ORF

global POLICY

GP-ORF Series

DIGITAL DEBATES

CyFy Journal 2017
Edited by Samir Saran

CyFy

Durham University

WILEY-BLACKWELL

GLOBAL POLICY

Digital Debates 2017

Edited by Samir Saran

Digital Debates
CyFy Journal Volume 4 (2017)

Authors:

Amelia Andersdotter, Chelsey Slack, Dennis Broeders, Elina Noor, Hugo Zylberberg, Logan Finucan, Madhulika Srikumar, Meghna Bal, Michael Khoo, Nikolas Ott, Peter Lovelock, Ryan Johnson, Sean Kanuck, Seha Yatim, Urvashi Aneja, Vidisha Mishra

Editorial Team:

Akhil Deo, Arun Mohan Sukumar, Bedavyasa Mohanty, Madhulika Srikumar, Meghna Bal, Vinia Datinguinoo Mukherjee (ORF)

Printed by:

Vinset Adveretising, New Delhi

Contents

EDITOR'S NOTE

Technology and Transformation

Samir Saran

In many parts of the world, tensions offline are now mirrored online. In the manner of a Wachowskis movie, machines influence both realities and the perception of such realities, often expressed online. The challenge for those seeking to "govern" or "regulate" cyberspace, then, is the umbilical connection between digital networks and their offline effects. How do you cut the cord? One or another way of regulating cyberspace today may have unintended consequences for all facets of economic life, social engagements and political discourse. Many governments, acknowledging this problem, have tried to regulate the effects of technology, rather than the technologies themselves. This year's edition of Digital Debates explores, in twelve engaging pieces, how this process of "cyber-" regulation has been influenced by watershed political and military events, upending the role of state and non-state actors as traditionally understood.

The year 2017 was tumultuous for politics, economics, and international relations. While the global community was still coming to terms with the United Kingdom's decision to exit the European Union, the American public voted for Donald Trump, who may be described as the unlikeliest yet of candidates to have contested the US presidency. President Trump ran a campaign that many had considered antithetical to the soul of America—the free flow of capital and people. By most indications, Trump is determined to reshape American foreign policy, global governance institutions, international trade and security.

President Trump's ascent to the White House — and indeed, the manner in which this was made possible — gives the international community an opportunity to reflect on the questions that are confronting cyberspace. Three developments are noteworthy, foremost of which was the shadow cast by Russia on the US presidential campaign. In an operation previously unheard of in American shores, Russia hacked into the Democratic National Committee's database and selectively leaked information that would eventually damage contender Hilary Clinton's efforts and favour Donald Trump. With this act, Russia showed the world how influence operations and information warfare can disrupt even the most entrenched democratic processes. It also signalled the brazenness of new technologies; nothing is sacrosanct.

Elina Noor, in 'Reconsidering cyber security' and Sean Kanuck, in 'Hacking democracy'write about Russia's influence campaign in 2016 aimed at the US presidential elections, noting how attacks in the future will continue to affect integrity of information infrastructures.

The second issue deserving of attention was Hilary Clinton's reliance on Artificial Intelligence (AI) and Big Data to make decisions during her campaign. For instance, confident in her team's analytical model which predicted that it was not necessary to spend time on the ground in Michigan and Wisconsin, Clinton failed to address what might have been a key constituency. Analysts say this oversight contributed to her loss.

A third focal point was the role of social media: in his campaign, Trump relied heavily on Twitter and Facebook to reach out to his audience, effectively bypassing the traditional media of print and television. Importantly, through algorithmic tailoring and personalised news feeds, social media was also responsible for creating what is called "information echo chambers" and polarising voters in the process.

Since assuming office, Donald Trump has worked to influence the US' digital policies and the government's role in cyberspace. Trump's withdrawal from the Trans-Pacific Partnership (TPP), which would have represented approximately 40 percent of global GDP and 25 percent of world exports, has imperiled the US' influence over digital norms. These norms would arguably have improved e-commerce and standardised internet rights amongst its member states. Similarly, Trump's nationalist leanings have created uncertainty over

America's immigration policy; for one, he is adamant to institute changes in the US' H1-B Visa programme to limit the number of foreign employees in the US' technology industries.

Along the same line, Trump has also signed a bill repealing the US' Internet Service Provider privacy rules, which currently impose limits on how ISPs can use and sell customer data. Defenders of civil liberties believe it is a blow to the people's privacy rights. Further, Trump's appointment of one of the fiercest critics of the open-internet norm, Ajit Pai, as head of the Federal Communications Commission (FCC) has challenged the principles of net neutrality which were laid out only two years ago under Tom Wheeler's Open Internet Order.

Another stakeholder in the ongoing conversation on cyberspace is China. As American hegemony continues to wane, China is offering alternatives and is working relentlessly to ensure that it has a role in defining the future of cyberspace. Tomorrow's digital trade and the flow of bits and bytes may well be very different from the model envisaged by the creators of the internet.

In the first half of 2017, China announced its ambitious blueprint to connect Asia through a series of rail, road, port and energy infrastructure projects. Even before that, it was already at an advanced stage of being a key player in the manufacture of global digital goods. According to McKinsey, China is the world's largest e-commerce market, accounting for more than 40 percent of the value of e-commerce transactions worldwide. Mobile payments in China amount to approximately 50 times that of the US, fuelled by the widespread adoption of e-wallets across its cities. One in three of the world's 262 unicorns are Chinese, making up 43 percent of the global value of these companies. In 2015, the Chinese government signed off on its "Made in China 2025" and "Internet Plus" initiatives that aim to digitise China's economy by integrating artificial intelligence, robotics, and digital services into manufacturing processes.

As part of its efforts to take the lead in the digital arena, China is making it clear that the retreat of the Atlantic powers will be complemented by Chinese propositions on digital commons. A March 2015 white paper setting out the vision for the Belt and Road Initiative (BRI) called for growth in digital trade and the expansion of communications networks to develop "an information silk road." State-owned Chinese telecommunication companies are increasingly investing in Asian countries to develop digital infrastructure; even private players like ZTE are investing in fiber optic cables in countries like Afghanistan.

In 2016, China released its first ever "National Cyberspace Security Strategy" to set out its positions on cyberspace development and security. Interestingly, the strategy sees cyber security as "the nation's new territory for sovereignty." At the 2016 World Internet Conference in Wuzhen, President Xi Jingping declared, "We should respect the right of individual countries to independently choose their own path of cyberspace development, model of cyberspace regulation and Internet public policies."

In characterising the internet as a fundamental domain of state control, China is challenging the long-held assumptions and principles that have governed the internet and have allowed it to proliferate over the past few decades.

The US' apparent withdrawal from international engagement in cyberspace and China's economic and political advance may well rewrite the rules of digital trade and openness in ways not envisaged by the internet's inventors. Neither of these two actors, however, will unilaterally script this new story, given that the effects of digital networks in economic and social activity are now widespread and diffused. From the very beginning, the evolution of technology has defied prediction and delineation. As it becomes more ingrained in human life, technology itself will rewrite traditional notions of ethics and social contract. This new 'machine conscience' will result in fresh challenges for policymakers and technologists alike.

The rapid pace of innovation in AI is heralding a world that is keen on moving from governing through data to being governed by data. While these developments will have transformational effects on the economy, they will also challenge the basis of human autonomy and ethics. Hillary Clinton's reliance on algorithmic decision-making during the US presidential elections has already offered us a glimpse into the inherent weaknesses of this new paradigm. As algorithms pervade every aspect of people's lives, they will determine most personal choices. However, it is worrying that these developments are taking place at a time when it is still unclear how machines will replicate the social values and norms that

human beings instinctively understand. This fear has prompted a fierce debate over the regulation of autonomous weapons, which are designed to be capable of making life-and-death decisions. Today, speculation is rife on what the future will look like when people's decisions are, as one commentator put it, "more mathematical than inspirational."

A future that is scripted through code, and not norms, may be cause for concern. As Vidisha Mishra and Madhulika Srikumar caution in 'Gender bias in artificial intelligence', algorithms written by humans should not reflect human biases and inequities. Instead, technology should be developed to empower, engage and enlighten. In 'Vulnerability, dependency, and profitability in a digital universe', Urvashi Aneja writes that people's ever-increasing dependency on technology seems "unwise", given the vulnerability of information infrastructures.

As the incumbent powers grapple with the changing dynamics of technology, emerging economies are gearing up to leverage it for the next billion users. Regulators are tackling the challenge of improving connectivity to harness the transformative potential of the internet. In 'The Importance of the open internet in driving internet adoption and growth', Michael Khoo and Peter Lovelock argue that governments in Asia need to ensure favourable market conditions and foster an open-internet environment that is non-discriminatory, neutral, and accessible. Similarly, Amelia Andersdotter, in 'Has the time come for less red-tape in Indian telecom?', looks at the role of regulation in facilitating adoption. The piece describes the introduction (and eventual removal) of licence and registration requirements for public WiFi in Italy and the lessons that India might learn from that strategy.

In this respect, a parallel transformation that is equally significant is India's digital payments explosion. Digital transactions in India have quadrupled in the past year, spurred in part by the demonetisation of 86 percent the country's currency and, in part, from the impetus provided by the Aadhaar initiative. The Aadhaar platform that sought to increase access and assist in the provision of subsidies has mass-sourced efficiencies, cut down the cost of transacting online, and moved bigger populations into the mainstream, formal economy than any other policy in recent history.

The success in the adoption of the Aadhaar ecosystem can serve as a model for other emerging economies struggling with efficient delivery of services. Coupled with open application programming interface layers that allow private companies to utilise its biometric database in a secure manner, the Aadhaar ecosystem offers a unique model that has the potential to catalyse growth and innovation in digital economies around the world.

In turn, these developments have had the cascading effect of strengthening civil liberties and improving the security of cyberspace. In August this year, a nine-judge bench of the Indian Supreme Court unanimously ruled that privacy is a fundamental right under the Constitution, harmonising over 60 years of conflicting pronouncements and granting the strongest possible protections to people's right to privacy. In fact, the Court has made specific references to informational privacy and the need to complement the right to privacy with strong data protection laws.

The Indian government, for its part, has established a 10-member expert committee to review existing data protection rules. These recommendations—likely to be tabled in the parliament later this year—can have the effect of modernising privacy protections and bringing them in line with international standards.

Governments in emerging economies should now go a step forward and make significant investments in newer technologies to give an additional spurt to their governance mechanism. Blockchain is one such technology. Originally seen as a financial innovation, blockchain's potential is now being recognised in a wide array of industries such as land rights, defence, art, precious jewels, and music. This technology has the potential to address even more complex issues such as checking the proliferation of nuclear stockpiles. In 'Licence in chains: Could media content be licensed through blockchains?', Meghna Bal explores how this innovation could be used to facilitate a more transparent licensing scheme for artistic copyrights, allowing the industry to manage the challenges that come with large copyright societies.

In 'Challenges for a new economy: the Fourth Industrial Revolution', Logan Finucan describes how the so-called "Fourth Industrial Revolution" (4IR) will bring significant progress in

productivity, such as in the use of advanced robotics and manufacturing techniques, the Internet of Things (IoT) and machine-to-machine (M2M) connections on a massive scale, autonomous vehicles, and new industrial materials, all powered by artificial intelligence (AI) and pervasive big data analytics. Meanwhile, in 'Applications and policy considerations for AI in cyber security and public services', Ryan Johnson and Seha Yatim ponder the question of how to manage the complex interrelationships between these new technologies, as well as the disruption they are likely to cause.

As economies increasingly rely on new technologies, it will be critical for them to ensure the stability of cyberspace and the integrity of their networks. This will require cross-sectoral cooperation – including that with the private sector – fostered by mutual trust. Three contributions in this volume ponder the issues related to the interaction between the private and public spheres in administering security over the internet. Chelsey Slack, in 'Tempering national and international tensions in cyberspace',provides an outline of the global discourse on security in cyberspace and highlights the need for cooperation among different actors. In 'The hybridisation of cyber security governance', Dennis Broeders identifies the emergence of cyber security assemblages – made up of government agencies, transnational corporations and cyber security companies. Finally, Nikolas Ott and Hugo Zylberberg argue in 'Addressing international security challenges while avoiding internet fragmentation' for interoperable policy regulations.

In addition to cyber stability, an equally important task for states would be to manage the "real-world" effects of new technologies, which spill into offline considerations of security and prosperity. Technology is in the process of rewriting the nature of the relationship between individuals, states and businesses. Machine learning and AI will question dominant models of labour, economics and social stability. However, these very technologies have the capacity to usher in unprecedented innovation, growth and progress. As the next billion internet users emerge from Asia and Africa, governments around the world should explore technological solutions to expand the scope and effectiveness of their governance. But as the presidential elections in the United States and the rise of China indicate, there is enough evidence to guard against any positive and deterministic outcomes from technology. It is likely that new innovations are going to be political and politicised: no longer can evangelists sitting in the comfort of their offices in Silicon Valley claim to be neutral vendors of technology, selling their products for the public good. As technological effects on offline realities become more prominent, state and non-state actors must be mindful of the effects of such rapid change on social structures. While technology can, and does, magnify existing faultlines between peoples and nations, it also offers a fleeting glimpse of greater harmony between humans, machines and states. The rules that will determine the nature of this relationship are still being written. The responsibility of all stakeholders is to ensure that new technologies do not lead to the creation of a world order that is haunted by the conflicts of the past, but rather of a new social contract that abandons the shackles of inequity and promises peace and progress.

INFORMATION SECURITY

01. **Reconsidering Cyber Security: Content, Context, and Critical National Infrastructure**

Elina Noor

For a time, it seemed that despite overlaps, cyber security and information security were set to traverse parallel paths in the stratosphere of policy discussions, never to converge. Securing critical national infrastructure (CNI)—as well as the computers, networks, and processes running them—against hacks and attacks in order to prevent a financial meltdown or worse, kinetic damage or destruction, became a priority point in nearly all the world's capitals. From Tokyo to Tallinn, the White House to Whitehall, political leaders, bureaucrats, and policy wonks were unanimous that a nation's assets and interests had to be protected and defended in cyberspace even as they disagreed on how it should be done.[1]

In less unison, and made at varying volumes, were calls to protect and defend information from unauthorised access, use, manipulation and abuse. These calls usually came from technical experts. But they also came from officials who understood that the value of information is only as good as the confidentiality, integrity and trust underpinning that information and the systems running it.

A number of states have proven acutely aware of the importance of information and its communication. Done right, information serves a range of domestic purposes: from preserving social cohesion and preventing/countering radicalisation to, more implicitly, maintaining political stability and continuity. But information can also mislead, subvert and undermine.

In Asia—where nation-building narratives are still unfolding—governments have long recognised the power and potential of information to shape conversations, with and amongst diverse communities. In developing states, nascent and maturing democracies, and countries that still bear the scars of post-colonial division, the opportunities and challenges of online narratives among multicultural societies in particular are often overlooked and underappreciated. Indonesia, for instance, has about 14,000 islands and its population of 250 million comprise roughly 360 ethnic groups speaking over 700 languages and dialects. The Philippines, meanwhile, has approximately 7,000 islands and 100 million citizens subsuming 70 ethnic groups living in the country's highlands and lowlands. Malaysia's landmass is cleaved by the South China Sea with 32-42 ethnic groups in Sabah, the country's easternmost state on the island of Borneo. Myanmar officially recognises 135 ethnic groups, and Laos, with its population of under 10 million, has 49 distinct ethnic groups, making it the most diverse country in South East Asia on a per capita basis. The task of building a shared national identity in nearly each of the South East Asian states is complex enough on its own but is made even more challenging by development imperatives and technological disruptions (both positive and negative).

