281/download.

7 See, Molly K. McKew, "The Gerasimov Doctrine"; Politico Magazine; 5 September 2017; available at https://www.politico.com/magazine/story/2017/09/05/gerasi mov-doctrine-russia-foreign-policy-215538. The United Kingdom and United States Army are also advancing new military doctrines for "cyber electro-magnetic activities (CEMA)" that include information operations, while China has collocated a range of hybrid warfare assets within its new Strategic Support Force.

8 For example, the fate of Malaysian Airlines flight 17 is represented very differently in the European versus Russian press. Examples of the conflicting media accounts are available at https://www.independent.co.uk/news/world/europe/flight-mh17-latest-russia-missile-malaysia-airlines-netherlands-australia-ukraine-a8368566.html and https://www.youtube.com/watch?v=6YwxhDhPB_w.

9 What constitutes definitive evidence has varied over time and between cultures. Europe's ecclesiastical inquisitors once sought a personal confession from the accused as proof of guilt, and some Islamic tribunals required the oral testimony of three adult males to establish proof. Now, we are in an era where even a photograph – or other technical information – may not constitute incontrovertible evidence.

10 Even the European Union – which allegedly prides itself on democratic traditions and the protection of human rights – has recently seen Danish and French laws prohibiting certain traditional Islamic clothing in order to preserve nationalist cultures.

11 Supra note 7.

12 See e.g., Devidutta Tripathy & Annie Banerji, "India cracks down on Internet after communal violence"; Reuters; 21 August 2012; available at https://www.reuters.com/article/net-us-india-violence-internet-idUSBRE87K0NM20120821.

13 See e.g., "New Generation Artificial Intelligence Development Plan" released by the State Council of the People's Republic of China on 20 July 2017; full translation by New America, 1 August 2017; available at https://www.newamerica.org/cybersecurity-initiative/digichina/blog/fulltranslation-chinas-new-generation-artificial-intelligence-development-plan2017/.

14 See generally, Jeff John Roberts, "The Splinternet Is Growing"; Fortune; 29 May 2019; available at https://fortune.com/2019/05/29/splinternet-online-censorship/.

15 Herb Lin, presentation entitled "Cyber Enabled Information Warfare and Influence Operations", Cyber and Artificial Intelligence Boot Camp; Stanford University; 27 August 2019.

Technology, Change, and the Inevitability of Conflict

Philip Reiner
Chief Executive Officer of Tech4GS

Introduction

Technology shifts play a crucial role in a number of negative trends that paint a bleak outlook for the future: a disastrous climate crisis,[1] horrifying physical[2] and cultural[3] genocidal campaigns, apocalyptic civil wars,[4] unchecked invasions of sovereign states,[5] and a resurgence of nationalist and authoritarian revanchism, all of which are compounded by - as Sean Kanuck insightfully writes in his piece in this volume - increasing global insecurity, disinformation, anti-globalization, and "un-enlightenment" trends.[6] There are, however, numerous significant positive trends worth noting at the same time: decreasing infant mortality rates,[7] declining global poverty rates,[8] and an expanding global middle class.[9] While the "great power peace" may be fading,[10] great power war continues in abeyance for the longest period in modern history.[11] Like Kanuck's trends, technology also helps drive these developments.

While the breadth of societal change borne of technological innovation is vast, when considering the face of conflict in the 21st century and its symbiotic relationship with technology, what can and must be asserted is that states have always and will continue to compete. This harsh, but undeniable reality, dates back to well before the modern nation state system was established via the Treaty of Westphalia (the "Peace of Westphalia") in the 17th century; "the strong do what they can and the weak suffer what they must" is a frequently-cited quote from the 5th century B.C. Athenian historian and general Thucydides[12]. The current historical moment is no different: global powers are vying for primacy, regionally and on the international stage. Within this context, technology simply continues to serve as part of that competition, as a means to an end. While these may serve to accelerate or accentuate varying levels of conflict - enhancing various forms of violence or creating distance from others - these are not what will drive or characterize conflict in the 21st century alone.

Current technological trends are creating novel tactical options; these can be bewildering at times. On this subject, Mr. Kanuck's analysis is insightful and accurate: the character of conflict is taking on new dimensions – it is faster, elusive, and at times, disruptive and even lethal. However, these are not game changing trends, at least not just from the specific categories that Mr. Kanuck chooses to focus. It is unlikely that, even if the recursive cycle he lays out is perpetrated for some time to

come, three of his four categories will change the real character of conflict, or lead to, much less characterise, large scale combat: insecurity has and always will persist; the 'disinfo'-infused gray zone conflict he begins to describe is actually vastly more complicated[13] and not entirely tied to technological change; and Enlightenment principles are arguably not pre-requisites for a more peaceful world. Of the four, the geopolitical anti-globalist trends he notes are the most ripe for bringing about a broader impact.

This paper will provide more detailed reasoning below for all these statements. First, however, it must be noted quite simply that evil is real and cannot be vanquished. History continues. The dimensions of conflict will have new faces, but at its core, conflict and competition will remain, and it will be brutal, violent, and occur on scales much larger than simply disinformation and disequilibrium. Just ask the citizens of Raqqa, Mosul, or Pervomaisk, in Luhansk Oblast, Ukraine, or even those short of an open, large-scale great power conflict.

There are technological innovations that will fundamentally alter the character of, and perhaps serve as the direct cause of, significant levels of conflict in the coming years. The hyper-speed of information access and processing on the battlefield, the contest for the electromagnetic spectrum that accompanies that trend, the ability to accurately anticipate adversary moves through automated means, and the introduction of "intelligentized" decision support systems, all point to a near-term future in which select nations with the necessary resources - the United States, China, Russia, and a small handful of others - will increasingly maintain step-order level advantages in capability. They will have the ability to put soldiers and droves of killing machines where they need to be, when they need to be, with the right resources securely in place to facilitate kinetic operations. As U.S. Lieutenant General Eric Wesley argues, "This isn't about adopting AI and commercial practices - suitably modified for the military - for the sake of mere efficiency…it's about new ways of winning wars"[14] that may not be a "Skynet" style solution, or even where humans are removed from "the loop."

Taking matters further, technological change is converging in other unintended ways that will increasingly undermine the assumptions that underwrite both the conventional and nuclear deterrence that global leaders have relied on for years, dramatically increasing both strategic and crisis instability.[15] Nuclear-conventional entanglement,[16] domination of the electromagnetic spectrum17, the "accuracy revolution",[18] and initiatives like "mosaic warfare",[19] will continue to undermine common conceptions of the character of conflict. Finally, the ever-increasingly lethal cyber element of warfare will continue to force nations to recalibrate their approaches to global conflict. In this final regard, this author is in violent agreement with Mr. Kanuck. The conflict in Ukraine offers a window into the confluence of these elements, along with those alluded to in part by Mr. Kanuck. Openly violent, characterized by cyber combat as well as the shelling of cities, many have lost their lives not only via the bullet, but by first having been identified through social engineering, targeted by digital methods, then eliminated through conventional means.[20] These are the elements of conflict that, as they change and evolve to incorporate emerging technologies, will most surely contribute to regional and global instability.

Insecurity

Returning to the four elements of Mr. Kanuck's "indisantiun" conceptualization: first, insecurity always has and always will persist, in vary degrees of flux - history continues to prove that states ignore this fact at their peril. Global insecurity is a constant. Mr. Kanuck is accurate in that technology is lending towards increased insecurity in particular domains; this is not, however, historically unique, and in this author's opinion, has not led to a greater global sense of insecurity: that sense has remained palpable well before these current technological trends. More important to recall is that states continue to vie for advantages out of a recognition that other nations simply cannot be entirely trusted. Technology is not the reason behind that reality. This example is illustrative: In January 2019, Subrahmanyam Jaishankar -- now India's Minister of External Affairs -- responded to a question from General David Petraeus as to whether India would "pick sides" by stating that India "should take a stand, and we should choose a side, and that's our side."[21]

Mr. Kanuck notes that the increasingly unequal distribution of wealth due to technological innovation can be potentially destabilizing - this was one of the causes that gave rise to Marxism and arguably, the wars of the 20th century. Are current national levels of insecurity being driven predominantly by technologically driven economic changes? This is up for debate, and much remains to be seen regarding the broader impact of AI and workforce displacement. These factors could end up pointing toward internally destabilizing trends and thus an increased risk of state on state conflict; however, this is too early to conclude. The tide could still shift, and there are an interesting set of issues for debate at CyFy 2019. The idea that populations are at greater risk today than in years past is also debatable; threats to civilians have persisted, but civilian casualties in combat have generally declined over the years. As Mr. Kanuck notes, cyber threats to infrastructure, banking, etc., present new challenges that governments must address. Herb Lin notes that "what is known from history and experience – that is, the metaphors, analogies and precedents with which policymakers are familiar – may break down when applied to the cyber domain."[22] Populations, however, have been and remain insecure.