For all these countries, the preservation of sociopolitical stability is crucial to the growth of the economic pie. Societies that have been riven by communal or ideological tensions are particularly vulnerable to the spread of polarising (mis)information and, in the age of the internet, the speed, magnification and multiplication of its dissemination. If radio proved a major vector of incitement in the initiation of the Rwandan genocide, the instantaneity of the internet could arguably exacerbate what Paul Brass, who has written extensively about communal relations and violence in India, calls an "institutionalised riot system."[2] In a region as diverse as Southeast Asia, with competing communal and national narratives, cyberspace has emerged as an especially contested domain, given its reach and accessibility.

As narratives jostle for profile, often the most sensational ones push through to prominence above the rest.

This opportunity for exposure has not been lost on extremists. In recent times, maritime South East Asia, especially, has had to deal with the challenge of online radicalisation. Content pushed through social media and messaging applications is testing even the most seasoned of authorities in these countries with decades of experience countering radicalisation and violent extremism by ideologues of all stripes. The threat is not entirely new, of course. Since the early 2000s, countries such as the Philippines, Thailand and Indonesia have seen an evolution in web outreach by domestic extremist groups from text-heavy material to the incorporation of multimedia and visuals. Now, authorities have to catch up to extremists' diversification to social media as the attention span among a younger audience grows increasingly shorter. In Malaysia, 75 percent of detainees arrested for terrorism-related activities as of May 2015 were radicalised online through social media.[3]

The phenomenon raises the question, of course, of how governments should manage the spread of online radical propaganda without unduly restricting civil liberties. As the ultimate arbiter of national security, governments have a role in monitoring this space for threats. Less certain is how and to what extent governments alone should be exercising that role.

Governments are keenly aware of the sway of information on their own political appeal or viability, some perhaps more than others. Long before "fake news" became a term of art, presidential pronouncement, or a hashtag, Malaysia had "surat layang" or anonymous poison-pen letters composed and spread to defame and unseat political personalities.[4] These letters were usually written by citizens themselves so the implications of these offences, if any, were confined domestically.

The stakes were exponentially raised, however, once allegations of foreign hacking, disinformation and electoral interference clouded the 2016 US presidential elections.[5] Quite apart from the fact that cyberspace was simply a new means for an established and widespread practice of electoral interference by major powers around the world,[6] the development brought to bear difficult international legal questions about attribution, evidentiary requirements, and recourse to action where operations in cyberspace fall below the threshold of physical damage, destruction or death.

For smaller, developing states—some of which themselves experienced electoral interference by foreign powers in the past—the turn of attention to information (in)security in cyberspace was both welcomed and viewed with caution. If before, a focus on content and its potentially destabilising effect on society was censured as censorship, and political obtrusion dismissed, it seemed now that the United States might empathise with both matters. At the same time, it also raised concern about what sort of expectations would be imposed in the future, on less developed states caught in the crosshairs.

Attribution remains problematic on at least three levels: technical, where the source of attack has to be traced and identified; political, where the author and executioner of the act may need to be profiled and her/his intention assessed according to the political climate in place; and legal, where the relationship between the actor and the state needs to be determined.[7] These criteria are often inconclusively satisfied for technologically advanced countries, let alone developing ones, but they are rendered even more daunting in the face of unsettled law.

Debate abounds, for example, on whether the burden of proof should be reversed with cyber operations because of difficulties with attribution.[8] The onus, the argument goes, should be on the accused state to prove that the cyber activity did not originate from its territory or infrastructure located within its jurisdiction. However, the traditional, mainstream approach of the burden of proof being on the complaining state seems to prevail for the present. The situation is more complex in cyberspace because cyber operations may originate not just from one territorial jurisdiction but many.

There is also no clear standard of proof for below-the-threshold cyber activity and analogies are borrowed from existing international law on state responsibility, criminal command responsibility, and the civil law test of balance of probabilities. Further, the law on the method of proof with regard to cyber operations is still nascent. While the International

Court of Justice seems to prefer the submission of official documentary evidence, this will likely not always be possible because the disclosure of such may compel states to reveal classified technological systems or data.[9] The ambiguities in the law and the differing levels of competency and capability among various states mean that there are opportunities for cooperation and exchange in the areas of law, policy and doctrine development.

Of larger import is the convergence between cyber security, narrowly defined, and information security that the events of 2016 catalysed. The immediate question is whether electoral systems count as CNI, triggering the observance of norms and the application of international law, as appropriate, in cyberspace. This is a legitimate and substantial consideration for democratic countries with electoral mechanisms because it impacts the political foundation of those states and public trust in the systems that enable it. However, this approach obviously favours only one political system.

There is nothing to stop an absolute monarchy or a Communist party system from declaring its own political foundation as unassailable and part of its CNI. In general diplomatic and international legal parlance, this is known as the principle of non-intervention, which states recognise through the precepts of sovereignty and territorial integrity. Given that every state has the prerogative to define its own CNI and not all governments are democratically elected, it may well be worth broadening the discussion of redefining CNI to include political systems writ large rather than only electoral systems. This may, no doubt, be unpopular in its presumption that there are non-democratic systems worth defending but the suggestion does, at least, merit a discussion. Not affording it would be ironically non-democratic and hypocritical.

02. **Hacking Democracy**

Sean Kanuck

Introduction

Cyber conflict as it pertains to the manipulation and/or compromise of democratic institutions–both directly and indirectly–has come of age. Academic speculation about hypothetical methods and objectives must yield to serious and pragmatic policy discourse. Direct intervention in a democratic election can comprise either public efforts to obstruct voters or else clandestine alteration of actual vote tabulations; indirect influence can consist of using proxy voices or inducing political, economic or media events with secondary impacts on voter turnout and election results. (See Figure 1). Manipulative actions that do not directly alter the voting process or results are to be considered "influence operations", while actual changes to voting rosters (including threats of violence or other means to physically deter eligible voters from attending the polls) or the ballots that are cast are typically deemed illegal "voter fraud", even when perpetrated by the state apparatus itself.

Information communication technologies (ICT) present many new vectors for potentially interfering with democratic elections. Foreign competitors, traditionally offset by geography, can now impose themselves on domestic political systems anywhere in the world. Social media platforms enable individuals or special interest groups to broadcast their policy positions at little or no cost and even to strategically misrepresent broader support for those positions. Internet-connected ICT networks are highly susceptible to unauthorised access, thereby rendering sensitive data vulnerable to theft and public release. In essence, the digital future–and liberal democratic processes that will rely upon it–is susceptible to interference and disruption.

Figure 1: Examples of Methodologies for Manipulation of Democratic Elections

	DIRECT INTERVENTION	INDIRECT INFLUENCE
OVERT	Intimidating or deliberately misinforming voters to deter turnout. For example, unofficial "robocalls" used during the 2011 federal elections in Canada to falsely claim changes to polling station locations.[1]	Public campaign donations and/or speeches by non-candidates in support of specific ballot choices. For example, President Barack Obama's 2016 speech in London opposing "Brexit" before that referendum.[2]
COVERT	Secretly altering the election results to favor a specific candidate. For example, the historical allegations regarding Lucien Bonaparte's inflation of voting results in the French constitutional plebiscite of 1800.[3]	Clandestine, third-party activity intended to increase or decrease support for specific candidates. For example, reputed Russian espionage and public dissemination of materials during the 2016 US presidential campaign.[4]

Historical Precedent

When evaluating the impact of cyber modalities (i.e., ICT) on democratic institutions, one must first consider what is genuinely new in either the objectives or possible impacts. Regardless of which quadrant of Figure 1 is of concern, there is ample historical precedent from geopolitics. Thucydides recounted Athenian efforts to lobby the magistrates of Melos to capitulate without battle (i.e., indirect and overt influence).[5] Similarly, *Radio Free Europe* and *Voice of America* were designed to provide the electorates of foreign polities with information that was otherwise unavailable and/or forbidden. Nor is history want for allegations of ballot-box stuffing (i.e., direct and covert intervention) or voter intimidation (i.e., direct and overt intervention). Digital manifestations of those forms of fraud are certainly illegal and deserving of policy attention, but they are not the focus of recent debate. What seems to capture the current imagination and concern is the heightened

opportunity for indirect, covert influence through cyber means. Careful analysis is required, however, to properly assess the nature and foundation of that concern.

If one reasonably acknowledges that foreign efforts to influence elections are as old as elections themselves, then one is left with either (i) a theoretical objection that is so counterfactual to historical practice that it is relegated to pure academic consideration, or (ii) a practical objection that employing a new technological means to an old political end is somehow unacceptable. It is worth recalling that public international law does not expressly outlaw espionage, which is merely accepted as a feature of international relations. Nor is the publication and dissemination of political opinions generally deemed objectionable in liberal democracies. So what is really at issue here? What is so new and inherently objectionable about digital influence campaigns compared to pamphleteering or foreign radio broadcasts that transcend sovereign borders?

By way of example, several former US intelligence officials have stated that they considered the theft of Office of Personnel Management (OPM) records to be a "legitimate" foreign intelligence target.[6] But even so, US government officials have said that the scale and import of that espionage crossed a line that was unacceptable. It would thus seem that the objection stems from the quantitative scope of the activity in question (e.g., the sheer number of records compromised, the gross imbalance between the cost of conducting the activity versus its harm to the victim, and the possible stand-off distance from which such an operation can be conducted without personal risk), rather than the qualitative nature of the activity itself (e.g., the theft of private information, the type of data targeted). Chivalric objections to the crossbow and guerilla warfare tactics should immediately come to mind, for new methods of conflict are often too efficacious for the establishment to accept at the outset.

There is no doubt that if one were sitting in the British Parliament in the latter half of the 18th century, then a certain group of colonials self-publishing and distributing pamphlets that advocated armed secession would have been deemed "terrorists" by today's standards. Some of those same "founding fathers" would even eventually publish the Federalist Papers under the pseudonym "Publius" that sought to imply broader support for their political positions, which is not terribly dissimilar to modern-day "astroturfing" on social media.[7] And the American Revolution is but one example, for the House of Bourbon would have had analogous views of the violent Jacobin upstarts. History is kind to the victors, and ruling elites always question the legitimacy and legality of challengers. How then shall democracies balance the rule of law with freedom of expression in the internet age?

When does a quantitative improvement in espionage constitute an unacceptable qualitative change? Do recent offensive cyber advances constitute a qualitative threat to democracy? These are indeed difficult queries. The only useful, historical metaphor that strikes this author is the large-scale expulsion of Soviet Bloc "diplomats"—who were suspected of espionage—from London in the 1970s.[8] The British Security Service (aka MI-5) simply did not have adequate personnel to effectively surveil all of those individuals, thereby requiring a reset of the acceptable parameters for Cold War human intelligence. As with the OPM hack, that policy decision reflected a purely practical objection based on quantitative versus qualitative standards.

Protected Infrastructure

The US Department of Homeland Security did not officially designate election systems as a critical infrastructure until January 2017.[9] Yet, almost four years earlier in March 2013, the US Director of National Intelligence (DNI) had identified an important incongruity related to how different nation states view online media and their political systems:

> "Online information control is a key issue among the United States and other actors. However, some countries, including Russia, China, and Iran, focus on 'cyber influence' and the risk that Internet content might contribute to political instability and regime change. The United States focuses on cyber security and the risks to the reliability and integrity of our networks and systems. This is a fundamental difference in how we define cyber threats."[10]

That fundamental difference (i.e., the underlying distinction between infrastructure and content) is also germane to the question of which ICT deserve protection as "democratic institutions". Most everyone would likely agree that public authorities must guarantee the security of polling stations, voting machines and official election returns. In other words, they are expected to prevent direct intervention that is contrary to the rule of law. This is represented by the US' "infrastructure-centric" view of cyber security that was highlighted by the DNI. Content poses a much more complicated challenge.

The discussion about where to draw the line regarding indirect influence quickly becomes muddied, as can be regularly seen with proposals for campaign finance reform. Managing the impact of informational content pits two democratic values against one another: freedom and equality. There has always been political disagreement about how much leverage freedom of expression should permit wealthy individuals and companies to exert on democratic processes. Today, we must also ask ourselves whether every mass media outlet or social media platform should receive a critical infrastructure designation simply because it can be utilised to influence public opinion (See Figure 2). Is the national government responsible for ensuring the confidentiality, availability and integrity of all resources that can influence a democratic electorate? If not, then why not? The decision regarding which entities are "entitled" to special protections and/or restrictions has become a genuine public policy dilemma.

Figure 2: Examples of Civilian Infrastructures that Impact Democratic Elections

	VOTING SYSTEMS	INFORMATION RESOURCES
PUBLIC	Government-administered polling stations and officially monitored vote tabulation. Susceptible to corruption by ruling party.	National television, radio, print and online media outlets. Subject to selective coverage and preferential treatment by ruling party.
PRIVATE	Hardware and software for voting systems and registration databases developed by commercial companies. Susceptible to supply chain and/or remote penetrations.	Independent mass media and online social media platforms. Subject to censorship by government as well as disruption and/or manipulation by third parties.

For example, the status of political parties and their proprietary resources raises difficult legal questions. If the compromise of an entity such as the Democratic National Committee or the Republican National Committee in the US is deemed a national security concern, then what level of governmental oversight and regulation of (i.e. access to) that party's ICT networks is appropriate in the national interest? Does that level change depending on whether that party is currently in power? Should smaller political parties be exempt from such regulation if they are not likely targets for foreign intervention? Once again, these cyber challenges are pitting core democratic values against one another—privacy versus national security—and policy trade-offs are inevitable.

Social media represents a uniquely influential and vulnerable feature of modern politics. Its impact during the Arab Spring was noted by governments and demonstrators alike around the world. Since then, the use and manipulation of social media has become an instrumental part of political campaigns, opposition movements and foreign influence operations. It is possible, at least to a certain degree, to reveal such social media manipulation, for instance, by technically determining the provenance of posted information, detecting automated programs for "re-tweeting" and "liking" posted information, and identifying patterns of coordinated "trolling." That requires, however, analysis of large tranches of proprietary data, including both content and technical metadata. In democratic societies, private ICT companies have no ex ante obligation to make their databases available to government authorities for speculative research. When, if ever, should private data be treated as a national asset, even against the will of its owner?

Data Integrity

Many forms of media have been used to spread both information and disinformation for political or economic effect (See Figure 3). History is certainly replete with examples of

interest groups "marketing" their views to the public–such as the US founding fathers' ascription of the moniker "Anti-Federalists" to their opponents to impute a negative connotation–but social media and other internet platforms present a new challenge, whereby they host content that is neither of their own creation nor necessarily attributable to physically identifiable third-parties. Accordingly, they become enablers for all sorts of online activities that can either foster or undermine democratic institutions. That schizophrenia is perhaps best characterised by the hacker consortium, Anonymous, which has both thwarted sovereign governments and also publicised child pornographers and corporate fraud to supplement law enforcement.[11] Is the "common carrier" model, which is ambivalent towards content, the right legal analogy for internet service providers and social media outlets?

All of the themes aforementioned in this article—espionage, privacy, influence operations, quantitative change, qualitative distinctions, public versus private infrastructure, freedom of expression, national security—coalesce around the key issue of data integrity. Because democracies rely on the ability of their populaces to make informed decisions, increased dependence on insecure ICT poses considerable threats. But how can the public ever differentiate truth from falsehood with certainty?