Disinformation

"Hybrid warfare" is not new. Irregular warfare has been a part of military toolkits since time immemorial. Disinformation is a long-standing tool deployed by a variety of actors to achieve their aims. Its resurgence may be on the rise due to new technologies and the spread of social media, but purposeful delusion has always been a character of conflict.[23] It does appear that America, and Europe to a lesser degree, were late to grasp those realities following the end of the Cold War: "the optimism of U.S. policy has outpaced the reality of other countries' own ambitions to create their own realities."[24] The United States and the Soviet Union engaged in broad, large scale disinformation campaigns that would shock today's publics if they were implemented today. Herb Lin has also said that "infowarfare takes advantage of vulnerabilities in cognition."[25] This isn't new. The "truth" has, to an extent, always been manufactured for public consumption. Today's trends are simply the result of nation states finding new levers to pull for their own gain: As Bradbury et al argue, "These are the conventional tools of demagogues throughout history, but this agitprop is now packaged in ways perfectly suited to the new environment."[26] Information warfare has always been part of conflict, shaping public opinion of the adversary's populace a key objective. The full breadth of what technology-driven disinformation

means for conflict in the 21st century is yet to be seen. Disinformation indeed has the potential to breed violence, as does social media even when it is simply serving its intended role: connecting people who otherwise would never know each other.

Anti-Globalization

Again, insecurity is perpetual, as is xenophobia, nationalism, and radicalization. One could argue that increased populism and anti-globalization trends in the European context are not driven by internal economic trends (which were already well underway), but in large part due to the climate crisis: droughts and devastatingly low crop yields led in part to the revolts that characterized the Arab Spring, and the Syrian civil war in particular.[27] Those in turn led to massive emigration and resettlement waves that caused European citizens to push back on their governments policies. The same could be said in the context of developments in Central American countries. Globalization was also bound to face backlash due to the cyclical nature of markets as well as powerful countries overplaying their hand. This is also in keeping with states preserving or increasing their distinct power. Global economic de-coupling, as Mr. Kanuck describes and as this author concurs, may create space/allow for greater levels of conflict in coming years. The European experiment may unravel due to Brexit, but I disagree that future conflicts will become more societal than military in nature. "War is the continuation of politics by other means"[28] remains an apt adage even in the digital information age. Finally, there is no indication that current anti-globalization trends will continue. Technological innovation in its current form inherently relies on global supply chains -- a fact that will continue to sway political decision making towards globalization, not away from it (for an example, see waivers provided to Apple in the Huawei instance).

Un-Enlightenment

As Henry Kissinger argues, "the age of Enlightenment gave us reason and reality as the foundations of political discourse, but information warfare in cyberspace could replace reason and reality with rage and fantasy.[29] This is an arrogant and hyperbolic view of history, as well as a mischaracterization of the challenges posed by both AI and cyber. Herb Lin has a logical argument to make, but if, for example, armed conflict occurs between the U.S. and China, it will not be a result of a global disavowment of Western "reason" and "rationality." National leaders have warped, flaunted, and obliterated these values repeatedly since the Age of the Enlightenment, to catastrophic effect. Additionally, the characteristics and goals of Enlightenment thought are entirely Western constructs, to which large portions of the global populace do not, and have never ascribed. Thus, there is little evidence that a lack of Western rational thought lends one more towards conflict and away from cooperation. In addition, modern democracy itself is still working through its own inherent challenges to be accurately considered the organizing, victorious force it was deemed at the end of the Cold War.[30]

Conclusion

The nature of war itself can be called into question in the face of "disruptive" technology,[31] as can specific temporal causes of conflict, war's actual conduct and termination. The fact of the matter remains: conflict is an intrinsic element of international relations. A powerful consideration, however, is not how technology

changes the predilection of states to desire and/or to hoard power, but rather the possibility that there is no historical moment where the rise of a new global power did not result in great power conflict and large scale violence. All of the current talk of "gray zone conflict" and "under the threshold of actual conflict" aside, historically speaking, great power competition inevitably leads to great power war, particularly when a hegemon feels its grip on power loosening. How could our current epoch end any differently? Will technology accelerate oncoming great power competition, as Mr. Kanuck's paper implicitly asserts, or does technological change hold promise a more peaceful potential outcome? The undeniable hegemon, the United States, has provided significant global public goods both since the end of World War II in 1945 and the end of the Cold War in 1989. However, that hegemonic status also, naturally, has drawn significant ire, and competition, on the international stage. What Mr. Kanuck argues is partially accurate: the trends he identifies help characterize some of the impacts of 21st century technologies and can perhaps help anticipate elements of future conflict. His analysis, however, also misses the forest for the trees, not to mention the broader catalyst for continuing global insecurity.

The former two-time U.S. National Security Advisor Lieutenant General Brent Scowcroft came from a particular school of thought, honed through decades of international crisis management experience. This viewpoint saw the world for what it is: respecting raw power as well as what was required in order to manage relationships necessary to maintain a common path forward. He understood, and respected - even earnestly sought after - the power and influence of multilateralism, but he also understood the need for raw power to maintain the ability for a nation state to meet its national security requirements. India's Minister of External Affairs, Subramanyam Jaishankar's view on this is shown via this statement: "more multipolarity...less multilateralism...you keep relationships well-oiled with all major power centers. The country that does that best has a political position in the world which may be superior to its structural strengths." However, this is wishful thinking: Chinese military capacity will not be awed by said political connectivity.

General Scowcroft accepted that not all nations will see eye to eye, and this will remain a perennial truth. Technological advantage was part o f the calculus, but only as means to the desired ends. Conflict will occur, but potentially stabilizing influences from technology will occur as well. The lack of understanding of an adversary's capabilities in the cyber domain, for example, or the implications of the "accuracy revolution" for nuclear deterrence, may demand greater levels of prudence in military decision making, to include with nuclear weapons. What Scowcroft would emphasize, however, is that technology will be deployed through the means necessary for states to ensure their own objectives are met. It is therefore not surprising that the internet is used for purposes other than originally intentioned; what is more difficult to grapple with is how nefarious technological applications are outpacing social policies.

The opportunity remains to think about how technological evolutions may present opportunities for nations to create constructive transparency, facilitate new norms of behavior, and balance access to resources that keeps those nations endowed with significant resources from punishing those without. History says this will be difficult. The better we understand the risks and threats, the better positioned we will be to chart a different course.

Endnotes

1 Intergovernmental Panel on Climate Change (IPCC). "Special Report on the Ocean and Cryosphere in a Changing Climate." Accessed on September 25, 2019 at: https://www.ipcc.ch/srocc/home/

2 United Nations Human Rights Council, "Myanmar's Rohingya Persecuted, Living under Threat of Genocide, UN Experts Say", report available on the Independent International Fact-Finding Mission on Myanmar website. Accessed on September 25, 2019 at: https://www.ohchr.org/en/hrbodies/hrc/myanmarffm/pages/index.aspx

3 Cronin-Furman, Kate. "China Has Chosen Cultural Genocide in Xinjiang—For Now." Foreign Policy, September 19, 2019. Accessed on September 28, 2019 at: https://foreignpolicy.com/2018/09/19/china-has-chosen-cultural-genocide-in-xinjiang-for-now/

4 Civil War in Syria. Council on Foreign Relations, Global Conflict Tracker. Accessed on September 25, 2019 at: https://www.cfr.org/interactive/global-conflict-tracker/conflict/civil-war-syria

5 Conflict in Ukraine. Council on Foreign Relations, Global Conflict Tracker. Accessed on September 25, 2019 at: https://www.cfr.org/interactive/global-conflict-tracker/conflict/conflict-ukraine

6 Kanuk, Sean. "Future Conflict: The Nays Have It!". Copyright 2019 by Sean Kanuck, all rights reserved.

7 United Nations Department of Economic and Social Affairs. "Levels and Trends in Child Mortality Report 2018." Accessed on September 25, 2019 at: https://www.un.org/en/development/desa/population/publications/mortality/child-mortality-report-2018.asp

8 The World Bank. "Decline of Global Extreme Poverty Continues but Has Slowed: World Bank." September 19, 2018. Accessed on September 25, 2019 at: https://www.worldbank.org/en/news/press-release/2018/09/19/decline-of-global-extreme-poverty-continues-but-has-slowed-world-bank

9 Kharas, Homi and Hamel, Kristofer. "A global tipping point: Half the world is now middle class or wealthier." Brookings Institution, Future Development series. Accessed on September 25, 2019 at: https://www.brookings.edu/blog/future-development/2018/09/27/a-global-tipping-point-half-the-world-is-now-middle-class-or-wealthier/

10 Brands, Hal and Edel, Charles. "The End of Great Power Peace", The National Interest, March 6, 2019. Accessed on September 25, 2019 at: https://nationalinterest.org/feature/end-great-power-peace-46282

11 Backer, David A., Bhavnani, Ravi, and Huth, Paul K., eds. Peace and Conflict 2016. Center for International Development and Conflict Management, University of Maryland. Accessed on September 25, 2019 at: https://cidcm.umd.edu/research/peace-and-conflict.