Figure 3: Examples of Information Propagation to Induce Political or Economic Behaviour

	INTENTIONAL MESSAGING	UNWITTING EXPLOITATION
INFORM	The 2007 airborne delivery of leaflets over Afghanistan by the US military in order to deter insurgent activity by the Taliban.[12]	In 2016, Twitter suspended thousands of suspected terrorist accounts that promoted violence and/or spread propaganda.[13]
DECEIVE	(1) Adoption of the title "Bolshevik" (i.e. "one of the majority") by a party faction that was numerically inferior.[14] (2) The ironic naming of "Greenland" by Erik the Red to encourage emigration to a new colony that was less temperate.[15]	(1) The Syrian Electronic Army's false "tweet" disseminated from the Associated Press's Twitter account in 2013, which led to temporary fluctuations in US stock markets.[16] (2) False news items posted on Facebook during the 2016 US presidential campaign.[17]

International humanitarian law (aka the law on armed conflict) struggles with a similar conundrum when it distinguishes between perfidy (i.e., the illegal intent to betray confidence) and ruses of war (i.e., permissible deceptions not based on garnering false status).[18] Interestingly though, "misinformation" is listed as a ruse vice perfidy; moreover, the relevant treaty distinctions explicitly do not "affect the existing generally recognized rules of international law applicable to espionage."[19] Thus, cyber operations premised on exerting indirect influence are particularly problematic, especially when they only reveal true information. Can two "rights" make a "wrong"? That is, should espionage (which is accepted in international relations) that exposes the truth (a core democratic value) be prohibited?

Ultimately, the most nefarious threat to democratic institutions is the corruption of the integrity of information. The pervasive introduction of false data into mainstream media could erode public confidence and destabilise society. That is, of course, exactly what authoritarian regimes are (i) highly concerned about happening to themselves and (ii) well-practiced in perpetrating against their adversaries. Yet, democracies pride themselves on permitting their citizens to hold and publicise contrarian (or even counterfactual) opinions, and modern ICT permit foreign voices to participate in domestic dialogues.

It seems then that the most conceptually disturbing challenge for democratic institutions is digital, highly efficient, indirect, foreign, misinformation campaigns that can neither be prevented nor easily identified. Furthermore, it is unclear what kind of government institutions (domestic or international) and/or private-sector initiatives could resolve that difficulty, for this seemingly new cyber concern tautologically reduces to the well-known game theory paradox of "who guards the guardians"?

Outlook

Democracy faces a significant challenge ahead. Whether the government and media institutions upon which it relies, can weather the imminent onslaught of influence operations – including ones that disseminate falsified content indistinguishable from the truth by average persons–remains to be seen. Developing nations, India in particular, have deeply considered the trilemma of access, security and human rights. All three are desired qualities, yet there appear to be implicit trade-offs between those values in the online environment. How does a government afford its populace the political and economic benefits of the global internet without sacrificing national security and regime stability?

One intriguing development is the potential return to direct democracy. The possibility of Internet referenda have opened the door to direct democracy in a way that has not been feasible since the citizens of a city-state could all convene in their agora. Is the world on the cusp of witnessing the waning of Burkean representative democracy, either in fact or at least in principle? Will elected representatives behold themselves to the popular will of their constituents, which can be now be theoretically measured in real time on every issue up for a legislative vote? Will the desire for re-election hold sway over the exercise of political expertise? Of course, the concern is how to ensure the integrity of those online "plebiscites" that are neither officially sanctioned nor orchestrated by the government. They remain extremely vulnerable to foreign influence operations as well as direct intervention through cyber attacks.

A second matter of concern should be the security of online voting systems. While some countries, like Estonia, made the transition years ago, others have faced profound difficulties in implementing secure internet-based voting. Even electronic vote tabulators in paper-ballot polling stations pose uncertainties. For example, in at least one state jurisdiction, ballots cast in the 2016 US federal election were recorded by machines that had been tested for accuracy with trial data sets rather than reverse engineering of the software. Unsurprisingly, those trial data sets consisted of fewer entries that the general election would require, and therefore, even a novice computer programmer could fathom a malicious subroutine that yielded accurate results when tested on an order less than a general election but provided false returns when processing data on the magnitude of the full electorate's ballots. How then does any properly registered voter who casts a ballot ever know that her vote is tabulated correctly in today's democratic elections? Are we to simply to trust the vendor's assurances?

This essay may appear to have come full circle after highlighting the dangers of indirect influence operations that compromise the integrity of media consumed by the electorate. But leitmotifs of uncertainty and vulnerability should resonate on a number of levels. Twentieth-century democracy prided itself on near-universal suffrage, monitored elections and secret ballots. But our desire to capitalise on the efficiencies of the digital economy and the machine age may be realised at the expense of big politics and new voices. The impact of technology and society may be best illustrated by asking how many millennials—whose political persuasions are most often easily deducible from their social media accounts—would prefer the opportunity to verify the tabulation of their personal votes over the secrecy of their ballot. Perhaps the world has merely reached another inflection point in the history of democracy.

DIGITAL ECONOMY

03. **Has the Time Come for Less Red-tape in Indian Telecom?**

Amelia Andersdotter

Introduction

In November 2016, the Telecommunications Regulatory Authority of India (TRAI) proposed a Model for Nation-wide Interoperable and Scalable Public Wi-Fi Networks.[1] The aim of TRAI was to facilitate, through standardisation, seamless authentication and payment for access to public Wi-Fi networks and further the agenda of Digital India.[2]

Affordable, accessible internet connectivity is an outstanding policy target in most of the world. It is widely accepted that an internet-enabled nation increases its opportunities for social, democratic, and economic development.[3] Still, efforts to enhance connectivity around the world with a view to strengthening human rights and economic development are dependent on the regulatory framework surrounding telecommunications in each of the countries where such efforts are being made.

This paper is a case study of licence requirements for public internet access facilities and mandatory user registration requirements for public Wi-Fi networks in Italy between 2005 and 2013, and the lessons the experience holds for India. It will cover why they were introduced and the factors that led to their ultimate removal.

Italy is an interesting case study because of the way security measures were rolled back due to their perceived harmful impact on business and internet user rights. The Italian campaign to remove mandatory user registration requirements in the public Wi-Fi network sector was advanced by small business and municipal network roll-out concerns. Italian membership in the European Union (EU) allowed activists and campaigners to use data from other EU member states to underline how the registration policy had led to detrimental effects on Italy in comparison with allied nations. The case study, therefore, provides useful lessons to activists and campaigners on how to invoke the competitive advantage of nations when addressing technology policy concerns that may have an impact on human rights, such as mandatory user registration.

In India the situation is clearly different from that of Italy. TRAI has recognised the need to integrate small-and medium-size businesses, as well as local and regional councils, into the efforts to deploy public Wi-Fi networks with a view to increasing general access to connectivity.[4] But India is a leading economy in its part of the world, unlike Italy, which is part of the EU and economically similar to many of its collaborating partners. In spite of similar problems in the two countries with domestic violent disturbances—Italy was rocked by terror strikes in the 1960s and 1970s, while India faced states of emergency due to wars—it is also clear that Italy entered the telecommunications liberalisation period of the 1990s in a much more industrialised state than did India. The Italian case study can only provide pointers to human rights campaigners on how to find synergies between human rights interests and economic interests.

The Origins of Registration Requirements

In the early days of telecommunications, access to telephony was bound to individual houses. The business model was post-paid subscriptions and each private subscriber needed to be identifiable at her or his residence for billing purposes.

With mobile telephony it became possible for end-consumers to access telephony without having a monthly subscription fee. Prepaid rentals have been a particularly successful

business model in the Global South, where many households cannot afford the financial burden of a monthly subscription fee.[5] As the end-consumer pays their dues to the mobile operator before enjoying the services, the operator does not need to collect billing information. Registration requirements are meant to ensure that a given subscriber can be tied to a specific person or address, irrespective of the operators' need to bill that subscriber. Registration requirements are assumed to deter criminal activities and assist the police during the investigation of crimes.[6]

The Efficiency of Registration Requirements

Little evidence exists to show that registration requirements contribute to a drop in crime.[7] In India, there is anecdotal evidence that the tracking of IP addresses has been helpful in bringing wrongdoers to justice,[8] but it is less clear that registration requirements were helpful in these cases. The same is true globally.[9] In Mexico, registration requirements for prepaid rentals were discontinued after an evaluation showed that crime increased, rather than decreased, after registration requirements were introduced.[10]

From the business perspective, it has been shown that registration requirements for SIM cards depress mobile penetration in developing countries in the short term.[11] A comparison of EU countries listed by the GSM Association as having introduced mandatory user registration requirements in 2013 with data on the general competitiveness of the mobile market (see, for example, DFMonitor.eu) indicates that countries with stronger mobile competition are less likely to have introduced registration requirements.[12]

The risk of administrative burdens on commercial and non-commercial providers of services decreasing providers' abilities to launch services has been observed in India as well. Leading industry bodies such as the Internet Service Providers Association of India (ISPAI),[13] Association of Unified Telecom Services Providers of India (AUSPI),[14] and Internet and Mobile Association of India (IAMAI)[15] all said so in their responses at the November 2016 consultation on public Wi-Fi networks organised by TRAI.[16]

The above discussion provides a setting for understanding mandatory user registration requirements in mobile networks and their efficacy in the fight against organised crime and terrorism. The following section describes the case of Italy in this context.

The Case of Italy

Not even a month after the 7 July 2005 bombings in London, Italy imposed registration requirements on public Wi-Fi networks.

It seemed at the time an insignificant addition to the already existing anti-terrorism framework. Between 1969 and 1982, some 2,712 terrorist acts had been recorded and 351 individuals murdered by terrorists in Italy,[17] the most infamous case being the killing of Aldo Moro, former prime minister, in 1978. In response to these early threats against the Italian state, the country had broadly expanded investigatory powers, introducing surveillance powers and prioritising the continued existence of the state over other considerations. After the attack on the Twin Towers in New York on 11 September 2001, support for extensive police powers was re-affirmed in the national parliament.[18]

However, the registration requirements of 2005 raised many objections that had not been envisaged by the legislators. There were, of course, privacy objections: it would make anonymous, or at least private, enablement of connectivity impossible. But there were also economic objections: it was said that the requirements would hold back economic development.

The 2005 decree required every provider of access to computer terminals, such as an internet cafe to register with local authorities and collect identity information on all users.[19] Libraries, schools and Wi-Fi providers were not required to obtain licences, but had to ensure proper identification of all users.[20] Further, the decree mandated that identification be performed through inspection of state-issued ID cards and that data thus recorded be stored in accordance with applicable data protection laws for a period of one year.[21] Other forms of verification, such as by SMS, were later approved by the responsible ministry, but doubts over the literal wording of the law caused providers to not rely upon such alternative

identification verification mechanisms.[22] Concerns were also raised that SMS verification, in spite of being a lighter identity verification regime than state-issued ID cards, would exclude tourists; this posed a problem for a country with a large tourism industry.[23]

In addition to these concerns, the telecommunications sector in the EU had undergone liberalisation in the 1990s, bringing with it commercial challenges to Italian telecommunications operators and, in turn, pulling down their appetite for increasing administrative burdens. In Italy, the market transformed from having only one government owned operator, Telecom Italia, with 100 percent share of the market for telecommunications in 1997, to one where, by 2008, Telecom Italia's market share was down to 65 percent.[24] New market entrants were struggling to position themselves, while Telecom Italia was facing the problem of having to simultaneously downsize while staying on good terms with labour unions and the government.[25]

Liberalisation of the telecommunications sector in European countries also shifted the regulatory framework for the sector from the national level to the European level.[26] The European Commission started compiling data on market shares of previous monopolists in each of the member states, consumer ability to switch providers in case of dissatisfaction with the existing provider on each of the European markets, the number and market shares of new market entrants in each of the countries, as well as measurements of overall digital development of each member state.[27] The EU-level market analyses, including from the private sector,[28] contribute to institutional competition between member states. By comparing data from different states, one can argue that a specific EU member state is doing worse in terms of public Wi-Fi roll-out than other EU member states because of its institutional or legislative framework.[29] This is precisely what happened in Italy.

When the Italian decree was reviewed in 2010, the campaign Carta dei cento per il libero Wi-Fi [Charter of the Hundred for Free Wi-Fi][30] had figured out that Italy had only one-fifth as many Wi-Fi hotspots as France.[31] Italy was also lagging behind other large European economies such as Germany and Spain in Wi-Fi deployment. The Carta dei cento demonstrated that the registration decree had adversely affected Italy's capacity to compete and garnered support from private-sector parties, regional authorities interested in local Wi-Fi projects, as well as academics and journalists.

In December 2009, journalist Alessandro Gilioli found that even former Minister of Interior Affairs Giuseppe Pisanu, who was responsible for introducing the decree, had reconsidered its merits:"[On] the one hand, security needs have changed since the passage of the decree, and on the other, access to the internet and other benefits of technological development must be facilitated," Pisanu told Gilioli.[32]

Registration requirements were subsequently relaxed in 2011, in what was considered a major victory for public Wi-Fi access. Italian internet providers' association AIIP quickly launched a campaign to wirelessly connect Italy: Internet Chiama Italia [Internet Calls Italy].

However, closer scrutiny of the 2011 decree revealed insufficient legal clarity for Wi-Fi providers and investments in Italian public Wi-Fi networks remained small. Therefore, more laws were passed in 2013 to reinforce the Italian legislators' commitment to a lighter regulatory scheme. This second round of regulatory reforms had immediate positive effects on development of public country networks.[33] By the end of 2016, the number of public Wi-Fi hotspots in Italy had increased from 4,802 in 2009 to over 28,000.[34]

But in spite of these dramatic developments of Wi-Fi infrastructure following the removal of mandatory user registration requirements, Italy is still considered by the European Commission to be "catching up" with the rest of the EU on digital developments. While Wi-Fi contributes to the ubiquity of connectivity in places where fixed connectivity is already accessible, the slow pace of back-haul network roll-out in Italy continues to hold the country back. The country is still dependent on its copper/ADSL networks and has the second-least developed high-speed broadband network in the EU.[35]

Implications for India

In light of TRAI's hopes that "panchayats and local entrepreneurs [can] create Wi-Fi networks offering e-learning, e-governance, e-banking, e-health, and other online services to the

community,"[36] it seems pertinent to review registration requirements currently looming over public Wi-Fi providers, to see whether easing such requirements would improve the chances of realising such hopes. Notably, the Department of Telecommunications appears not to have made such an assessment in advance of passing its regulation on user authentication in 2009.[37]

In India, there is still legal uncertainty around licensing requirements for public Wi-Fi providers. In Italy, in spite of licensing of public Wi-Fi never having been mandatory, registration requirements alone were sufficient to hamper Wi-Fi deployment.

In many countries, registration requirements have been introduced under the assumption that user registration contributes efficiently to the fight against organised crime or terrorism. Evidence from countries that have evaluated registration requirements does not, however, support such assumptions. More than eight years since user authentication requirements were introduced for Wi-Fi networks in India, a reassessment of the Indian registration requirements seems appropriate. To evaluate whether the administrative burdens of registration requirements on businesses are indeed a worthwhile sacrifice, it is necessary to determine whether the requirements have led to either a real drop in crime or facilitated the bringing of more criminals to justice. Such an assessment should be carried out at all levels of government where law enforcement authorities exist.

The Italian case study should also encourage reflections on the necessity of core network investments. Public Wi-Fi increases access to connectivity only up to a point. Over longer distances, or to connect villages with the global internet, a strategy for developing backhaul networks is still necessary.