12 Thucydides. The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War. Strassler, Robert B., ed. New York: Simon & Schuster, 1998. Print.

13 Dalton, Melissa, Hicks, Kathleen, et al. "Gray Zone Project", Center for Strategic and International Studies. Accessed on September 25, 2019, at: https://www.csis.org/grayzone. "From fake news and online troll farms to terrorist financing and paramilitary provocations, these approaches often lie in the contested arena somewhere between routine statecraft and open warfare—the "gray zone."

14 Freedberg, Sydney. "Forget The Terminator For Future Army AI: LTG Wesley ", Breaking Defense, Networks & Cyber. Accessed on September 26, 2019 at: https://breakingdefense.com/2018/11/artificial-intelligence-key-to-commanding-future-army-ltg-wesley/. "The ability to decide — (to) synthesize the volume of information that will be available to us (to) make decisions — is the biggest problem we have."

15 See Long, Austin and Green, Brendan Rittenhouse, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy", Journal of Strategic Studies Vol. 38, Nos 1-2 (December 2014), pp. 38-73; Lieber, Keir A. and Press, Daryl G., "The End of MAD? The Nuclear Dimension of U.S. Primacy," International Security Vol. 30, No. 4 (Spring 2006); Kristensen, Hans M., McKinzie, Matthew, and Postol, Theodore, "How U.S. nuclear force modernization is undermining strategic stability: The burst-height compensating super-fuze," Bulletin of Atomic Scientists, March 1, 2017.

16 Acton, James. "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War." International Security. Volume 43 | Issue 1 | Summer 2018 p. 56-99. Accessed on September 25, 2019 at: https://www.mitpressjournals.org/doi/full/10.1162/isec_a_00320

17 Clark, Brian, et al. "Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance." Center for Strategic and Budgetary Assessments, October 5, 2017. Accessed on September 28, 2019 at: https://csbaonline.org/research/publications/winning-in-the-gray-zone-using-electromagnetic-warfare-to-regain-escalation

18 Lieber, Keir A. and Press, Daryl G., "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," International Security Vol. 41, No. 4 (Spring 2017). Also, Press, Daryl G. "NC3 and Crisis Instability: Growing Dangers in the 21st Century." Forthcoming publication via Technology for Global Security at www.tech4gs.org, October 2019.

19 Defense Advanced Research Projects Agency (DARPA). "DARPA Tiles Together a Vision of Mosaic Warfare: Banking on cost-effective complexity to overwhelm adversaries." Accessed on September 28, 2019, at: https://www.darpa.mil/work-with-us/darpa-tiles-together-a-vision-of-mosiac-warfare. More information found here: https://www.google.com/

20 Brantly, Aaron, and Collins, Liam (Colonel). A Bear of a Problem: Russian Special Forces Perfecting Their Cyber Capabilities." Association of the United States Army, November 28, 2018. Accessed on September 28, 2019, at: https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare; Collins, Liam (Colonel). "Russia Gives Lessons in Electronic Warfare." Association of the United States Army. Accessed on September 28, 2019, at: https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare. Also, Brown, Daniel. "Russian-backed separatists are using terrifying text messages to shock adversaries — and it's changing the face of warfare." Business Insider, August 14, 2018. Accessed on September 28, 2019, at: https://www.businessinsider.com/russians-use-creepy-text-messages-scare-ukrainians-changing-warfare-2018-8

21 S. Jaishankar quote taken directly from 2019 Raisina Dialogue panel conversation with General Petraeaus. Paraphrased summary found in "A World Reorder," ORF Raisina Dialogue Conference Report 2019, accessed on September 29, 2019 at: https://www.google.com/

22 Lin, Herb and Kerr, Jackie. "Cyber-Enabled Information Warfare and the End of the Enlightenment." Stanford University Center for International Security and Cooperation Seminar. Accessible on September 25, 2019 at: https://cisac.fsi.stanford.edu/events/cyber-enabled-information-warfare-and-end-enlightenment. Their older paper on the topic was accessible on September 25, 2019 at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680

23 Rid, Thomas. Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux (Forthcoming, April 21, 2020).

24 Hamre, John. Foreword, "Zone Defense: Countering Competition in the Space between War and Peace". Center for Strategic and International Studies. Accessed on September 28, 2019 at: https://www.csis.org/features/zone-defense

25 Heffernan, Virginia. Live tweeting the 2019 Doomsday Clock unveiling. Accessed on September 25, 2019 at: https://threader.app/thread/1088451489473785863

26 Bradbury, Roger et al. "How information warfare in cyberspace threatens our freedom." The Conversation, May 14, 2018. Accessible on September 25, 2019 at: http://theconversation.com/how-information-warfare-in-cyberspace-threatens-our-freedom-95512

27 Kelley, Colin P., et al. "Climate change in the Fertile Crescent and implications of the recent Syrian drought." Proceedings of the National Academy of Sciences of the United States of America. March 17, 2015, 112 (11) 3241-3246; first published March 2, 2015 at https://doi.org/10.1073/pnas.1421533112, accessed on September 25, 2019 at: https://www.pnas.org/content/112/11/3241; Fountain, Henry. "Researchers Link Syrian Conflict to a Drought Made Worse by Climate Change." New York Times, March 2, 2015. Accessed on September 25, 2019, at: https://www.nytimes.com/2015/03/03/science/earth/study-links-syria-conflict-to-drought-caused-by-climate-change.html; Rowling, Megan. "Climate stress drove wave of Arab Spring refugees - researchers." Reuters, January 23, 2019. Accessed on September 25, 2019 at: https://www.reuters.com/article/us-climatechange-conflict-arabspring/climate-stress-drove-wave-of-arab-spring-refugees-researchers-idUSKCN1PH23B

28 Clausewitz, Carl Von. On War. Indexed Edition, Edited and Translated by Michael Howard and Peter Paret. Princeton University Press; Reprint edition (June 1, 1989).

29 Kissinger, Henry. "How the Enlightenment Ends." The Atlantic, June 2018 Issue. Available at: https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/

30 Rosenberg, Shawn. "Democracy Devouring Itself The Rise of the Incompetent Citizen and the Appeal of Populism." Psychology of Political and Everyday Extremisms, 2019. Accessed on September 29, 2019 at: https://uci.academia.edu/ShawnRosenberg/Papers.

31 Hoffman, F.G. "Will War's Nature Change in the Seventh Military Revolution?" in Exploring War's Character & Nature, Parameters 47(4) Winter 2017-18, p. 19-31.

How the Cyberspace Narrative Shapes Governance and Security

James A. Lewis
Director, Technology and Public Policy Program at the Center for Strategic and International Studies

Cyberspace has become a global infrastructure, essential for business and security. When it was created, no one understood how it would bind economies and societies together in new and complex ways. In the broadest sense, governance is the understandings and expectations among states on international behavior, a framework for relations that provides a degree of predictability in interactions in security, trade or politics. Governance of the internet and cyberspace is a new and important aspect of this, as countries are bound more closely together and as the perception of transnational risk increases. In this context, cybersecurity becomes the ability of countries to defend their national sovereignty and advance their national interests individually and cooperatively.

The initial approach to governing the new infrastructure was ad hoc, voluntary, and based on engineering and business concepts. Non-state actors from companies and civil society would work as equal partners with governments organized into a multistakeholder community providing light governance that did not get in the way of growth. This minimalist approach was the right way to rapidly build a global network, but now that it is built, it needs reconsideration. However, light governance also created the "Wild West" environment that nations have been quick to exploit and where crime is untrammeled. Imperfect software sold without liability quickened adoption and implementation, but also contained the many vulnerabilities that today make cyberspace a shaky pillar for global commerce. This model of governance was the right one to launch and build the new global infrastructure, but now we need to ask if it needs to change.

How cyberspace now actually works and how it is changing cannot accurately be explained by the idealized, millennial, multistakeholder beliefs from the 1990s of a borderless world of shared values. One explanation for the current lies in the work of Antonio Gramsci and his theory of hegemony. The hegemony under consideration here is that of the cyberspace narrative, which distorts our perceptions and justifies the status quo. Gramsci wrote that our consent to a governance system is achieved through ideology, when people believe that existing economic and political conditions are natural and inevitable, rather than the creation of groups with a vested interest.

The U.S. invented the internet and for fifteen years after it commercialized the internet, American ideas dominated views and shaped policy. That period has come to an end but what will take its place is unclear, given the growing role of states in cyberspace and the declining power of the U.S. (perhaps accompanied by the growing power of other countries) in shaping global governance. Better cybersecurity requires a fresh look. Let's begin the discussion with two testable assertions:

1) States are the most powerful actors in cyberspace and responsible for the majority of dangerous cyber actions.

2) The multistakeholder model of governance is too western, insufficiently democratic, and too limited for the political challenges that a dependence on digital technologies is creating.

This is heresy, of course, but both assertions are provable and important for cybersecurity, since the cyber actions that pose the greatest risk demonstrably come from state actors or their proxies, not from some amorphous or unidentifiable source. This means that finding ways to constrain the behavior of states in cyberspace is the most important task for security.

Some of the initial ideas about the internet are no longer in serious contention. It is not a democratizing force per se, but one that erodes political legitimacy and authority and encourages extremism. Cyberspace clearly has borders, since it is based on a physical infrastructure located in national territories (or subject to national jurisdiction if undersea or in space). State sovereignty and international law clearly apply, endorsed unanimously by all member states in 2015, but how they apply is a subject for dispute. It is not a borderless commons.

If there is consensus that cyberspace is no longer a commons, there is no consensus on what it has become. The trends created by technology and political changes complicate our ability to understand the core political dynamics of cyberspace, but at their center are three significant issues that will shape governance and cybersecurity. These are questions about the changing nature of sovereignty, new requirements for legitimacy, and the effect of resurgent nationalism.

Sovereignty

The multistakeholder model was an attempt to replace the Westphalian system modified after 1945 with one that recognized the diffusion of economic and political power away from states and the erosion of borders in the face of economic and social globalization. A new model of governance that substituted a global stakeholder community for Westphalian states was expected to work best in this new space in providing public goods. There was even discussion of the end of Westphalian model of sovereignty as a result of globalization and the effect of the internet, but the sovereign state has proven to be both resilient and flexible. While the multistakeholder model is strong at managing the technical resources of the internet, there is general dissatisfaction with the performance of a "light," privately guided and shared governance, in privacy, anti-competitiveness, and security. However, the alternatives to the post-1945 order—untrammeled authoritarian sovereigns or fuzzy multi-stakeholder governance—prove even less attractive.

The expansion of sovereignty in cyberspace, while unavoidable, raises troubling problems. When cyberspace was ungoverned and considered ungovernable, it

became a playground for spies and criminals, but the same openness provided a new and untrammeled arena for the exercise of fundamental rights, most importantly the right to free expression. The pioneers of cyberspace believed it would be democratizing, even liberating. This was somewhat optimistic, but as governments expand their power to protect their interests (and this includes the safety and privacy of their citizens), the space for free expression is shrinking. The multistakeholder community is too weak to protect it, and some states ignore their commitments under the Universal Declaration of Human Rights. An inability to confirm commitment to human rights is one of the greatest impediments to new models of governance and the difficult and not well understood relationship between online information and security (information is not a weapon, but it can be "weaponized, i.e. used for coercive purposes online) also affects the ability to devise common understandings for cybersecurity.

As cyberspace has become a central domain for international conflict (and not the millennial vision of an end to conflict), security and the role of states has become more important. States see cyberspace as an unconstrained arena for espionage and coercion, and several powerful states also support cybercrime, either as a tool of state power for simple profit. Those who argue, for example, that states have lost their monopoly on force usually have never experienced the full range of violence a powerful state is able to inflict and equate a cyber-attack with kinetic or nuclear action. The most dangerous and damaging attacks require resources and a degree of engineering knowledge that are beyond the capabilities of non-state actors. A few criminal groups possess these capabilities, but these groups are located in states where they are in effect proxy forces, beholden to the national government.

Legitimacy

Legitimacy requires the assent of the governed. There is no good mechanism for expressing this assent for cyberspace. In the international system, states are the legitimate representatives of their societies (acquiring or asserting legitimacy through the mechanism of national elections). States possess sovereign rights and authorities, and they coordinate the exercise of sovereignty with other states through a series of understandings and mechanisms. The governmental and international approaches developed in the West in response to the global crises of the 1930s—multilateral institutions and rules, and the macroeconomic, managerial state—are no longer adequate (unless reformed). The original model of governance no longer ensures the assent of the governed.

Nor are all 'stakeholders' equal. States are understandably reluctant to entrust their fundamental security to private actors. Big companies have significant power over how cyberspace operates but are ultimately second to states if those states choose to challenge them and have the resources to do so. Gramsci would say big companies have until recently been unchallenged because of the dissuasive effect of the old, hegemonic multistakeholder narrative. Big tech companies will assert their independence from governmental control insofar as it does not cost them significant market share. The current governance model does an excellent job on the technical management of the internet, but it needs to be more representative of a global population, more transparent in its processes. In this we need to recognize that no actor other than a state has the legitimacy, legal authority or armed force necessary for security.

Nationalism

The internet brought western and American ideas to previously insulated nations. In cyberspace, cultures rub against each other; there are interconnections that bring change to even the most remote locations. One unexpected result of the internet is a general discontent with the ideas we once thought embodied progress since they were at the center of an American-driven globalization. The result is a powerful reaction in defense of national cultures and state sovereignty.

The reaction to globalism and the spread of western and Americanized culture has been resurgent nationalism, as societies seek to protect their own values, accompanied by a general discontent with western values on governance and individual rights that were once thought to embody progress. This is the antithesis of the "one world, no borders" approach of internet visionaries. The reemphasis of sovereignty and the right of a state to govern itself without external interference - and the internet is seen by many as external interference - sharpens conflict and makes international cooperation more difficult.

One result of this resurgent nationalism is that it has moved the global community to a post-1945 world when it comes to rules and institutions, and this has broad implications for cyberspace security and governance. Before 1945, governments played a role that was less constrained domestically and internationally. Some nations would prefer to return to this traditional definition of sovereignty, where universal rights were less important than sovereign interests in guiding national policy.

Once the lens through which we view cyberspace moves away from the outdated 1990s narrative, securing and controlling cyberspace becomes an engineering problem, where states will need to build (or acquire) the tools needed for management and security. Borders can be better defended, and rules imposed with the right policies in place and the right technologies to implement these policies. Governance can be established with the ability to write software to strengthen borders, manage online activity, and increase sovereign control.

Next Steps for Cybersecurity and Governance

Securing cyberspace is a complex problem for the international community. It involves a set of interrelated issues affecting business, human rights and national security. Other governance structures for international activities, such as air travel or finance, are more apolitical and lack the political consequences of cyberspace. This connection of political values makes the internet governance and cybersecurity problem much more difficult. What worked in the pioneering phase of cyberspace will no longer suffice.

While there is debate over the extent to which new rules and new mechanisms (including multistakeholder mechanisms) are needed, nations are gravitating toward an approach to cybersecurity that is placed within the exiting framework of international relations and creates shared understandings and rules for better cybersecurity. For governance, change is more difficult as incumbents and the powerful millennial ideology slow any transformation, but there is also impatience in many countries over key areas such as data protection, public safety and competitiveness where the status quo is seen as unacceptable.

This points to a reconsideration of the relationship between cybersecurity and internet governance. Cybersecurity is an element of a larger governance framework and while there does not need to be some single, overarching entity to govern cyberspace, the growth of reliance on digital technology means that it is time to transition to new approaches on how it is governed that assigns governments the central responsibility. This process of change will require the continued involvement of the multistakeholder community, but the nature of this involvement, the change in the relative positions of governments and private entities mean that the old model of governance will need to be replaced to make it less western, more inclusive and more democratic.

Such a change may be difficult for the "West," given the power of the old internet ideology, and new models of governance are more likely eventually to emerge from other sources, albeit in a piecemeal basis that addresses issues like data protection or localization first. If there is a contest over the future of governance, it may be well be between the democracies of the global source and the re-energized authorization states.

The need for better cybersecurity is a central driver for change in how we think about cyberspace. The current international approach is to further develop and implement norms, confidence-building actions, and capacity-building measures, but this has been expanded to consider the need for permanent mechanisms and binding rules (topics that came up in the 2015 GGE). Progress will also depend on finding ways to involve the multistakeholder community, after a fresh look that recognizes both its strengths and its limits.