As opposed to Italy, where a comprehensive data protection framework has been in place for many decades, India is currently still discussing such a law for protecting personal data.[38] In the digital age, individuals are exposed to risks from unauthorised access, leak, or breach of their personal data. These risks include receiving threats, identity theft and payment fraud. Just recently, it was even observed that unforeseen dissemination of Indian identity data can have repercussions on national security.[39]

Conclusion

In its efforts to incentivise business and entrepreneurship, as well as build a sustainable and secure connected environment for the benefit of all Indian citizens, the Indian government should consider the following:

- Assessing the efficiency of the current mandatory user registration requirements for Wi-Fi and prepaid rentals with respect to law enforcement activities and crime rates, and the possibility of removing them with a view to strengthening locally based and small-or medium-sized domestic businesses.

- Clarifying that there is no intention of applying licensing requirements to public Wi-Fi networks.
- Developing a national strategy for increasing investments in backhaul networks and core networks.

- Continuing the efforts to introduce a privacy act, for the protection of individual citizens and their identity information in an increasingly insecure cyberspace.

As India becomes digitally empowered, it should ensure that its domestic business climate is such that smaller local actors have the capacity to enter the Wi-Fi market. One way of enabling a larger range of companies to participate in Indian infrastructure roll-out is to decrease "red-tape," namely, laws that impose administrative requirements in such a way that only larger companies are able to afford manoeuvring the legal landscape. The Italian case study serves as a cautionary tale, where security-through-administration needlessly held a nation back in its digital economic development.

04. **The Importance of the Open Internet in Driving Internet Adoption and Growth**

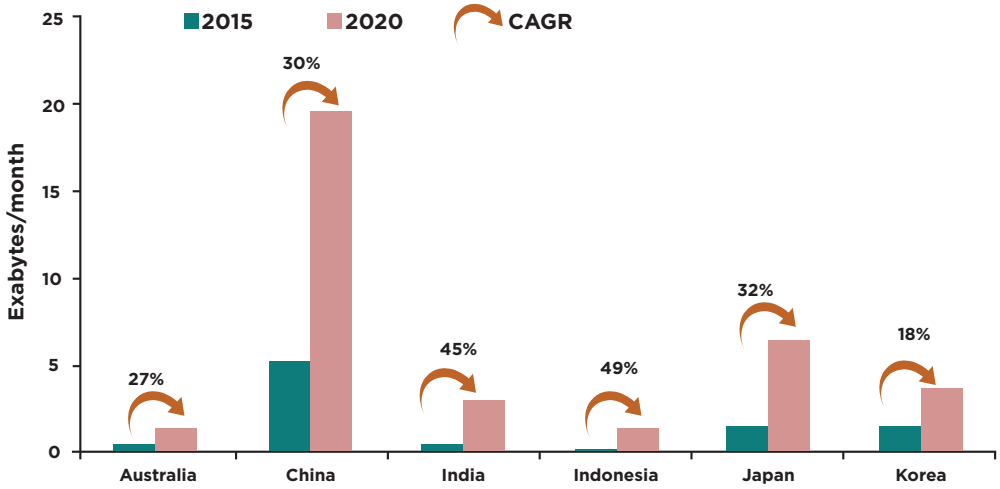
Michael Khoo and Peter Lovelock

The number of internet users and the volume of internet traffic is growing in Asia. But while the Asia-Pacific is leading globally in the absolute number of online users, 55 percent of the region's population is yet to be connected to the internet.[1] This trend must be reversed; Asian policymakers acknowledge the importance of the internet in terms of economic growth and social development. This is attested by the increasing number of national broadband plans and the inclusion of digital economy policy in their respective national development agendas.

While the number of internet users has been growing at a steady pace, internet traffic is surging at an exponential rate. New users are not only coming online, but they—together with existing users—are consuming more and more content and services, generating rapidly increasing data traffic volume. According to TeleGeography, between 2012 and 2016, the compound annual growth rate of broadband subscribers in Asia was 10 percent, while total broadband bandwidth grew by 29 percent. This bandwidth growth is primarily driven by a voracious appetite to consume more content in the form of information services, social media, online games and streaming video services.

In 2015, video content alone accounted for 65 percent of total consumer IP traffic in Asia, or 14,534 petabytes, figure that is forecast to rise to 82 percent by 2020.[2] India and Indonesia are showing some of the highest growth rates in internet video consumption, while in China around 91 percent of consumers already "binge watch" content, and over 50 percent watch more than two hours of video every day.

Figure 1: Internet Video Growth in the Asia-Pacific (2015 to 2020)



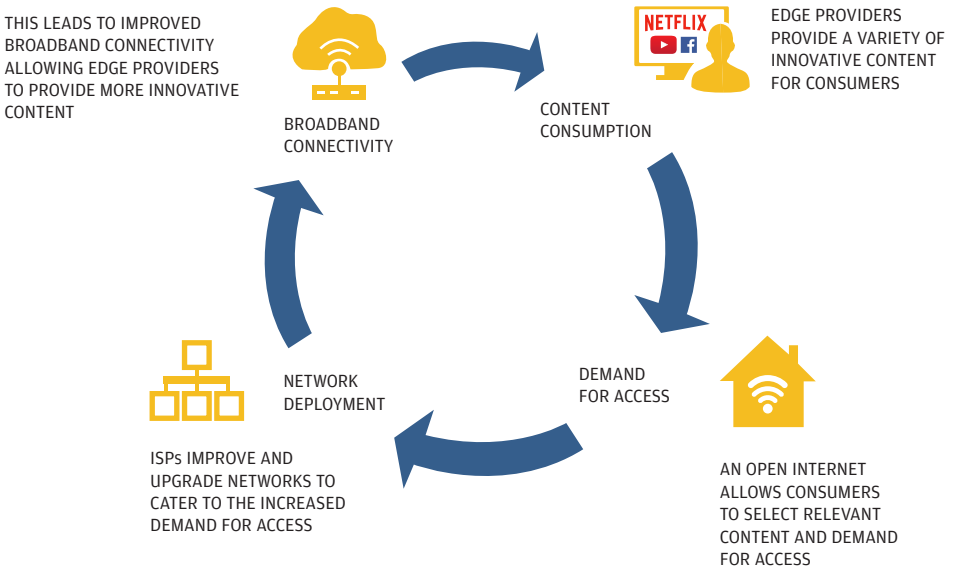
Source: TRPC analysis based on statistics from Cisco VNI reports

Low-cost smartphones and increasingly affordable mobile data services are the primary enablers of going online. Since in most Asian economies, the cost of personal computers remains prohibitive, these countries are less "mobile first" and more "mobile only." More importantly, issues of broadband accessibility and affordability persist, as well as questions in quality of service. These challenges can be addressed by encouraging greater competition in the telecommunications market, and by incentivising or mandating network providers to improve and expand their wired and wireless broadband infrastructure.

As regulators face the challenges of both improving connectivity and encouraging adoption, it is important that they foster an environment that allows for the free flow of content and services on the internet as these are the main drivers of broadband adoption.

The desire to access content and services creates further demand for broadband access and increased bandwidth. This prompts Internet Service Providers (ISPs) to invest in network deployment to provide better and faster networks. This, in turn, improves connectivity, enabling the further development of innovative content and services, driving consumer demand for access, and so on. The growth of this virtuous circle of consumption (demand) and investment (supply) depends on fostering an open internet — a level playing field where everyone has the same opportunities to participate and where markets are competitive, net neutrality principles are adopted, and internet connectivity is accessible and affordable.

Figure 2: The Virtuous Circle



Restrictions placed on the open internet can lead to unintended consequences, such as higher prices of content and connectivity, and more limited content availability. These could restrict adoption and usage, and artificially constrain the self-perpetuating momentum of the virtuous circle. This is not to argue that illegal and harmful content should be freely available but to say that the internet should remain non-discriminatory and allow consumers to freely choose and consume content of their choice.

To enable this virtuous circle of consumption, innovation and growth, governments in Asia need to ensure favourable market conditions and foster an open internet environment that is non-discriminatory, accessible and affordable.

How the Open Internet Can Drive Asia's Digital Growth

In many Asian economies, the rising demand for connectivity has not been accompanied by the deployment of sufficient broadband infrastructure capable of handling the upsurge in bandwidth. The challenge to provide faster and more robust connectivity for an increasing number of internet users has not been met by regulators and operators, who still attempt to manage the growth in demand using linear models, as opposed to planning for exponential growth in data usage.

Economies where broadband infrastructure deployment is able to keep pace with user demand tend to have more competitive and open telecommunications markets with better and more affordable access and increased adoption. Myanmar, for instance, opened up its telecommunications sector in 2013 to allow new foreign entrants to compete with local companies, and since then, mobile prices have fallen almost 200 percent with adoption rates rising from seven percent in 2012 to 90 percent in 2016. During the same period, the number of internet users grew from two million to 39 million, primarily accessing the internet through mobile phones.

However, even with competitive markets, less populated and less affluent remote and rural parts of Asia tend to remain underserved by providers, who are wary of not being able to realise a return on their investments. In such areas, policymakers can employ the use of universal service access funds to subsidise network rollouts. Thailand's government, for example, has announced that it will use the proceeds from spectrum auctions to fund a national broadband network for 70,000 villages. Similarly, the Malaysian government has implemented over 6,000 universal service provision projects for underserved areas and groups throughout the country.

Non-Discriminatory Access

An important principle of the open internet is non-discriminatory access. Zero-rating schemes, which offer subsidised data on certain applications or websites, are a good case in point. As zero-rated content and access are gaining popularity in Asia, policymakers need to ensure that such schemes are offered on a non-discriminatory basis. This provides a safeguard for the long-term benefits of competition and innovation from the perceived short-term benefits of discriminatory plans, such as higher adoption and usage.

In practice, a non-discriminatory zero-rating scheme might offer free data usage at certain hours or be open to all content providers within the same class. Non-discrimination ensures that all forms of content and services remain competitive and consumers are able to choose their providers. New or smaller edge providers are also able to compete based on the content and services they offer, rather than being left behind as they are unable to afford subsidised access channels.

Tools and Approaches for Good Network Management

Policymakers should enable and encourage the use of network management tools by ISPs and content providers to ensure a quality user experience. According to TeleGeography, the proportion of internet traffic in Asia originating from international sources has already been steadily declining throughout the last decade, in strong part due to network management techniques, such as local caching and neutral Internet Exchange Points (IXPs) in Asia. Caching has become the prevalent method for data delivery among large edge providers and ISPs. Through Content Delivery Networks (CDNs), traffic is localised as close as possible to end users, shortening the network and geographical distances that data bits have to travel. This benefits consumers, ISPs and internet users in general. It makes the internet more efficient and scalable to support requests for content.

Cached data can be distributed during low bandwidth periods and stored in CDNs. Small content companies can utilise regionally based CDNs to take advantage of the reduced latency and lower transit costs they offer. Open and settlement-free interconnections between ISPs and CDNs allow all content providers to compete on a more level playing field. An example is Netflix's Open Connect programme, which involves direct peering between Netflix and hundreds of large and small ISPs on settlement-free terms. By caching and pre-positioning content during off-peak hours, the ISPs minimise use of expensive transit bandwidth, as up to 95 percent of traffic can be served from the Open Connect appliances.

Carrier-neutral IXPs with open access are also useful tools in managing the rising demand for data. In Mongolia, local latency was reduced to less than 10 milliseconds per transaction from a minimum of 1,300 milliseconds with the establishment of the independent Mongolian IXP. Similarly, domestic bandwidth facilitated by the Nepal IX rose by 28 percent, and by 2013 its members were saving up to $100,000 monthly.

By allowing for and encouraging innovation, the internet has revolutionised society, introduced new forms of communication and created more content and services that ultimately will benefit and drive growth in Asia. For this to happen, policymakers must continue to support the fundamental principles of the open internet by establishing the necessary regulatory frameworks that promote competition, non-discriminatory access, net neutrality principles, and accessible and affordable connectivity. These are key to enabling the virtuous circle by ensuring that consumers can access and consume content of their choice. The resulting demand for broadband access will drive investment into network infrastructure, which opens the door for further innovation and the growth of the digital economy.

(Further information and details on these findings and recommendations on fostering an open internet in Asia are available in the new white paper by boutique technology research and consultancy firm TRPC titled "Connectivity, Innovation and Growth: Fostering an Open Internet in Asia." For the full report, please visit http://trpc.biz/connectivity-innovation-and-growth/)

05. **"They Say It's Friendship. We Say It's Unwaged Work"[1] Vulnerability, Dependency, and Profitability in a Digital Universe**

Urvashi Aneja

The vulnerability of information and technology infrastructures is becoming more visible and alarming by the day. In the past few months alone, two separate malware outbreaks–WannaCry and Petya–have affected hundreds of thousands of people and organisations around the world. WannaCry crippled over 230,000 computers across 150 countries, with the UK's National Health Service, Spain's phone giant Telefónica and Germany's state railways among those hardest hit. Thousands of machines running on Windows, including ATMs, ticketing machines, hospitals and numerous industrial control systems across the globe were also compromised. First reported in Ukraine, Petya affected government services, banks and power utilities, along with Kiev's airport and Metro system. The radiation monitoring system at Chernobyl, too, was taken offline for fear of an attack. Petya also affected operations at India's largest container port JNPT, in Mumbai; data put out by Symantec suggests that India was the worst affected country in Asia.[2]

Researchers initially blamed the shutdown on ransom-ware, which seeks to make money by holding data hostage unless the victim pays a hefty ransom fee. But soon after, a more bleak conclusion emerged: that the malware was a "wiper" with the objective of permanently destroying data. The aim, in other words, was to create chaos. Earlier this year, data of 17 million Zomato users was stolen in India and supposedly re-sold on the dark web. An IBM-Ponemon Institute 2017 study notes that the average cost of data breach in India has grown from INR 9.73 crore in 2016 to INR 11 crore in 2017.[3] In addition to this, a report by The Centre for Internet and Society, New Delhi notes that the Aadhaar[4] numbers of over 13 crore people and bank account details of about 10 crore have been leaked through government portals in India because of poor security practices.[5]

At the same time, human dependency on these very systems is increasing. At an individual level, Fitbit and other such devices tell users if they are walking enough, eating too much or sleeping soundly. Many people would be lost without Google Maps, even in cities they call home. As technology becomes more invisible and omnipresent, and interactions more seamless—think Alexa or Siri[6] —the dependency will only increase. At a social level, people already increasingly rely on social media platforms to make friends, find jobs, decide where to go on holiday and even make electoral choices.[7] For many, social media is the primary portal to the internet. In rural India, for example, Facebook is typically the platform through which most users access the internet.[8] With the Internet of Things, 26 billion devices will be connected around the globe—smart appliances will communicate with each other and pre-emptively respond to user preferences, and public utilities will be integrated and made responsive to population movement and consumption patterns. The dependency is so great that some studies have noted the rise of "digital amnesia"—people are beginning to use their computer devices as extensions of their brains and, in the process, are ready to forget important information in the belief that it can be immediately retrieved from a digital device.[9] Such dependency amid such vulnerability seems unwise. Yet, in India, as in some other parts of the world, this dependency is being mandated and enforced by the state: from demonetisation and the push to digital finance, to the Aadhaar number and India stack.[10]

Indeed, data is the new oil. A staggering 90 percent of the world's data has been created in the past four years. When the dot-com bubble burst in the late 1990—early 2000s, Silicon

Valley desperately needed a new business model. Then, in 2001, the World Trade Centre was attacked in New York, convincing the US government that its traditional methods of intelligence gathering were no longer working. Julia Angwin, in her book *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance,* convincingly argues that the coincidence of these two events created a common interest between government and technology companies to track internet behaviour. Both the US government and Silicon Valley technology companies "arrived at the same answer to their disparate problems: collecting and analysing vast quantities of personal data," writes Angwin. This confluence of interest, she argues, led to the birth of the "surveillance economy."[11] "Cookies" became central to this new model, as they wacked web users across sites and collected data on individuals.