Relations among states are defined by an elaborate web of power, influence, expectations, goals and commitments. Cyberspace is a still undefined element in this web of relationships. Governments are increasingly reluctant to accept the limited role assigned to them in securing an essential global infrastructure upon which their economies depend, and which has become the source of new and powerful threats, but at the same time, they cannot govern without the involvement of other actors from the private sector and society. There are steps that could be taken in the near term to reduce risk and uncertainty in cyberspace and reshape the landscape for governance in positive ways. Defining a post-millennium model for governance of the digital environment and creating new rules and mechanisms in the international community is the central task for a more secure and stable cyberspace.

05.
Livelihood

Small-Town Youths, Digital Lifestyle and Sustainable Urbanization

Winston Wenyan Ma
Adjunct Professor, NYU Law School

China's mobile economy today is not defined by the middle class in cosmopolitan cities like Shanghai and Beijing. Instead, the so-called "small-town youths" (*xiaozhen qingnian*) – the young generation of lower-tier cities and rural areas – are at the front line. In China, 'Tier 1 Cities' refers to the four cities of Beijing, Shanghai, Guangzhou and Shenzhen, while 'Tier 2 Cities' is loosely defined to include about two dozen other large cities, mostly in the coastal regions. 'Small town' essentially means any other residential centers in China.

With the development of China's broadband infrastructure and mobile payments, small-town youths have adopted the internet lifestyle as much as those in urban areas, where the internet is an integral part of daily life: from watching films and buying brands to hailing a ride and having food delivered to their doorstep. As such, the life-quality gap between cities and less developed areas is narrowed, and the small towns and rural areas are shaping up to become the engine of growth for China.

E-Commerce

Take the rise of e-retail startup Pinduoduo for example, which has caught the established e-commerce giants such as Alibaba and JD.com by surprise. Within four years of its inception, Pinduoduo boasts more active users than 15-year veteran JD.com and has beaten JD.com to become the second largest e-commerce platform in China. The key factor behind the success of Pinduoduo is its focus on young customers living in Tier 3 and lower cities. Customers from these cities are more frequent buyers, spend more time at e-commerce platforms than their counterparts in larger cities, and, collectively, have remarkable purchasing power.

The sudden rise of Pinduoduo is in line with equally surprising findings by Alipay, the mobile payment arm of Alibaba. Alipay reported in early 2018 that mobile payment is more popular in China's underdeveloped western regions than in the coastal cities. Guizhou and Shaanxi led the country in mobile payment adoption, followed by another nine provinces including Tibet, where on average the consumers processed over 90% of the online payments via mobile devices. The reason behind this: a lack of bricks-and-mortar retail infrastructure in those regions, leading people to turn to online shopping.

The same trend is evident in the food delivery market. According to a new report by iMedia Research, the market reached 358 million users in 2018, representing a 17.4% increase compared with the year prior. As delivery order volume in upper-tier cities become more saturated, users from third- and fourth-tier cities contributed to most of the growth. It is expected that the fifth- and lower-tier cities will soon emerge as a new battleground for food delivery players.

The Creative Economy

Small-town youths are also the driving force behind the market for online novels, videos and movies. In China, online creators write and post in installments, and the mobile payment systems makes it convenient for readers to make small, repeating payments for their serial reading. Users can pay a tiny fee, equivalent to a fraction of US$ 0.01, to read each update: this turns many small-town youths into avid readers.

It is also quite easy for the fans to become authors themselves. Before the Internet age, it was almost impossible for young writers in China to emerge, because only a small number of authors have access to publishing houses in major cities. Online, however, anyone can publish his or her story as soon as a few installments are finished and discuss them with readers. Because internet has leveled the playing field for aspiring young writers, even unknown authors from remote areas could pen popular hits.

The same is happening on the video platforms as well. Those sites provide video templates, guidance and examples to ensure users' interest on creation. Some platforms like Tik Tok and Kuaishou even offer users a wide range of background audio and special effects to make the videos richer, such that even ordinary users could create highly polished videos. Not surprisingly, most of the recent addition of users come from the small-town youths.

Revitalizing Rural Jobs

Besides online shopping and entertaining, small-town youths are capturing the digital businesses opportunities themselves. For example, when new channels are created to transport farm produce to the cities, villagers can be online merchants, tapping into the growing demand for fresh, safe agricultural products in the cities.

Today a rural entrepreneur only needs to have a 20-square-meter space, a second-hand computer and a basic internet connection to become an online retailer. With social media-messaging-and-payments infrastructure provided by the major platforms like Alibaba and Tencent, they could easily handle large trade volume and even reach global markets. Most recently, they have begun to add videos to their marketing, bringing more products made in rural China to urban dining tables: building up vibrant businesses, while creating new jobs to revitalize local communities.

The Sharing Economy

Finally, it is only natural that the small-town youths are also a main driver for the sharing economy in China. Unlike Airbnb and Uber, which provide a platform that

connects users to under-utilized, existing resources like spare rooms and private cars, sharing in China is more like 'mobile renting'. The online sharing (renting) services involve frequent, small payments from changing locations, and the users can simply complete them with a simple tap.

From cars and bikes, basketballs and refrigerators, to clothes and massage chairs, exercise rooms and phone chargers, these sharing services enable people to simply access the things they once had to buy. This is a faster and more efficient way to give people a better quality of life, especially when considering that the average incomes in China are still very low and the consumers are still very price conscious.

Conclusion

Overall, the digital economy creates more business opportunities for both rural and urban residents, but also narrows the living standard gap between them. When the 'internet lifestyle' reaches less developed regions, small-town youths can find a new path to quality livelihood in their hometown. They do not have to give up their cheaper housing, shorter commute time, cleaner air and direct access to fresh foods– all things city dwellers long for.

Therefore, urbanization does not need to entail people migrating from rural regions and leaving them desolate while overcrowded mega cities are challenged by transportation, environment and social issues. As the urban-rural divide on quality of life is narrowed through digital technology and services, the global urbanization push can potentially end in more balance than conflict.

The Promise and Reality of Digital Technologies in Bridging the Rural-Urban Divide

Aditi Kumar
Executive Director, Belfer Center for Science and International Affairs, Harvard University

The rural-urban economic gap is one of the most important factors that shape overall economic inequality. Digital innovation undoubtedly carries the promise of accelerating rural development, and various public and private sector-led initiatives – such as India's broadband expansion program, BharatNet, and China's concerted investment in digital education to reach rural areas – are trying to harness its potential. But is this innovation enough to allow rural workers to engage in productive, fulfilling work without migrating to cities?

The trends in income and employment in urban versus rural areas, particularly in low- to middle-income countries, are murky at best. In India, the rural-urban income gap narrowed between 1983 and 2010, but this is attributed in part to rural areas "urbanizing" and being absorbed into fast-expanding city centers that provide higher paying jobs and better services to citizens.[1] In general, it is quite challenging to isolate the effects of digital technology on rural income, rather than confounding factors such as rural to urban migration and social welfare programs targeting rural populations. In this sense, data from China may provide a better indication of trends, since the hukou system of permits prevents rural workers from moving to more productive urban regions. In China, the income gap has actually increased: urban households earned 2.2 times as much disposable income relative to rural ones in 1990, and 2.7 times as much in 2017.[2]

No doubt digital technology has facilitated important quality of life improvements in rural areas – access to online markets, food delivery, and streaming entertainment, for example, have narrowed the gap between the lived experience of urban and rural populations. However, this is markedly different from narrowing the productivity or economic gap between these groups. Three principal, albeit not exhaustive, ways in which digital technology can bridge the urban-rural economic divide are:

1. Attracting higher-paying jobs to rural areas, chiefly through the development of digital infrastructure that allows remote work and the development of tech ecosystems;

2. Increasing the gains from rural economic activity, for example by leveling the

competitive landscape for pricing and market information or increasing access to global markets;

3. Facilitating higher participation in systems that improve the productivity of rural workers, such as access to finance, education, and healthcare.

For each of these mechanisms, the reach and impact of digital innovation in low- to middle-income economies have been mixed.

First, digital technology holds the promise of attracting higher-earning jobs to rural areas by facilitating remote work and the development of tech ecosystems, thus addressing the 'brain drain' problem of highly skilled individuals having to move to urban centers. While this may be a viable path for advanced economies, the impact of such innovation is relatively muted in developing economies where the services sector comprises a minority share. In India and China, the agricultural and manufacturing sectors together account for 69% and 56% of labor force participation, respectively.[3,4] In these economies, proximity to farms and factories remains key, and the advent of teleworking infrastructure is less relevant to workers' livelihoods.

Second, digital innovation has the potential to increase the gains from rural economic activity, in part by allowing rural workers to capture larger pieces of the economic pie. One way is by facilitating greater transparency in pricing and other market information through public information systems. In India, for example, the Ministry of Agriculture runs AgMark: a web portal that disseminates pricing information from wholesale markets, allowing small farmers to better understand demand and obtain fair pricing for their produce. Similar price information systems have attracted public and private sector investment in other developing economies, with a well-documented track record of easing access to market information and improving incomes.[5]

Another is by democratizing channel access, such as giving small farmers and rural entrepreneurs the opportunity to reach more buyers through online marketplaces. Here, the advantages to rural workers are less clear, as e-commerce has delivered outsize gains to a few oligopolistic platforms. In the U.S., Amazon accounts for an incredible 49.1% of all online retail spend, followed not so closely by eBay, which accounts for 6.6%.[6] This is a losing proposition for small retailers: as more go online, they must compete for premium positions on just one or two online platforms. As a result, customer acquisition costs have increased by 50% over the past five years, while the average value of an online order has remained flat.[7] The same trends are visible in the growing Indian and Chinese e-commerce markets. In India, FlipKart and Amazon India together capture 60% of online sales,[8] while in China, Alibaba alone captures 60%. Rural enterprises and entrepreneurs may be absolutely better off by being able to access a larger market, but it is difficult to imagine relative gains to rural workers in this system of concentrated market power.

Third, and most promisingly, digital technology can help close the rural-urban economic gap by allowing rural populations to participate in long-term productivity-enhancing systems, including education, finance, and healthcare. In both India and China, the digitization of education, which aims to deliver quality teaching to rural students using online platforms, has become a government priority. The links between educational attainment and income are well-established: in India, the urban-rural wage convergence is in part attributed to a convergence in educational attainment, with the urban advantage narrowing from 164% more education-year

completed in 1983 to 78% in 2010.[9] The expansion of online learning tools is projected to accelerate this trend.

Similarly, technologies like Aadhaar, the biometric database of unique IDs, has been a driving force in lowering the unbanked population from 60% of Indian adults in 2011 to 20% in 2018.[10] While only the first step, higher financial inclusion combined with financial literacy and tailored financial products will be critical to enhancing rural productivity. Finally, advances in healthcare -- including remote diagnostic capabilities and web portals that disseminate basic health information -- can help bridge shortages of trained medical professionals in rural areas. Improved health outcomes affect economic well-being by increasing worker productivity and reducing the financial burden of illness.

Of course, the gains to rural populations stemming from digital innovations are predicated on myriad factors, including access, affordability, and literacy. The idea that the average rural worker in India or China who cannot today rely on around-the-clock electricity could launch on online store or participate in a virtual classroom appears far-fetched. In both countries, rural internet penetration remains at roughly 20% today, compared to nearly 60% in urban areas.[11,12] While China has been largely successful in expanding broadband coverage, only 7% of Indian households have access, and almost all in urban centers.[13] Significant investment in digital infrastructure is needed to fully harness the potential of the digital revolution in rural areas.

Overall, the impact of digital innovation in bridging the rural-urban economic divide is mixed. On the one hand, greater access to markets, market information, and finance, education, and healthcare resources can help rural workers lower transaction costs, identify growth opportunities, and improve long-term productivity. On the other, the oft-touted benefits of remote work enabled by digital technology are less relevant in many low- to middle-income economies reliant on non-services sectors. Moreover, digital innovation has created new oligopolistic systems, concentrating market power and profits among a few service providers and further enhancing the rural-urban divide.

Endnotes

1 Viktoria Hnatkovska, "Urbanization is Narrowing India's Rural-Urban Wage Gap", World Bank, 27 October 2014. Accessed: 30 September 2019. https://blogs.worldbank.org/jobs/urbanization-narrowing-india-s-rural-urban-wage-gap

2 National Bureau of Statistics of China. Annual per capita disposable income of rural and urban households in China from 1990 to 2017 (in yuan). 2018. Statista. Accessed: 30 September 2019. https://www.statista.com/statistics/259451/annual-per-capita-disposable-income-of-rural-and-urban-households-in-china/

3 World Bank. India: Distribution of the workforce across economic sectors from 2008 to 2018. 2019. Statista. Accessed: 30 September 2019. https://www.statista.com/statistics/271320/distribution-of-the-workforce-across-economic-sectors-in-india/

4 National Bureau of Statistics of China. China: workforce breakdown across economic sectors from 2007 to 2017 (in millions). 2018. Statista. Accessed: 30 September 2019. https://www.statista.com/statistics/278346/economic-sector-distribution-of-the-workforce-in-china/

5 Luc Christiensen, Siddhartha Raja, and Esteve Sala, "Can Technology Reshape the World of Work for Developing Countries?", World Bank, 1 June 2017. Accessed: 30 September 2019. https://blogs.worldbank.org/jobs/can-technology-reshape-world-work-developing-countries

6 Ingrid Lunden, "Amazon's share of the US e-commerce market is now 49%, or 5% of all retail spend", TechCrunch, July 13, 2018. Accessed: 30 September 2019. https://techcrunch.com/2018/07/13/amazons-share-of-the-us-e-commerce-market-is-now-49-or-5-of-all-retail-spend/

7 Don Davis, "Ecommerce Profitability is Down", Digital Commerce 360, 13 May 2019. Accessed: 30 September 2019. https://www.digitalcommerce360.com/2019/05/13/ecommerce-profitability-is-down-here-are-some-things-retailers-can-do-about-it/

8 Daniel Keys, "Flipkart is poised to Overtake Amazon in India by 2023", Business Insider, 29 March 2019. Accessed: 30 September 2019. https://www.businessinsider.com/flipkart-will-overtake-amazon-india-2019-3

9 Hnatkovska, ibid.

10 Ramesh Iyer, "Financial inclusion in India is soaring. Here's what must happen next", World Economic Forum, 14 January 2019. Accessed: 30 September 2019. https://www.weforum.org/agenda/2019/01/financial-inclusion-in-india-is-soaring-heres-what-must-happen-next/

11 Surabhi Agarwal, "Internet users in India expected to reach 500 million by June,'' Economic Times, 20 February 2018. Accessed: 30 September 2019. https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-expected-to-reach-500-million-by-june iamai/articleshow/63000198.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

12 Meng Jing and Sarah Dai, " Behind the great firewall, China's internet is thriving – even in rural areas", South China Morning Post, 3 February 2018. Accessed: 30 September 2019. https://www.scmp.com/tech/apps-gaming/article/2131730/behind-great-firewall-chinas-internet-thriving-even-rural-areas

13 Devina Sengupta, "Subscriber base of broadband to grow 44%: Study", Economic Times, 1 January 2018. Accessed: 30 September 2019. https://economictimes.indiatimes.com/tech/internet/subscriber-base-of-broadband-to-grow-44-study/articleshow/62321272.cms?from=mdr

Productivity vs Well-being: The promise of tech mediated work and its implications on society

Astha Kapoor and Dr. Sarayu Natarajan
Co-founders, Aapti Institute

Introduction

This paper is a response to the framing proposition, which states that the advent of technologies can narrow the urban-rural productivity gap by enabling younger generations in productive, fulfilling work without migrating to big cities. This proposition has been put forth in the context of China's "small town youth" who are at the frontline of the country's digital boom. However, this proposition disregards how labor relations are skewed as a result – workers do not have autonomy to decide tasks, negotiate payments or form worker collectives and are under the control, though fragmented, of the platform. In this context, the question of productivity gains as output is narrow, and disregards questions of worker well-being and more fundamentally, labor rights.

This paper examines the prompt by looking at the question of productivity in work generated on digital platforms. It asserts that the new digital economy needs a new definition and way of measuring productivity, which takes into consideration questions of labor well-being. The paper buttresses its arguments with analysis from India, which like China, has become a point of focus and expansion of the sharing economy, with Indian, American and Chinese platforms in the mix.

Understanding productivity in the digital age

The productivity gap, which is the measured difference in output between workers, or the gross domestic product per worker, is a cause of some debate globally. It is widely acknowledged that there has been a slow-down in productivity. There are three main reasons given for this perceived slowdown in productivity.

First is the claim by Robert Gorden[1] that today's innovations do not compare in scale or impact to breakthroughs of the past such as the telephone or the internet, which had immediate, economy-wide implications. This view has been challenged on the grounds that new digital technologies are in their nascent phases.

Second, the OECD[2] argues that productivity has not slowed down; rather, it has become concentrated in a few firms that are more innovative and therefore more profitable.

Finally, some claim that traditional measures of productivity have not accounted for the impact of the internet and digital technologies. Machines are outperforming humans in many industries[3] and there may not be a good way to capture this sea-change.

In this context, this paper examines the prompt, moving away from the perspective of productivity gains from tech-enabled work toward one that examines how to think about broader notions of well-being. While technology has, through gamified micro-tasking and AI labelling, as well as the gig economy, expanded opportunities for work-seekers, it has not necessarily enhanced well-being. These kinds of work are done often by those who are outside Indian megapolises, and those who lack avenues for employment elsewhere.