Growing amounts of data and technological advances have now ushered in an era of 'Big Data', allowing advertisers to not only provide curated product suggestions, but also predict present and future preferences and capacities. Most websites now have a tracker inside: at any given time, unless a user's browser is protected by a robust anti-tracking extension, the personal computer is making between 50—100 connections—if not more, and without consent or prior knowledge—to other websites that track, store and share data.[12] Consent in fact is rendered almost irrelevant: it is almost impossible to obtain consent from an individual when data that is collected can be used for multiple purposes by multiple bodies. It is further rendered meaningless with the Internet of Things: billions of devices will be connected and sharing data, but the data may not always be encrypted, making it easily vulnerable to third-party usage.

As people create their digital selves—making profiles, listing habits and preferences—choosing to 'like' and 're-tweet' certain items - they allow business to extract value from their preferences, personality, lifestyle, relationships, and ambitions. Social media presence has itself been commoditised by companies that measure influence on social networks and give chosen users 'perks', or free products from various brands, ostensibly piggybacking on the users' 'reach'.[13] Facebook is unsurprisingly a prime staging ground and profiteer in the surveillance economy. A recent speaker at the Aspen Ideas Festival shared a story that highlights how the surveillance economy exploits our deepest vulnerabilities. Concerned she might have a drinking problem, she searched on Google for symptoms of alcoholism; a few hours later, she received an advertisement on Facebook for her local liquor store.[14]

Technology companies also adjust pricing and product promotions on the basis of past buying history and known traits. Amazon, for example, differentially prices goods depending on pin-code and expected income level.[15] Last September, Google received a patent on technology that lets a company dynamically price electronic content. For instance, it can push the base price of an e-book up if it determines that a shopper is more likely to buy that particular item than an average user; conversely, it can adjust the price down as an incentive if the user is judged less likely to purchase.[16]

The current business model for many websites thus offers 'free' content in exchange for personal data. But, in the process of volunteering data for free, users have become the labourers of the digital economy. Writing about immaterial labour in the mid-1990s, Maurizio Lazzarato warned that capital's grip would only grow tighter as it sought "to involve even the worker's personality and subjectivity within the production of value."[17] In 2012, Facebook reached more than 1 billion users and generated revenue of US$5.1 billion. It is the first social media website to be traded on the stock exchange wherein all content on its site is created by its users. Might what users do on Facebook be called a form of work? A recent and very popular campaign, titled wagesforfacebook.com is worth quoting at length: "They say it's friendship. We say it's unwaged work. With every like, chat, tag or poke, our subjectivity turns them a profit. They call it sharing. We call it stealing."[18] The point is not to demand actual wages from Facebook, but to initiate a way of thinking, a political posturing, that recognises how its users have become the subjects of their own commodification.

Despite the fact that less than 40 percent of India's population is online, the sheer size of the Indian population means that India has one of the highest numbers of internet users. Most of the data generated, however, is held in servers outside Indian borders. The top five data storage facilities are in the US,[19] and more than half of the world's rentable cloud storage is controlled by four major corporations—Amazon, Microsoft, IBM and Google—each of which adopts a similar global pattern of server farms.[20] India is thus one of the largest exporters

of data worldwide. With rural India being ushered into the digital economy via social-media platforms, on shared devices and often without knowledge of, or access to, privacy software, this trend is poised to continue. To make matters worse, India does not have a data protection regime, which means the interactions with social media apps are governed only by a contract, i.e the dense and often overlooked Terms of Service. And again, the state seems to be interested in institutionalising the commodification of personal data. Already, organisations in India are looking to build new businesses on the capabilities of Aadhaar and India Stack. *The Economist* reports that venture-capital firms are funding hackathons to encourage software developers to come up with new ways to use the technology.[21]

So, as TV news channels report on the "most-watched videos online," and "hashtags" are the new symbols of protests across the world, the online and offline worlds are getting increasingly enmeshed. Governments are furthering this enmeshment as they digitise governance services and make "citizenry" conditional on digital enrolment. But this system is deeply fragile and vulnerable to external shock and disruption, and this is without even bringing in the geopolitics of cyber security. And the real rot lies within: people are dependent on a system in which they are themselves the labour, in which their subjectivities and relationships are being commoditised and sold back to them.

Where is this headed? Probably a tiered internet, where the rich can afford secure internet, accessed through VPN networks and patched with the latest browser extensions to keep hackers, trackers and advertisers at bay. This is already happening, of course, with most major newspapers now offering either a monthly subscription option or a free-service with advertisements; the paid-for content is typically of much better quality as well. The rich will also insulate themselves from day-to-day digital dependencies; many in Silicon Valley send their children to tech-free schools and digital detox programmes are booming across wealthy cities around the world.[22] Netropolitan, the "Facebook for the rich," has a US$9,000-joining fee, promises no advertising, along with cloud storage and other benefits.[23] The masses, on the other hand, will be unable to afford their freedom or privacy and will continue to perform digital labour, accessing the internet through insecure free servers. Without the knowledge or financial means to safeguard their data, they will mine their own preferences, so that products can be continued to be sold back to them. At least click-workers—that other set of invisible and exploited labourers supporting the internet—get paid for their work, albeit often less than a decent wage.[24]

Headed down this road, the internet will soon become the staging ground for a new kind of class war. Unless, of course, societies choose the more sensible route of recasting the internet as a critical public utility, revisiting government initiatives that parcel citizenship and economic participation into a digital bundle, implementing stringent data protection laws, investing in robust security infrastructure as a prerequisite not an afterthought and, finally, on a broader level, recognising technological trajectories as social choices that should not be left to market forces alone, even if in the name of innovation.

CYBER GOVERNANCE

06. **Between a Rock and a Hard Place: Tempering National and International Tensions in Cyberspace**

Chelsey Slack*

Introduction

"To contrast national solidarity and international cooperation as two opposites seems foolish to me."
—Gustav Stresemann

Headline-grabbing cyber attacks punctuate the global debate on security in cyberspace. In response to the growing calls to address this threat, a number of initiatives have been taken up across the globe. Several strands embody this effort to develop voluntary norms for responsible state behaviour in cyberspace, to create communication channels through confidence-building measures, and to bolster resilience through capacity building. Underpinning this web of activity is the notion that greater cooperation is critical for everything from information sharing to fighting crime and developing capacity. However, given recent cyber attacks, coupled with the resurgence of Westphalian politics and anti-globalisation sentiments, this assumption favouring cooperation seems increasingly under threat. Are states less willing to cooperate based on a calculus that using cyber attacks brings more advantages than restraint and cooperation? Which current tracks are the most compelling to prevent a slide to permanent cyber (in)-security? This article will explore these questions with a view to providing perspective on the tension between national and international aspects; between rivalry and interdependence in cyberspace.

A Weak Case for Restraint and Cooperation?

There are myriad international efforts designed to foster stability in cyberspace. However, recent examples of cyber incidents in various parts of the world cast doubt on the effectiveness of these activities to encourage restraint. Take the cyber attacks on critical energy infrastructure in Ukraine as an example. In July 2015, a report by the United Nations Group of Governmental Experts (UN GGE) proposed a voluntary norm against targeting critical infrastructure. Less than six months later, in December 2015, a cyber attack left over 200,000 people without electricity in Ukraine for several hours. Another incident was reported in December 2016 following a power outage in Kiev. These incidents highlight the difficulty in the interpretation and enforcement of norms or other activities designed to restrain behaviour. Democratic institutions are also increasingly becoming targets, as demonstrated by the unprecedented hack on political institutions, notably the Democratic National Committee of the United States in the run-up to the presidential elections in 2016. While some states have advocated for a norm that prohibits the intervention of states in the internal affairs of other sovereign states, it could be argued that the precise opposite is happening in practice. Last, but certainly not the least, the recent global cyber incidents have also been noteworthy in scale and scope. The WannaCry incident in May 2017 saw more than 200,000 victims in 150 countries: from hospitals and schools to telecommunications firms, and a host of public and private entities. This was followed by NotPetya in June, which had a significant impact in Ukraine, but with effects reported in multiple countries across several sectors. Against the backdrop of these developments, it would appear that restraint is far from being the operative term for some actors in cyberspace.

Cyber tools facilitate the conduct of time-old activities such as sabotage and espionage.[1] Instead of breaking into a building to steal sensitive documents, one could potentially achieve the same objective sitting safely behind a computer screen. States can also benefit

** Chelsey Slack is a member of the International Staff at NATO working on cyber defence policy issues. For this article, she is writing in a purely personal capacity. Any views expressed in this paper therefore reflect those solely of the author and do not represent those of, nor should they be attributed to any organisation.*

from the activities of non-state actors. For example, a *New York Times* report outlined the case of Evgeniy Bogachev, the Federal Bureau of Investigation's most wanted cyber criminal. At one time, Bogachev illegally controlled between 500,000 to 1 million compromised computers (a botnet) through a malicious software called GameOver ZeuS. While initially used to conduct financial theft, according to one analysis, "computers under Mr. Bogachev's control started receiving requests for information – not about banking transactions, but for files relating to various geopolitical developments pulled from the headlines."[2] In essence, GameOver "wasn't merely a sophisticated piece of criminal malware; it was a sophisticated intelligence-gathering tool."[3] This potential case of 'piggybacking' demonstrates how states may stand to benefit from harnessing the efforts of non-state actors, which are used as force enablers. Why exercise restraint or cooperate to put cyber criminals in jail when such activities can help to advance strategic objectives?

The manipulation of the global payment messaging system, Society for Worldwide Interbank Financial Telecommunication (SWIFT), which resulted in the theft of USD 81 million from Bangladesh's central bank in 2016, provides another prescient case. The story continues to evolve with a potential link to North Korea now under scrutiny. However, when asked whether he believed that "nation states are now robbing banks," one former senior US official went as far to respond "I do."[4] Additionally, the means by which criminal activities in cyberspace can be prosecuted are complicated at best and limited at worst. It can take months for requests under mutual legal assistance treaties to be processed, and that is if states are willing and able to comply with such a request. This may serve as a disincentive for states against making a concerted effort to prosecute such cases.

Considering the above examples, the benefits for states to use cyber tools and shelter non-state elements, including cyber criminals, seem apparent. To date, state practice has been limited when it comes to setting out declaratory policies, drawing red lines, and enforcing these with consequences for behaviour that is deemed unacceptable. The challenge is how to deter those activities that fall below the threshold of armed conflict. It could be argued that there is a calculus that some states and criminal elements can get away with certain activities in cyberspace. This hinders efforts to combat nefarious activities from which some states may perceive a benefit. In other words, "absent meaningful consequences, states and non-state actors may simply lose their fear of getting caught, as a lax de-facto norm of negligible consequences emerges."[5] There is also the problem that some actors might not care if they are caught. They simply accept this risk as the benefits of the activity outweigh it. However, without clear signaling bolstered by state practice on the issue, the incentives for restraint and cooperation may be less compelling.

Turning The Tides and Investing in Incentives

The tides may be turning. In recent years, states have signaled more openly the types of activity they consider unacceptable. Notable examples include a litany of diplomatic responses, sanctions and criminal indictments brought forward by the US for incidents such as the theft of intellectual property attributed to hackers from the People's Liberation Army in China (2014), Russia's alleged meddling in the US election through cyber attacks on the Democratic National Committee (2016), and the indictment of four individuals, including two Russian security officials, related to the 2014 breach of 500 million Yahoo! accounts (2017).[6] Public reports unveiling cyber attacks on democratic institutions such as the Bundestag in Germany, political parties in France, or government systems more broadly in a handful of other European countries also reinforce this trend.[7]

There is debate on the motivations behind and the effectiveness of such public actions for deterring similar activities in the future. However, a case can be made that the discussion now, at a minimum, includes a precedent of the consequences for pursuing certain activities in cyberspace that are deemed unacceptable. The Yahoo! case, in particular, aptly highlights how cooperation between states and non-state actors can go both ways: the alleged culprits (criminal hackers with potential links to security services) as well as the responders (private sector in cooperation with government).

Attribution—whether public or private—can be a useful tool to incentivise restraint because states are able to better ascertain where attacks originate from, and publicly and privately warn about the potential consequences of certain behaviour. State practice is developed in part through attribution. Attribution is ultimately a political decision, and a complex one, which involves blending both technical and contextual factors. There are strategic

considerations in deciding whether or not to make attribution public, such as not wishing to disclose potentially sensitive intelligence gathering methods and sources. While weighing these important factors, it can nonetheless be argued that attribution can help to inform state practice, which in turn facilitates the formulation of rules of the road for behaviour in cyberspace.

What further incentives might encourage restraint and cooperation? In the end, states need to understand that "...it is simply not possible to have both a strategically exploitable cyberspace, full of vulnerabilities, and a secure and resilient cyberspace."[8] In political terms, the case of the 2015 US–China agreement offers pertinent insight into potential incentives. In this instance, both sides agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property..."[9] While the real intentions are difficult to decipher, one potential hypothesis revolves around two types of pressure that may have been exerted. These include "the threat of U.S. sanctions" and the potential realisation by China that their "activities in cyberspace were creating unacceptably high levels of risk for the U.S.-China relationship" as a whole.[10] This is but one proposition: however, the ramifications of targeted sanctions or the deterioration of a broader strategic relationship cannot be discounted. It is also a question of understanding thresholds of tolerance when provocations are frequent.

If there is any cause for motivation, it is the prospect of something to lose. If behaviour goes unrestrained, like in the case of the manipulation of SWIFT, interdependency becomes a liability, not an asset. According to one report, the "annual costs of global cyber crime could surpass the value of the internet's benefits by 2030."[11] Improving the way states cooperate across borders to combat malicious activity is a shared priority. One example is Operation Avalanche. This operation was unprecedented in scale, bringing together prosecutors and investigators from 30 countries to take down in 2016 one of the largest botnet platforms. After more than four years of investigation, five individuals were arrested, and the victims of malware infections spanned over 180 countries.[12] This underscores the complexity of conducting global operations with multiple stakeholders, both public and private. It also underlines the need to further streamline the processes that frame this cross-border cooperation. Although related specifically to cyber crime and law enforcement aspects, the modalities of cooperation demonstrated in this example could provide further impetus for collaboration in other cases of international cyber incidents.

Finally, recent global cyber incidents are also illustrative of this interdependence as well as the need for multistakeholder cooperation given the multitude of victims. This raises interesting questions regarding the role of governments considering the privately owned and operated nature of most critical infrastructure. If a cyber incident on critical infrastructure threatens economic prosperity or national security, what is the role of the state: to assist when requested? The lack of restraint witnessed in the conduct of recent malicious cyber activity should spur even greater cooperation to curb the benefits of such activity. In the end, it is imperative to alter the calculus by placing a focus on the incentives and benefits for restraint and cooperation in cyberspace. After all, everyone stands to lose eventually when instability reigns.

Which Tracks Hold the Most Promise?

How can the benefit/risk calculus be altered to lower the benefits while increasing the perceived risks of malicious cyber activity for the adversary? What can be done to increase the benefits and lower the risks of interdependence? To help restrain behaviour and encourage cooperation in cyberspace, more state practice is needed in terms of calling out unacceptable behaviour and imposing costs, including targeted sanctions or related consequences. There is also a need for a frank discussion and improved understanding of the grey areas that fall below the threshold of armed conflict in cyberspace: for example, activities related to sabotage and espionage. As has been demonstrated, this is a profound source of instability. Sabotage and espionage can be rapidly misunderstood and cause further escalation. In effect, "[a] cyber attack that causes a minor power outage could be a warning shot, a failed attempt at a major strategic network breach, or an inadvertent result of reconnaissance."[13] The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, published in 2017, is a useful tool to help facilitate the discussion on clarifying the grey areas that fall below the threshold of armed conflict. The European Union's (EU) recent decision to develop a "Cyber Diplomacy Toolbox" should also be noted as an effort to

clarify and signal the likely consequences of a joint EU diplomatic response to malicious cyber activities and, therefore, "…influence the behaviour of potential aggressors in the long term."[14]

It may be too soon to tell whether recent cases of public attribution, with corresponding sanctions and indictments, are effective in deterring future attacks. However, it is increasingly understood that some form of pushback to give credibility to emerging norms is necessary. Moving forward, three particular aspects to help encourage restraint and cooperation stand out: further promoting voluntary norms of responsible state behaviour in cyberspace, notably when it comes to critical infrastructure; bolstering networks such as the Group of Twenty (G20) and Group of Seven (G7) in dealing with cyber risks to the global financial system; and further building up regional initiatives on confidence-building measures for cyberspace.

As mentioned at the outset of this paper, there are many efforts underway to enhance stability. More specifically, the development and promotion of voluntary norms, notably those that would limit attacks on critical infrastructure, found common ground in the 2015 UN GGE report. Reports of cyber activity against critical infrastructure in a number of countries, including nuclear power stations in the US and other energy sectors in the United Kingdom and Ireland, are of obvious concern.[15] This appears to run counter to the spirit of previous discussions in fora such as the UN GGE. The manipulation of the SWIFT network demonstrated the potential to undermine confidence in the global financial system. Given the volatility and prolonged recovery of global markets since the 2008 financial crisis, a major shock to the financial system exacerbated by cyber attacks has to be avoided. Moreover, the potential of malicious cyber attacks to inflict widespread disruption, damage and loss around the world should incentivise cooperation between sectors, public and private entities, and states, particularly when it comes to defining and upholding norms related to protecting critical infrastructure. The question remains how to incentivise compliance with norms given their voluntary nature. States may define critical infrastructure in different ways. While consensus could unfortunately not be reached on a new UN GGE report in 2017, work should continue to further clarify those norms first proposed in 2015. Be it through multilateral channels, global commissions, bilateral arrangements or coalitions of likeminded countries, setting out clear benchmarks for state behaviour and addressing behaviour that is viewed to the contrary is critical to forging greater predictability.

Linked to this development and promotion of norms, networks such as the G20 could be well placed to treat cyber risks to the global financial system, given the common interest to ensure the way money is made and moved across the globe remains secure. Traditionally, the true cost of cyber (in)-security has been difficult to quantify, with broader security aspects featured more prominently in the debate. However, the lens needs to be refocused on the economic aspects of cyber (in)-security in the context of international relations. To this end, there has been some mainstreaming of economic aspects into the development of global norms. For example, following the 2015 agreement between then US President Barack Obama and Chinese President Xi Jinping, a similar text tackling cyber-enabled theft of intellectual property was introduced as part of the G20 communiqué later that year. This illustrates the potential for best practice at the state level to be captured and reinforced in the multilateral context of the G20 and other international networks. At their meeting in March 2017, G20 finance leaders pledged to "promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20."[16] Key to this effort is also enhancing cross-border cooperation. Although more limited in membership, the G7 also provides a vehicle for building consensus. The G7 "Declaration on Responsible States Behaviour in Cyberspace," adopted in April 2017, reaffirms the applicability of international law to cyberspace, and reiterates those voluntary norms developed in both UN GGE and G20 contexts. More specifically, the G7 has also set out guidelines in 2016 for cyber security in the financial sector against the background of the SWIFT incident. Such guidelines could be widened to encompass more states, and thus raise the bar when it comes to mitigating cyber risks to the global financial system.

Finally, regional efforts can be a good place to build stability due often to shared histories and cultural affinities. Earlier this year, for the first time a joint conference was organised by the Organization for Security and Co-operation in Europe (OSCE) and the Republic of Korea. This is a pertinent example of how different regions and organisations can share experiences and improve understanding of cyber security issues. More of these inter-regional activities

should take place. For instance, inter-regional cooperation on confidence-building measures could be expanded to include activities of the Organization of American States (OAS). Later this year, India will host the 2017 Global Conference on Cyberspace. This will provide a welcome perspective from Asia, including from many emerging economies. As of December 2015, 4 billion individuals were not connected to the internet.[17] Enhancing stability is, therefore, even more important against a broader backdrop of on-going concerns about equality of access and capacity.

Tempering Tensions Through Interdependence

Despite the dense web of interdependence that characterises cyberspace, motivation for restraint and cooperation should not be taken for granted. Recognising this fact and examining closely how these elements can be incentivised is a useful starting point. Further compounding the issue is that while "[i]nternational cooperation on cyber issues has become an essential part of wider global economic and security debates[,] [i]t is a rapidly evolving area of policy, without a single agreed international vision."[18] The benefits of maintaining cyberspace as a free and open space need to be better articulated as states continue to craft their national and international policy positions. The question becomes how to demonstrate that states stand more to benefit from interdependence than rivalry. The calculus must be tipped towards restraint and cooperation, by clarifying grey areas, signaling red lines, and enforcing consequences, including through attribution, targeted sanctions, and the increasing indictment and successful prosecution of those responsible, for instance through extradition agreements. Further elaborating norms, empowering network and cultivating inter-regional ties should also be priorities. In the absence of formal enforcement mechanisms, clarifying standards for behaviour and reinforcing them collectively become all the more important.

More broadly, further examination of the power dynamics at play in the international system is also warranted. This is particularly relevant against the growing prevalence of state-centric political narratives in international discourse. It also underscores the "tension between the nature of the internet, as a global, unified network and national, sovereign approaches to the governance of privacy, freedom of speech, protection from hate speech and personal data protection."[19] As a counterbalance to this tension, the multistakeholder approach that has been cultivated to address the distributed nature of the internet and cyberspace more generally offers particular benefits. Applying strict Westphalian notions to this space will not yield greater stability, rather, it will only reinforce walls that hinder this free and open space. New treaty instruments to regulate this space also remain unfeasible. Instead, the focus should be placed on strengthening the normative toolbox. More than ever, at a time when the international stage is increasingly crowded by a constellation of actors—state and non-state—"[m]aintaining networks, working with other countries and international institutions, and helping establish norms to deal with new transnational issues are crucial."[20] The openness in societies that has built and enabled states to foster these relationships must be upheld.

While all politics might be local, the implications of cyber attacks are progressively global. The scale and consequences of the issue necessitate perspective beyond national borders. The benefits unleashed through cyberspace—unprecedented growth, connectivity, and innovation—have the potential to be undermined from the top (by states) and from below (by criminal elements). This leaves the international community at a turning point before the advantages of this dynamic space are lost. The year 2017 marks an important opportunity to underwrite cooperation by further developing the agenda outlined above. Ultimately, it is interdependence in cyberspace that is key to tempering the tensions increasingly coded into the digital age.

07. **The Hybridisation of Cyber Security Governance: The Emergence of Global Cyber Security Assemblages**

Dennis Broeders

Blurred Lines in Cyber Security Governance

In many countries, cyber crime, cyber attacks, espionage, and cyber warfare are topping the lists of official government threat assessments, even though the empirical evidence underlying these assessments is often sketchy. Governments are actively raising public awareness of cyber vulnerabilities at all levels of cyber security but, at the same time, do not necessarily want to shoulder the burden of protecting citizens and companies in cyber space; nor are they capable of doing so. While capacity in law enforcement, intelligence and security agencies and the military is growing, it is dwarfed by the threats that governments insist are endemic and rising. Both citizens and corporations are, to a large extent, expected to take responsibility for their own online security. The mismatch between government threat assessment—indicating a high-risk environment—and limited government capacity and political will to protect companies and citizens online is transforming the government's role as provider and guarantor of (national) security.

Moreover, many scholars have noted that the internet blurs classical distinctions deemed crucial to International Relations and security studies: those "between individual and collective security, between public authorities and private institutions, and between economic and political-military security."[1] This echoes ongoing academic debates about the privatisation of security.[2] In the cyber domain, the privatisation of security also has a dimension of (in)formality. Privatisation can take either a formal route—through the (regulated) security market—or a more informal route, through the support or 'benign neglect' of digital vigilante forces, which is sometimes a proxy for state involvement. Abrahamsen and Williams maintain that security privatisations are part of a profound transformation of the state and its security functions, which goes beyond the dominant frame of stronger and weaker states.[3] They use the concept of global security assemblages to analyse the reconfiguration of the state and the re-articulation of traditional distinctions between the public and private, and the local and the global. The security challenges in cyberspace and the quest for the means and methods to address them are well suited for this frame of analysis, given the extreme interdependence between the local and the global on the internet, the interdependence between private industry and government authority, and the interplay between high (perceived) threat levels and a limited state capacity to investigate, attribute, counter and prosecute cyber crime and cyber attacks.

The Emergence of Global Cyber Security Assemblages

For governments, the "symbolic claim of providing the public good of security is a source of tremendous power." This symbolic claim may be undercut if the state fails to deliver security and/or if private parties deliver security in the absence of adequate public protection.[4] Striking the right balance between providing public protection and leaving matters to security markets is therefore politically important: a widening gap between rising levels of threat, on the one hand, and limited government protection against cyber crime and cyber attacks, on the other, carries a risk of eroding the legitimacy of the state's provision of security. In its ideal form this essential state role relates to both the internal Weberian monopoly on the use of force, which outlaws the use of force by parties other than the state,[5] as well as for the external monopoly on force which is tied to the Westphalian model

of sovereignty based on the principle of non-intervention between equal sovereign states. Externally, international security and, ultimately, warfare are considered to be a state matter, to the formal exclusion of private parties and non-state actors.[6] Obviously, both internal and external sovereignty are to some extent—always have been—more theoretical ideal types than reality, but they still inform important notions about the internal and external legitimacy of the state and its relations with its citizens and with other states.

Much of the debate around the privatisation of security has been framed as a weakening or strengthening of the state, almost a zero-sum game, leaving the nature of the state as "a basic unit or category of analysis unchanged and ontologically intact."[7] Abrahamsen and Williams, however, maintain that security privatisations are part of a profound transformation of the state and its security functions, which goes beyond the dominant frame of stronger and weaker states. They use the concept of global security assemblages as analytical framework, which they define as: "Complex' structures where a range of different global and local, public and private security agents and normativities interact, cooperate and compete to produce new institutions, practices and forms of security governance."[8] Two aspects of the formation of security assemblages are important in the cyber domain: (1) privatisation, and the question of whether public and private roles can still be demarcated or merge into new hybrids; and (2) informalisation, and the question of whether security solutions operate within legal bounds. Both have implications for the legitimacy of emerging cyber security assemblages.

Global security assemblages reconfigure relations between public and private actors in terms of the governance mix between the two in the provision of security. Rather than using a lens that sees the state losing power vis à vis private actors, the question becomes one of how states may exercise power through its relations with multiple private actors. Indeed, the state has become much more a 'central node in a network of power'[9] than the overall provider of security. Moreover, the combination of security as a public good and the inherent dependency on private organisations in the cyber domain ensures that the governance mix in the assemblage will consist of cooperative, hierarchical and contractual relations. Sometimes public and private actors will cooperate only on shared interests. At other times, private actors will be obliged by law or policy to act in the interest of public cyber security and still at others, private parties will be under government contract to perform certain tasks. In both the hierarchical and the contractual relations, the interest and the risk assessments between the principal (the state) and the agents (various private parties) may differ, leading to various possible agency problems. If the principal cannot effectively monitor the agent's behaviour, this may lead to adverse selection (selecting an incompetent agent) or a moral hazard problem (selecting an agent that will not put in the required effort).[10] Global cyber security assemblages will effectively be a patchwork of hierarchical and contractual relations aiming to provide effective and legitimate cyber security solutions, but will also entail considerable vulnerability for the state on both effectiveness and political legitimacy.

The state's ultimate and symbolic responsibility for security as a public good makes it possible to legitimise effective private security solutions, and this may strengthen its position as the guarantor of security, albeit indirect. But it also creates an opening for vulnerabilities: either when private solutions sanctioned by government are not working out (i.e. agency problems) or when private solutions fill a gap that public opinion actually considers to be part of government responsibility (legitimacy problems). Given the predominantly private nature of the internet, public—private cyber security governance is, to a large extent, unavoidable. Government white papers on cyber security, especially in 'the west', highlight the need for public—private cooperation, even though realities reveal divergent interests.[11] The resulting drive towards public—private solutions at all levels of security—overall cyber security, critical infrastructure protection, cyber crime, cyber security and national security—is powered by both public actors and market forces. The relationship between formal and informal is another element of power constellations within global cyber security assemblages. The edges of these emerging global cyber security assemblages can blur into corporate cyber vigilantism on the internal side and the use of formal and informal cyber mercenaries on the external side of sovereignty. These may be part and parcel of emerging global cyber security assemblages in an empirical sense, but may at the same time be outside the legal order, raising questions of legitimacy.

Three Trends of in Cyber Security Governance

Cyber security—in a broad sense—depends on the interaction between government agencies, (transnational) corporations and cyber security companies. Global cyber security assemblages will emerge from the interactions between these three sets of actors. What these will look like in terms of effectiveness, respective roles and legitimacy will depend on where they will land on three continuums that map degrees of public-private and private-private interaction and cooperation. The classical public-private cooperation continuum runs from information-sharing to deputation in which private companies assume—or are forced to assume—responsibilities for the provision of public security. The private-private continuum starts with private responsibility for corporate and customer cyber security and runs via 'active defence' to cyber vigilantism, either developed 'in-house' or contracted out. The public-private cooperation that underlies the provision of national security in cyberspace runs from outsourcing security services to contracting in cyber security consultants, sometimes to the degree of effectively merging into a cyber security hybrid. On the fringes of this last relationship emerge questions on the (in)formal use of proxies. Although empirical studies in this field are scarce, there are indications that all positions on these three continuums are filled, even though the evidence for the more extreme positions is anecdotal. Taken together, they sketch the emergence of a global cyber security assemblage that is characterised by increasing degrees of hybridisation, informalisation and secrecy.

From Public–Private Cooperation to Deputation

Carr argues that many government cyber security strategies build on a rather rosy notion of "public-private partnerships" and seem to ignore the rather "fundamental disjuncture between the expectations of the two 'partners' in terms of roles, responsibility and authority."[12] This plays out especially when governments conflate corporate interests with public interests. Moreover, certain corporate actors—seen from a government perspective—hold the keys to solving a number of cyber security problems. Especially Internet Service Providers (ISPs) and Online Service Providers (OSPs) on whose networks and platforms all internet traffic passes are crucial players when it comes to addressing security problems such as botnet takedowns but also more political desires such as surveillance and policing domestic laws such as copyright and intellectual property legislation. This moves cyber security assemblages from cooperation in the direction of deputation,[13] in which governments are 'enlisting' third parties to enforce policy.

Information sharing is at the heart of most public-private cooperation in government cyber security strategies and serves to circulate knowledge about relevant cyber threats and remedies. Governments are especially keen to gather information from companies to get a more accurate threat assessment. Companies, on the other hand, are often reluctant to share information with the government because they fear reputational damage—both with the general public and with their peers—and legal liability in case their cyber defences are found to be poor or lacking. Many governments have a special regime for the cyber security of critical infrastructures. Definitions and regulations vary widely per country but as a general rule, sectors such as energy, banking, telecom and water are designated "critical infrastructures" and fall under a regulatory regime that sets specific standards for online security. However, even the information exchange between companies and government at the level of critical infrastructure protection remains unbalanced. In the US, a representative of the banks' information sharing council summed it up as: "We give you all of our information voluntarily, and we get nothing back."[14] The government cavalry is found to be lacking.