To unpack the complex intersection of productivity gains and technology enabled work, we examine two areas, mediated by digital technology, which have opened up for young people outside of Indian megapolises participation in the platform economy, and low-skilled digital micro-tasks (often gamified) such as object-labelling. This work, because it is mediated by technology and renders geographic location of the worker inconsequential, seems to provide opportunities for a large number of people and may appear to enhance productivity and opportunity. However, the nature of this work, and the protections and meaningfulness it offers to workers is under question.

There is a growing case, as Sen and Stiglitz[4] have suggested, for measuring well-being. If people's lives will no longer be defined by the work they do, then is it important to measure contributions to GDP or should countries and firms be measuring labor health, education, political participation, charity contributions, and subjective well-being?

Labelling and micro-tasking: Little meaning beyond productivity

India is increasingly becoming a hot-bed for microtasks for the artificial intelligence (AI) industry. With the growth in the use of AI across sectors, data-labelling has become a key requirement. Simultaneously, the growth of the e-commerce sector has spawned demand for several labelling micro-tasks. Thousands of people scattered across tier II and tier III cities in India are engaged in labelling and annotating data.

The task of data-labelling requires relatively low levels of skill. Workers view data from cameras, sensors, emails and social media to highlight differences and similarities, or identify objects. Or they label objects on e-commerce websites (such as apparel) into proper categories. When this labelled data is fed into the algorithm, it can rightly infer the data, find patterns and learn from it over time. Data is used, for instance, for the self-driving car industry, to label images of road signs, traffic lights, and pedestrians. This data will be used to train the autonomous vehicles to navigate real life situations. Data labellers are the "construction workers" of the digital economy, putting together the pieces that hold together technological companies[5].

This industry, like the previous influx of business process outsourcing (BPO) work,

can use India's large, untrained workforce. Amazon's MTurk was a popular way of crowd-sourcing micro-tasks in India, but restrictions were imposed for non-US based workers due to security concerns. As a response, Indian companies such as Playment,[6] iMerit and Infolks have been set up to cater to global clients and evolve into a hub for labelling and annotation work. Other companies like Squadrun provide labelling services by gamifying the labelling tasks to further engage those doing the work.

Data labelling companies, as mentioned above, tend to work out of smaller towns and cities, which are cheaper locations to set up these large centres as cost arbitrage is a significant element of the business model. The workforce is sourced locally, and often comes from families that make less than USD 100 per month[7]. Companies claim to pay labellers anywhere between USD 300 to USD 400 per month, adding significantly to household incomes.

There is little information about work conditions of data labellers in India. Even if one regards this work force as formalized, the quality of work, the nature of the work conditions, and the meaning workers derive from it raises concerns. The primary cause for worry is that these low-skilled jobs appear transient, which is that they only exist until machines themselves can be trained to label and annotate objects. Once that shift occurs, these hundreds and thousands of jobs could vanish and the people doing them would have to acquire new skills to stay relevant.

This work has been defined as "ghost work" - invisible labor that powers technology platforms.[8] The labor force working to label data, is invisibilised, as technology companies tend to treat them as "code" and not real workers. This invisibilization also keeps up the idea of technological magic[9], a much-marketed myth which positions automation as a way of freeing up human time, but in reality, is fuelled by humans themselves. Perhaps, it is also why these jobs are kept out of big cities and are performed in far-off parts of the world such as rural India and China.

That such work able to provide opportunities for India's youth, particularly in the rural and peri-urban areas is clear. However, how satisfying and sustainable these opportunities are, what opportunities they provide beyond transient gains in productivity and how well-being needs to be understood in context must be explored further.

Platform/gig economy work industry (Ride sharing): precarity and well-being

Ola and Uber both have recently launched "lite"[10] versions of their apps to reach out to the vast number of users and drivers in tier II and tier III cities in India. The apps are built to load on lower end phones, and use less than 1MB of data. In addition, both platforms are aggressively expanding their two-wheeler outreach in smaller cities, with investments in business such as Ola Bike, Bounce, Rapido and Yulu. Ola has also expanded to over a hundred cities in India and is becoming ubiquitous in state capitals across the country. Related to this national expansion of several technology platforms, a total of 1.3 million Indians joined the platform economy between October 2018 and March 2019.

As these platforms expand into smaller cities, there is an assumption that workers will be sourced from neighboring towns and villages, coming into cities as short-term migrants. A recent study shows that 30% of drivers[11] on ride-sharing platforms in Bangalore were agriculturalists or garment workers from neighbouring areas, pushed to the city due to agricultural distress. As in the case of labelling, the skills required to participate in the ride-sharing economy are limited. Increasingly, commercial driving licenses, which have a stricter criterion for approval, are not required for driving taxis.

Aapti's empirical research shows[12] that workers lack job security and do not have social security in the form of insurance or health benefits from the platforms through which they work. Most workers in the platform economy do not consider this work to be a long-term option. They also must navigate complex and opaque contracts, keep impossible work hours to fulfil targets to unlock incentives. Workers experience arbitrary deactivation, surveillance and do not appear have any avenues for grievance redressal.

Platforms experience attrition rates which can range from 40% - 300% for some companies. Interestingly, half the workforce that is below the age of 23 years leaves these jobs in the first three months, either because of new opportunities, or because living in cities in these informal jobs becomes unviable.

While the gig economy does indeed add to productivity and opportunities available for those outside of big megapolises, the precarious nature of the employment raises questions about the meanings of well-being.

Implications: The well-being argument

As illustrated by the examples above, digitization offers several opportunities to people, especially the technologically savvy, smartphone-using youth, so that they do not have to move to live in metropolitan cities. They can also find work closer to their homes in smaller towns and villages. However, the kind of work being mediated by technology raises several questions from the paradigm of well-being for the workforce, and the broader implications of these jobs.

While jobs in AI labelling and related micro-tasking indeed provide economic opportunity and enhance productivity by utilising idle time, their very nature (limited prospects for betterment and growth) and uncertainty complicate how to infer well-being. Similarly, in the driving platform economy, questions around hours, surveillance and emotional labor and more go to the core of inferring well-being. While new legislative efforts, such as the Code of Wages Bill, 2019 do attempt to include the platform economy and gig workers within their scope, we need to evaluate the broader set of concerns that arise in the tussle between enhanced productivity and opportunity on the one hand, and well-being on the other.[13]

The thrust of some of this innovation has been an entrepreneurization of labor. While this may offer some advantages in terms of flexibility and choice, especially to those with some privileges such as social and economic capital, it may push those currently in the margins further out. Those who cannot afford the car or a smart phone that is a crucial requirement for entry into this sector, may be left at the margins of society, being unable to access these forms of employment. Women, especially, are significantly disadvantaged here.

Conclusion

We go back to Sen, Stiglitz and Fitoussi's argument[14] that well-being is a better measure of growth and productivity and a focus should be on jobs that improve the quality of life by providing better health, education, social security and safety etc. It is crucial to better understand the aspirations of people and find opportunities for work that create a space for individuals to find meaning as opposed to performing jobs that enact transient ideas of productivity.

This is possible to do through investments in small and medium enterprises outside Indian metropolitan cities, encouraging the adoption of digital tools such that they are no longer on the margins of productivity, whatever the definition. It would also come from a thoughtful evolution of a legal framework to offer protections for those in the platform economy, and avenues to seek redress.

It is also crucial to move forward from static meanings of both productivity (increased GDP) and well-being to understand the platform economy in context. While there is freedom, flexibility and empowerment that come from participation on the platform economy, a focus on productivity alone may limit opportunities for those on the geographical margins in the long-term.

Endnotes

1 Gordon, Robert. “Is U.S. Economic Growth Over? Faltering Innovation Confronts the Six Headwinds,” 2012. https://doi.org/10.3386/w18315

2 Andrews, Dan, Chiara Criscuolo, and Peter N Gal. “Frontier Firms, Technology Diffusion and Public Policy.” OECD Productivity Working Papers, December 2015. https://doi.org/10.1787/5jrql2q2jj7b-en

3 Mohan, Deepanshu. “India Is Very Much Part of the Global Productivity Slowdown.” The Wire. Accessed September 18, 2019. https://thewire.in/economy/india-global-productivity-slowdown

4 Fox, J., 2014. The Economics of Well-Being. Harvard Business Review 8 October 2014. https://hbr.org/2012/01/the-economics-of-well-being [Accessed 17 Sep 2019].

5 Yuan, L., 2018. How Cheap Labor Drives China’s A.I. Ambitions. The New York Times 25 November 2018 https://www.nytimes.com/2018/11/25/business/china-artificial-intelligence-labeling.html [Accessed 17 Sep 2019].