Botnet takedowns are a more active collaboration between law enforcement and private parties. Dupont identifies two public-private 'models' that have had some success in taking down botnets.[15] One model is that pursued by Microsoft. Between 2010 and 2014, Microsoft took down at least nine botnets, either alone or in partnerships with public and private parties, with the legal backing of civil court orders. Some cases – such as the Citadel botnet takedown, created the considerable collateral damage of taking up to five million unrelated websites off line. According to Dupont, this highlights the fact that national courts lack the capacity and knowledge to supervise such technologically complex cooperations.[16] The second model is that of the polycentric regulation of botnets in which countries have placed ISPs and anti-virus companies at the heart of the takedown operations, instead of the police or a single multinational corporation. The various national botnet programs and ISPs differ

in the "toughness" of their stance towards end users that are part of a botnet, with more interventionist approaches touching upon debate about online rights such as freedom of expression. This moves public-private cooperating in the direction of "third-party policing" in which law enforcement is no longer a monopolist but works to build collaborative security networks that involve the most suitable organisations and are coordinated by public institutions."[17]

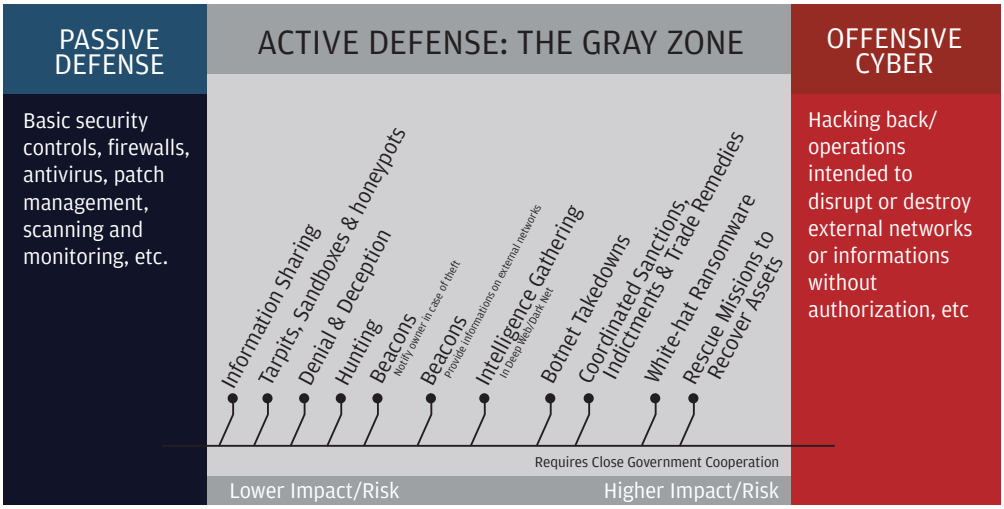
Deputation and content control. The legitimacy of private enforcement becomes much more contested when governments turn to central nodes of the internet and the World Wide Web, such as ISPs, and OSPs such as Google and Facebook. Many governments require these key private players to help enact and police government policies, such as (national) security policies, the policing of copyright and intellectual property protection, or policing the limits of free speech. Here, serious questions arise about (a) whether governments are technologically savvy enough to know the implications of some of the legislation they pass and (b) which tasks can be legitimately outsourced to the private sector. When private actors start policing the content that runs over their networks—as they do in various parts of the world[18]—the question of legitimacy becomes even more poignant. The risk here is that content monitoring—and, by extension, censorship—shifts to the anonymous layer of ISPs and other internet intermediaries, characterised by Zuckerman as the rise of "intermediary censorship."[19] Things are taken to the next level if these companies start to reject content preventively to avoid private damage claims and lawsuits or conflicts with governments. In that case, government has not only contracted out the letter of the law to private parties, but the spirit of the law as well.[20]

From Self-Defence to (Contracted) Vigilantism

Companies have a responsibility to defend their networks and to organise effective cyber security for its operations and/or clients. Some large multinational companies are able to organise their cyber security in-house, but most companies depend on the market for cyber security. As the protection in cyberspace by governments is generally considered to be inadequate, private solutions dominate and seem to be developing in the direction of active defence against cyber intrusions and attacks. Corporate defence that crosses ill-defined legal thresholds may end up looking like corporate cyber vigilantism that transcends territorial borders and may even violate the sovereignty of other states. This challenges the traditional role of the state in law enforcement and international relations.

The push towards active defence. One of the most vociferously debated issues in cyber security governance is "active defence." The idea of active defence is still very much under debate and the legal demarcation of the concept determines whether certain behaviour in cyber defence is considered legal or illegal. "Hacking back," which is considered to be offense, should not be used interchangeably with active defence, although it is precisely the notion of retaliatory hacking back that makes the debate so crucial. A 2016 report by the Centre for Cyber and Homeland Security[21] plots a number of cyber operations on a continuum between passive cyber defence and offensive cyber operations, indicating a grey zone between defence and offense (See Figure 1).

Figure 6: The Continuum Between Defensive and Offensive Cyber Operations



Source: TRPC analysis based on statistics from Cisco VNI reports

A 2012 survey indicated that 36 percent of 181 surveyed companies had at least once engaged in retaliatory hacking. Even though figures like these are rare, there are many hints and indications that not all companies remain passive under attack. In the United States, there is a lively debate about where the line should be drawn between legal "active defence" and illegal offensive retaliatory operations. Think tanks, especially, are trying to move the debate in the direction of more leeway for companies to actively deal with cyber attacks and cyber crime. These reports call for greater legal clarity about what is and is not permitted, but most also suggest more active solutions based on different models and historic analogies, with some public involvement to provide legitimacy. The proposed schemes vary from creating a "cyber privateering regime" based on the issuing of "letters of marque and reprisal" that rewards, enables and empowers the private sector to defend itself in concert with the government[22] to proposals to "not prioritise the investigation or prosecution of companies that push the limits of the law when defending against cyber attacks."[23] Other proposals envisage government licensing to create and formalise private cyber security companies analogous to the private security industry, into modern day Pinkerton agencies and/or to private investigators.[24] Government would thus licence and legitimise new central nodes in the cyber security assemblage. The most recent report on this matter, by the Carnegie Endowment for International Peace draws an analogy to the Private Maritime Security Companies, an industry that bloomed as a result of the piracy crisis in the Gulf of Aden and the Indian Ocean starting in the 2000s. Here the sector itself and the insurance industry took the lead in providing security and building the operational framework for it. Governance effectively followed private practice.[25] This report also suggests that governments may elect to deputise certain companies to engage in active cyber defence.[26]

Outsourcing active cyber defence? Most companies, even large multinational ones, do not have in-house capacity for advanced cyber defence and call in the cavalry, usually a private cyber security firm, when they have been hacked or are under attack. Companies such as Crowdstrike, Mandiant, Fire-eye, RSA, Kasperksy Labs and Fox-IT are some of the internationally operating cyber security companies of choice that gather evidence, close off leaks and vulnerabilities and often provide the forensics for any further action by law enforcement. They also set up active defence mechanism that are aimed at preventing and/or monitoring new attacks and intrusions. Just as in the case of in-house cyber security capacity, these companies often operate in the grey zone of active defence and sometimes push up against the boundaries of the law. It is difficult to ascertain how far these companies go. This author interviewed professionals working in the private cyber security sector in the Netherlands who indicated that they got frequent requests from their clients to "take down the server" that commands an attack, even when it is likely to be located abroad. Although the interviewees indicated that their companies would decline such a request, they also indicate that there are firms operating on the Dutch market that do provide such services, but these usually fly below the radar. Such outsourcing may create a degree of (legal) separation from (active) cyber defence activities for companies that make use of such "services."[27]

From Outsourcing Security to Cyber Security Hybrids

The state has a long tradition of buying military and security products from private companies and contracting out security activities, such as mercenary services, in the past, and in more contemporary times, private security companies (PSCs) and private military companies (PMCs). In the cyber domain, state security agencies are increasingly contracting in private cyber security expertise instead of sourcing them out. This development builds on the ongoing privatisation of security tasks in combination with the fact that military and intelligence cyber operations require a constant interaction between the operational and the technical. Product and process have to a large extent become indistinguishable. In the cyber domain commissioning security products increasingly becomes a process of consulting, resulting in public-private hybrids that work behind the closed doors of security and intelligence agencies and the military. Consulting for intelligence and security agencies brings in an additional layer of legal informalisation as their activities—unlike those of the armed forces—are effectively unregulated by international law.[28] The degree of informalisation deepens when states resort to sanctioning, supporting or sponsoring non-state actors to act as their proxies in cyber conflicts.

A cyber military complex. Traditionally, the manufacturing and maintenance of weapons outside of a specific military action are considered to be civilian functions.[29] However, in

the cyber domain, high-end weapons, i.e. intrusion and weaponised code, require constant development and fine-tuning, also during operations. An analysis by the Stockholm International Peace Research Institute (SIPRI) puts the services of arms industry companies active in the cyber security domain under four headings: "network and data protection software and services; testing and simulation services; training and consulting services; and operational support."[30] These categories move from traditional outsourcing of services that are considered supplementary to categories of "consulting" and "operational support" that suggest a more hybrid form of the provision of security. Especially, 'operational support' is interesting when thinking about the question of who is actively involved in cyber conflict in terms of personnel and practice, as these companies all stress that they offer 'solutions', i.e. a combination of products and services. In the cyber domain, traditional outsourcing will be supplemented with various forms of hybridisation by making private contractors and consultants part of the team. Even though the debate about the demarcation of what constitutes cyber conflict and warfare is still in full swing, at the level of the actors the teams are increasingly likely to be public–private hybrids.

Between consulting and hybridisation. The distinction between actual combat and other military activities that could be legitimately outsourced is vague in the cyber domain. In the ideal situation, the private military contractor is a legitimate actor within a global security assemblage as long as it does not engage in the exercise of force. The idea is that their efforts are supplementing the military tasks of the state, although in terms of democratic oversight this often comes at a cost in terms of limited accountability, regulation and oversight.[31] These consultants are often shielded by a legal secrecy that obscures their work from public scrutiny. In the off-line world, contractors are civilians "and therefore not subject to military command and control structures; nor are they subject to military law." However, the increasing hybridisation of public and private actors in national cyber security provision, combined with a lack of conceptual clarity on issues such as what constitutes a cyber weapon or a cyber attack, makes this a domain in which legitimate roles and legal thresholds for private action are yet to be determined. The intimate relation between the military (governed by the law of armed conflict) and the intelligence and security agencies (which are effectively ungoverned by international law) in the cyber domain confuses the issue even further. Another complicating factor is that in the cyber domain the demarcation between "traditional espionage" between states increasingly gets mixed up with state-sponsored industrial espionage. Whereas the former is a nominally accepted state practice unregulated by international law—because all states reserve the right to intelligence gathering—the latter is causing serious international tensions, for example between the United States and China.[32]

As much of the cyber activity of states may be better characterised as intelligence and espionage than as military activity, it is not always clear which legal framework applies. The line between non-military activities and the use of force is less obvious than in traditional conflict zones where kinetic weapons usually mark the difference. Some legal scholars have argued, however, that the nature of cyber weapons puts pressure on the idea that one can separate out the "triggermen." Padmanabhan[33] argues that the complex nature of cyber weapons requires "states to use contractors with technical expertise to constantly modify the features of a weapon in order to overcome the defence of the target, thus blurring the line between the traditional civilian task of weapons development and the traditional combatant task of weapons use." Because of the "interpenetration of public and private spheres, the dissolution of the inside/outside distinction and the enmeshment of state and non-state actors' in modern military affairs," Ettinger speaks of combatant assemblages,[34] which suits the hybridisation of the military cyber domain as well.

Informalised hybridisation: proxy actors. The informal version of privatisation of state tasks could be characterised as vigilantism or as the use of proxies.[35] Some countries mix their 'uniformed' cyber soldiers with volunteer forces that are called upon when the need arises. China, for example, has a mix of a uniformed cyber command and unofficial groups of hackers that can be mobilised in times of conflict and crisis.[36] Russia is also associated with the use of patriotic hackers, even though the efforts to prove that the May 2007 DDoS attacks on Estonia and the 2008 attacks on Georgia were the work of state-sanctioned patriotic hackers responding to unofficial calls from the FSB have not been definitive. Patriotic hackers are aligned with the military aims and course of action of their country but are not formally under the command of the military: they join in 'spontaneously'. Due to their patriotic enthusiasm, they are not always easy to co-opt or coerce in line with state objectives.[37] Gazit notes that vigilantism can function as an informal mechanism of political

power. Vigilantes are usually considered a disruptive political force that challenges state power, but sometimes, their priorities align informally in a process of 'state collusion' that achieves the state's goals while officially being able to keep some distance from the dirty work.[38] Determining the relationship between a state and proxy actors is difficult even in kinetic conflicts where the actors wear uniforms and are captured on camera, but more so in the context of cyber conflict. Various (legal) degrees of separation—'dependent on the state', 'effectively under control of the state', or 'under overall control of the state'—determine the relationship and responsibilities between a state and proxy actors but are difficult, to substantiate.[39] In the cyber domain, however, most proxies remain unclassified in the legal sense, even when political—but not legal—attribution sometimes does happen. But even though proxies are legally outside the playing field, they are a very real part of cyber security assemblages in practice.

The Future is Hybrid?

The emergence of global cyber security assemblages is built on a profound dependency between public and private actors, the commodification of cyber security and the inability and unwillingness of states to provide overall cyber security to companies and citizens. Three trends seem to materialise when looking at various studies of the public-private interactions in cyberspace. The provision of cyber security—especially when understood as a public good—cannot be provided without private-sector involvement resulting in an increasing hybridisation of the provision of (national) cyber security. A second trend is that of informalisation. The combination of insufficient government capacity and legal uncertainties makes companies seek private solutions for cyber security problems that push up against the legal limits that are grounded in the state's monopoly of the legitimate use of force. Governments deputising companies to enforce government policies in cyberspace further informalises power and sometimes even relocates it into the back offices of the private sector. In the realm of national and international security in cyber space, governments themselves push the legal limits by blurring the roles and tasks between military and intelligence actors. Whereas military operations are regulated by the law of armed conflict, intelligence operations are effectively unregulated under international law, creating room to manoeuvre and strategic advantages for top-tier states. Moreover, both the increased use of private consultants—fuelling hybridisation at the heart of national security—and proxy actors are forms of informalisation. Paradoxically, the militarisation of cyberspace seems to be accompanied by a de-militarisation of those that do the 'fighting' in cyberspace conflicts, as intelligence actors, private consultants, vigilantes and proxies are increasingly the prominent actors in cyber conflicts. A third trend—building on the previous two—is secrecy. Both corporate and public solutions to (advanced) cyber security problems are increasingly shrouded in (legal) secrecy and/or a lack of transparency.