6 Playment, in fact, states that it engages over 300,000 workers, and recognises about 25,000 of them, as “highly skilled”.

7 Murali, A., A. Sen & J. PK, 2019. How India’s data labellers are powering the global AI race. FactorDaily 20 March 2019 . https://factordaily.com/indian-data-labellers-powering-the-global-ai-race/ [Accessed 11 Sep 2019].

8 Chen, A., 2019. How Silicon Valley’s successes are fueled by an underclass of “ghost workers”. The Verge 13 May 2019. https://www.theverge.com/2019/5/13/18563284/mary-gray-ghost-work-microwork-labor-silicon-valley-automation-employment-interview [Accessed 16 Sep 2019].

9 BBC News, n.d. The ‘ghost work’ powering tech magic - BBC Worklife. BBC News. https://www.bbc.com/worklife/article/20190829-the-ghost-work-powering-tech-magic [Accessed 11 Sep 2019].

10 ETtech.com, 2019. How Uber Lite is trying to reach a new set of potential riders in emerging markets - ETtech. ETtech.com 10 January 2019 . https://tech.economictimes.indiatimes.com/news/mobile/how-uber-lite-is-trying-to-reach-a-new-set-of-potential-riders-in-emerging-markets/67466890 [Accessed 20 Sep 2019].

11 Surie, A., & Sharma, L. V. (2019). Climate change, Agrarian distress, and the role of digital labour markets: evidence from Bengaluru, Karnataka. Decision, 46(2), 127-138.

12 Gupta, S., 2019. Future of Workers: Building safe workplaces of the future. Medium 18 September 2019 https://medium.com/aapti/future-of-workers-building-safe-workplaces-of-the-future-83cf5bbe6983 [Accessed 18 Sep 2019].

13 Jha, S. & N. Alawadhi, 2019. Gig workers set to come under labour laws, get social security benefits. Business Standard 18 September 2019 . https://www.business-standard.com/article/economy-policy/gig-workers-set-to-come-under-labour-laws-get-social-security-benefits-119091900052_1.html [Accessed 18 Sep 2019].

14 Fox, J., 2014. The Economics of Well-Being. Harvard Business Review 8 October 2014 . https://hbr.org/2012/01/the-economics-of-well-being [Accessed 15 Sep 2019].

Authors

Nikhil Pahwa

Nikhil Pahwa is the Founder, Editor and Publisher of MediaNama (www.medianama.com), the leading publication for news and analysis on the evolving digital ecosystem in India. Nikhil is also a TED Fellow, as well as a co-founder with SaveTheInternet.in and Internet Freedom Foundation.

Paula Kift

Paula Kift is a privacy and civil liberties engineer at Palantir Technologies, which she joined upon graduating with a master's degree in media, culture, and communication from New York University in 2016. At Palantir, she primarily focuses on the technical implementation of European Union data protection law.

Tanuj Bhojwani

Tanuj Bhojwani is a Fellow at iSPIRT Foundation. Most recently, he helped the government formulate and implement Digital Sky, a real-time low altitude notification and authorization platform for commercial drones.

Dennis Broeders

Dennis Broeders is an Associate Professor of Security and Technology and Senior Fellow of The Hague Program for Cyber Norms at Leiden University's Institute - of Security and Global Affairs. His research and teaching broadly focuses on the interaction between security, technology and policy, with specific areas of interest in cyber security governance, internet governance, surveillance, Big Data and security studies.

Arindrajit Basu

Arindrajit is a Senior Policy Officer at the Centre for Internet & Society with the Cyber Security Project. Arindrajit's primary interests lie in the fields of International Relations and Public Law. His work at CIS focuses largely on developing normative frameworks for the regulation of emerging technologies internationally and conceptualizing the strategic role that India and other emerging economies can play in this space.

Anushka Kaushik

Anushka Kaushik is currently running the cybersecurity policy programme at the GLOBSEC Policy Institute in Bratislava and is responsible for the organisation's research efforts and initiatives in that sphere. She specializes in cyber strategies, attribution processes in cyber-attacks, and cyberspace governance. She has a Masters degree from Sciences Po, Paris and has previously worked at the International Chamber of Commerce and the Centre des Recherches Internationales.

Lydia Kostopoulos

Dr. Lydia Kostopoulos is a Senior Researcher at the Digital Society Institute in Berlin. Her work lies in the intersection of people, strategy, technology, education, and national security. She regularly speaks internationally on disruptive technology convergence, innovation, tech ethics, and national security. In efforts to raise awareness on AI and ethics she is working on a reflectional art series [#ArtAboutAI], and a game called Sapien 2.0 about emerging technology and ethics www.lkcyber.com

Terri Chapman

Terri Chapman is a Visiting Associate at the Observer Research Foundation in the economy & growth and cyber & media programs. Her research focuses on the impacts of technology on democracy and governance, labour markets, and employment and social protections. More broadly, her research interests include social mobility, welfare, and inequality. She also leads outreach activities for ORF in South Asia and Africa. Prior to joining the Observer Research Foundation, Terri worked as a management consultant advising public sector clients on regional economic development.

Mihir S. Sharma

Mihir Swarup Sharma is a Senior Fellow and Head, Economy and Growth Programme at ORF. Hwas trained as an economist and political scientist in Delhi and in Boston. From 2008, he edited and wrote a column for the opinion pages of The Indian Express and Business Standard, both based in New Delhi, and has won a Sriram Sanlam award for financial journalism. His book Restart: The Last Chance for the Indian Economy was published in 2015, to considerable critical acclaim; it won the Tata LitLive best Business Book of the Year and was longlisted for the Financial Times–McKinsey Business Book of the Year. He is also the India columnist for Bloomberg View.

Sean Kanuck

Sean Kanuck is Founder and CEO of EXEDEC LLC, as well as Distinguished Fellow at ORF. As a globally recognised cyber expert, he advises governments, corporations, law firms, and entrepreneurs on the nexus between technology, law, and security. Sean led cyber analysis for the United States as its first National Intelligence Officer for Cyber Issues from 2011 to 2016. He previously served 11 years in the CIA Information Operations Center, including both analytical and field assignments, as an Intelligence Fellow with the Directorates for Cybersecurity and Combating Terrorism at the White House, and as a member of the US delegation to the UN Group of Governmental Experts on international information security. Prior to government service, Sean practiced corporate law with Skadden Arps in New York.

Philip Reiner

Philip J. Reiner is the Executive Director of Technology for Global Security, a non-profit network based in the Bay Area focused on solving international security challenges with a technological nexus. Additionally, he serves as Director for Advisory, North America at AETOS Strategy & Advisory, is an Affiliate at Stanford University's CISAC, and is an advisor to Do No Digital Harm. He served at the White House as Senior Director for South Asia on the National Security Council staff, and previously as Senior Advisor for Afghanistan and Pakistan, and Director for Pakistan.

James A. Lewis

James Andrew Lewis is a senior vice president and director of the Technology Policy Program at the Center for Strategic and International Studies (CSIS). He has authored numerous publications on the relationship between technology, innovation, and national power. His current research examines international security and governance in cyberspace, the geopolitics of innovation, the future of warfare, and the effect of the internet on politics.

Winston Wenyan Ma

Winston Ma was Managing Director and Head of North America Office for China Investment Corporation (CIC). Prior to that, Mr. Ma served as the Deputy Head of Equity Capital Markets at Barclays Capital, a VP at J.P. Morgan Investment Bank, and a Corporate Lawyer at Davis Polk & Wardwell in New York. He is the author of China's Mobile Economy, Digital Economy 2.0, The Digital Silk Road, and forthcoming China's Data Economy (2019, Hayakawa).

Aditi Kumar

Aditi Kumar is the Executive Director of the Belfer Center for Science and International Affairs at the Harvard Kennedy School, where she also leads the Economic Diplomacy Initiative. She was previously a Principal at management consultancy Oliver Wyman in the financial services and public policy practices. Her research interests include U.S. international economic policy, financial technology, and financial regulation.

Astha Kapoor

Astha Kapoor is Co-founder at Aapti Institute, a research firm examining the interface between tech and society. She works on data governance, basic income, digitization of welfare, work and social architectures of technology. Astha is well-published in The Wire, DailyO etc. She is a two-time TedX speaker, and Global Governance Futures Fellow (2018-19). Astha has a Masters from Erasmus University, and a Bachelors from St. Stephens College.

Sarayu Natarajan

Sarayu Natarajan is Co-founder at Aapti Institute. Dr. Natarajan is a political scientist as well as co-host of the podcast, Ganatantra.

Cover Design

Background vector created by pikisuperstar - www.freepik.com