The emergence of global cyber security assemblages is not a monolithic development but resembles Nye's concept of a cyber security regime complex:[40] a loosely coupled set of regimes dealing with various governance aspects of cyberspace. Similarly, cyber security assemblages are loosely coupled constellations of actors and expectations that partially overlap. Moreover, the governance mix in the assemblage will consist of cooperative, hierarchical and contractual relations; each with its advantages and challenges. This highlights the need to analyse them both as subsets and as an assembled whole. It is in the interactions between the various subsets that new norms, institutions and practices of cyber security governance will emerge. In that process vital questions will emerge about the effectiveness and legitimacy of security solutions and how that will affect the position of the state as the responsible actor for security as a public good. It seems that many governments are currently prioritising the effectiveness of cyber security solutions—by deputising companies, outsourcing to various markets and sourcing in consultants—perhaps banking on output legitimacy as the prime source of political legitimacy. Given limited government capacity and private expertise and capabilities this may be an effective governance strategy, but only if the state remains the central node in the configuration. It also weakens traditional democratic legitimacy (input legitimacy)—especially if control slips away from public authorities—and creates problems of unaccountability.

08. **Doomed to Fragment? Addressing International Security Challenges While Avoiding Internet Fragmentation**

Nikolas Ott and Hugo Zylberberg

Introduction

Considering the recent spike in news coverage on ransomwares, hacks, cyber attacks, data breaches and intrusions, it is easy to forget the significant economic and social opportunities that digital transformation can provide on a global scale. New innovations, as well as ubiquitous connectivity around the world, are reshaping technology and its role in people's daily lives. In turn, digital transformation opens up new economic and social opportunities: the sharing economy, decentralised crowdfunding platforms, and accessible global communications have the potential to increase political stability worldwide.

This is true both in the developed and in the developing world. The digital economy "contributed $2.3 trillion to the G20's GDP in 2010 and an estimated $4 trillion in 2016, [and] is growing at 10% a year – significantly faster than the overall G20 economy."[1] Moreover, there is evidence that connectivity drives growth in a development context. As the World Bank report on digital dividends states: "For businesses, the internet promotes inclusion of firms in the world economy by expanding trade, raises the productivity of capital, and intensifies competition in the marketplace, which in turn induces innovation. It brings opportunities to households by creating jobs, leverages human capital, and produces consumer surplus. It enables citizens to access public services, strengthens government capability, and serves as a platform for citizens to tackle collective action problems."[2] As connectivity becomes a crucial factor for economic development, the security–development nexus is increasingly being recognised as a key sustainability factor.[3]

As the 2016 World Economic Forum (WEF) report on internet fragmentation correctly outlines, these economic and social outcomes rely on the "Internet [remaining] stable and generally open and secure in its foundations."[4] Yet, the model for cyberspace governance can hardly be that of one uniform internet. In the spirit of the inventors of the internet,[5] states should aim at producing interoperable policy frameworks allowing the possibility of governance across stakeholders, while leaving states in charge of implementing these frameworks at the national level.[6] The WEF report identifies 28 issues of current or potential fragmentation along three buckets: technical, commercial, and governmental fragmentation. This paper focuses on governmental fragmentation, which refers to governmental rules that hinder the introduction or further development of international policy guidelines, or that affect the perception of a unique network.

When it comes to both national and international security concerns, the international institutions governing cyberspace face a dilemma: they cannot fully satisfy all relevant stakeholders at the same time. Finding the right balance between the interest of states, the private sector, and citizens is a delicate process that is deliberated in various multistakeholder fora such as the Internet Governance Forum (IGF). The discussions touch on themes as diverse as data protection, privacy, freedom of expression and law-enforcement responsibilities. However, so far, addressing security challenges in cyberspace through such fora has had limited results. Instead, influential states, such as the United States (US), Russia, China and France, are trying to address such challenges through national legislation with extra-jurisdictional reach. While national legislation might seem easier for states, they tend to worsen governmental fragmentation and further complicate the creation of international procedures addressing global cyber security challenges.

Recently, much of this governmental fragmentation appears to be driven by security concerns: be it in France where a filtering system for jihadist websites was implemented in 2015,[7] in Germany where a recent law forced platforms to remove obviously illegal hate speech[8] in a context when fake news and the security of election infrastructures is under question, or in a series of other countries proposing to ban end-to-end encryption. This is by no means limited to authoritarian states and has become an issue that concerns policymakers around the world, as reflected in the joint anti-encryption opinion piece penned by the Manhattan district attorney, the Paris chief prosecutor, the commissioner of the City of London Police, and the chief prosecutor of the High Court of Spain,[9] and more recent declarations of the UK Home Secretary against terrorist usage of end-to-end encryption.[10] Taking stock of the security rationale for such government policies that will further increase internet fragmentation, this paper argues for the establishment of interoperable policies, through a holistic "fragmentation impact assessment" and increased involvement in international security discussions to limit what this paper labels as "security-based fragmentation": governmental fragmentation related to international and national security in and through cyberspace, which also includes security incidents relying on legitimate uses of cyberspace.

States' Westphalian Notion of "Sovereignty" in the Digital Age

The current internet governance structure (a multistakeholder governance framework) is ideologically and conceptually at odds with the Westphalian notion of states' sovereignty in its current understanding and practice. While in most states, multinational technology companies have a crucial role in ensuring the accessibility and the maintenance of cyber infrastructure, this does not automatically give them a role within the international policy decision process. One could rightfully argue that the states' permission to integrate technology companies and civil society in these negotiations is an exercise of their sovereignty.[11] Indeed, many non-state actors are now involved in the practical application of international law to cyberspace, through 'Track 1.5' dialogues[12] or efforts such as the Tallinn Manual,[13] where leading academics assess how existing international law apply in cyberspace. Despite many states being uncomfortable with this development, the fact that a large part of the infrastructure is owned and operated by the private sector and loose communities of researchers makes their participation crucial to advancing international discussions.

To understand the challenges that states are facing, it is necessary to further clarify the different concepts surrounding cyber security. Broadly speaking, these can be captured in four categories:[14] international security, national security, device security and data security.

1. International cyber security focuses on interstate issues of cyber conflict. Policies in this category include: exchanging national security doctrines, creating communication channels, and reviewing the applicability of international law in cyberspace. The most active fora for these policy discussions are the United Nations Group of Governmental Experts (UNGGE)[15] and the Organization for Security and Co-operation in Europe (OSCE),[16] though other fora, such as the Organization of American States or the Association of Southeast Asian Nations (ASEAN) Regional Forum are contributing to these discussions as well.

2. National cyber security addresses the challenges of intelligence agencies, law enforcement, policing and other entities that are responsible for addressing crimes committed in and through cyberspace. In addition to national entities, the Budapest Convention on Cybercrime and INTERPOL, too, play a crucial role in facilitating cooperation and information exchange between state entities.

3. Device security focuses on the integrity and stability of internet infrastructure and related cyber-physical systems: systems in which "operations are integrated, monitored, and/or controlled by a computational core."[17] Related efforts are mostly technical and led by national institutes for standards and technology, or offices for information security, within large multinational technology companies.

4. Data security mostly centres on maintaining security and privacy throughout the data lifecycle: collection, storage, treatment (or processing) and use. Few states have dedicated agencies for privacy issues but some have special commissioners or governmental representatives to assure proper inclusion of privacy concerns in related policy discussions.[18]

This piece focuses on the first category of cyber security: international cyber security. Unfortunately, few policy discussions draw upon these distinctions. One example is the current discussion about a digital Geneva Convention, brought forward by Microsoft. The current proposal covers several of the aforementioned categories at the same time, which makes it difficult for policymakers to properly address the proposed changes, given the lack of compatibility with existing policy structures. However, it is important to note that decisions taken within the realm of international security have both direct and indirect effects on the other categories. For example, a discussion between states can have an impact on multinational technology companies that operate globally and rely on internationally recognised procedures, certification standards, or treaties. At the same time, interstate negotiations affect the daily work of national law enforcement entities that rely on productive interstate relations.

Despite the inherent borderless nature of cyberspace, most policy solutions to date are tailored on a national (Russia/China) or regional (European Union) basis. States seem to 'muddle through' instead of working with non-state stakeholders towards suitably interoperable actions. This is especially true for international and national cyber security issues. However, more recently, multinational technology companies have been trying to contribute to this policy debate as they are increasingly affected by its outcome. This is reflected in ongoing legal discussions about the legality of access for states on data stored in another country. Microsoft's lawsuit against the US government over rightful access of data is only one out of many cases where companies come into conflict with government demands for access to data stored abroad.[19] As cloud computing is expanding drastically, it is reasonable to expect that overall technological developments introduced by the private sector have and will most likely continue to outrun the pace at which policy decisions are made. Therefore, multinational technology companies should continue to play an important role in the development and implementation of security policies that affect cyberspace.

Whether it is because states operate on the assumption that policies that increase fragmentation are necessary to maintain their security in cyberspace across all four aforementioned categories, or because fragmentation is an unanticipated second-order effect of their policies, it seems that this security-based fragmentation has indeed been on the rise. This paper now examines the assumption that fragmentation can lead to better security, before proposing a framework promoting interoperable policy frameworks to avoid it.

An Increase in Internet Fragmentation does not Necessarily Lead to Better Security

States' practice has shown that the restriction of cross-border data flows[20] for privacy or security reasons, and increased power to lawfully access this data is becoming more widespread, even as the extent of such restrictions and surveillance is being debated. The European Union's (EU) General Data Protection Regulation (GDPR),[21] associated with the negotiation of the Privacy Shield agreement, creates a framework whereby data flows are restricted towards countries where the data protection framework is too weak. Another example of this trend is the United Kingdom's Investigatory Powers Act,[22] which requires internet and phone companies in the UK to maintain the capability to intercept their customers' personal data; this is unlikely to be the case in other countries, including in Europe. The UN Special Rapporteur on the Right to Privacy, Joe Cannataci, recognised this growing trend in a recent report,[23] calling for an international treaty to protect people's privacy from unfettered cyber surveillance. However, such calls mostly address the fourth of the previously introduced categories, namely, data security. While ensuring citizens' privacy deserves significant attention, the increasing friction between states within cyberspace needs more attention as well.

The belief that a more fragmented internet—bringing borders to the digital realm—leads to a more secure interstate environment is flawed, for three main reasons:

First, it is currently much harder to secure a network than to attack it.[24] While this mostly affects device security, it also entices states to engage in deterrence-based cyber security strategies through the development of offensive cyber capabilities. As a well-resourced and motivated attacker always succeeds, digital borders at the national level will be bypassed just as physical borders, i.e. bypassing firewalls. This leads to a perpetual state of insecurity that can currently only be addressed through diplomatic means, such as confidence-building measures and legal agreements.

Second, tools to circumvent national borders (e.g. virtual private networks) will continue to appear and be used precisely by those actors who present the most serious security threats. Moreover, prohibiting or limiting the use of end-to-end encryption will take it away from regular people and companies that rely on such security measures. On the other hand, terrorists, criminals and other nefarious actors will eventually find new ways to avoid surveillance efforts. Therefore, efforts to limit the use of such tools are not just ineffective in the long term, as adversaries adjust, they also negatively affect data and device security in the short term.

Third, cyberspace is the domain, not the source of security threats. As countless government reports have argued, governmental shortcomings in the security realm do not come from a lack of institutional capacity to collect data, but from a lack of integration and coordination between law enforcement, the justice system, and the intelligence community. This is a long mission that the United States (US) started ahead of other countries in the wake of 9/11, by creating the Office of the Director of National Intelligence,[25] but the ongoing discussion on the proper division between military (US Cyber Command) and espionage (National Security Agency) activities shows that the debate is far from being concluded. Ultimately, it is important to highlight that security measures most often fail due to human, not computer, error.[26] While such concerns generally affect domestic cyber security policy, a lack of such domestic capacity significantly hinders the ability of states to engage in constructive interstate dialogues. Consequently, having a comprehensive national cyber security strategy is highly desirable to further increase the likelihood of successful international negotiations. Moreover, it is especially important to get national cyber security policies right, to be properly prepared for a cloud-based and borderless operational environment, where international cooperation on law enforcement and other issues are becoming even more important for properly addressing security challenges within this domain.

Calibrating A Multistakeholder Discussion on Security-Based Fragmentation

Even though more government control can help secure cyberspace in the short term, it is often unlikely to do so in the long run. As technologists weighing in on the debate over backdoors have shown,[27] short-term solutions (developing a system where law enforcement is able to access any system given judicial authority) can eventually be subverted by malicious actors for their own purposes, undermining global cyber security. While short-term issues are crucial in a world where serious security threats can put human lives at risk, any solution must take into account the consequences of enabling malicious actors to gain state-level mass surveillance capacities. Developing partnerships with the private sector is a crucial element of any potential solution. Without developing new infrastructure-enabling mass surveillance, security services can often find the data they need in existing privately-owned infrastructure. Therefore, some countries have now adopted the position that instead of laws requiring companies to give them access to their servers, they can be satisfied with a point person available at all times to help with urgent requests related to national security.

In addition to this balance between short-term and long-term concerns, international discussions on cyber issues need to consider their own impact on the security and stability of cyberspace. Indeed, policy choices affect cyberspace stability, and conversely, a state's evaluation of its stability affects its policy choices. Inspired by the recent publication of Laura DeNardis through the Global Commission on Internet Governance,[28] this paper suggests that in the same way that companies have to produce privacy impact assessments or human rights impact assessments, fragmentation impact assessments (FIA) could be developed for policies that appear to drive fragmentation in an excessive fashion. These FIAs could include an introduction to the policy being discussed, as well as an evaluation of its impact on the issues below.

Basic principles:

- **Protection of personal data:** All actors should respect fundamental data protection principles giving citizens—not states or companies—power over their personal data.
- **A neutral network:** No technical restrictions at the infrastructural level should restrict which applications the general public can or cannot use.
- **Network generativity:** Should there be any limits to innovation at the end nodes?

Principles affecting the private sector:

- **Interoperability:** All services provided online should be interoperable.
- **Industry standards:** Technical standards should not be subverted for national security purposes.
- **Global commons:** Is there a subset of the internet that should be declared a global

commons?

Principles affecting states' behaviour:

- **Data sharing:** States should streamline data-sharing processes between law enforcement, judicial and national security institutions.
- **Integrity of data:** States should not alter the integrity of data, at rest or in motion.
- **Accessibility:** When is it legitimate to block content travelling to one state from another through whatever technical means?

Building interoperable policies regarding acceptable behaviour for states vis-à-vis access to data and public–private partnerships are key to limiting security-based fragmentation. International and regional efforts, such as the Global Commission for the Stability of Cyberspace, the UNGGE and the OSCE or ASEAN, provide platforms to identify common interests and acceptable standards of behaviour between states. Here again, stronger integration of the private sector during policy negotiations, despite the increased difficulty, is key to finding interoperable solutions that work in practice.

In parallel to building interoperable policy frameworks using FIAs, states should develop an understanding of when and where fragmentation can be legitimate. There is a need to find the characteristics of legitimate national regulation with limited externalities on internet fragmentation. Such a discussion could start with the following questions:

- Is there a "public core of the internet"?[29] Governments can agree on a limited set of targets that should be protected from both states and intervention, e.g. the Domain Name Systems or some fundamental internet routing protocols.
- Which components of the internet should be regulated on a national basis, and which ones on an international basis? In areas where states will continue to regulate on a national basis, how can this regulation be made interoperable with others to mitigate the economic cost incurred? International efforts in building policy frameworks in a transnational fashion must be encouraged so that legislation can continue to develop on a national basis but produce outcomes that are increasingly interoperable with neighbouring ones.
- Are there alternatives to satisfy states' security needs that include more or less policy fragmentation? More academic work to understand fragmentation can help states produce FIAs to measure the consequences of a specific policy proposal.
- Where and when does fragmentation matter most? Academic efforts taking stock of existing internet fragmentation, and asking when and where its consequences are most limited, are still lacking.

Conclusion

Despite growing concerns over security incidents in and through cyberspace, the internet still holds significant economic and social opportunities. The securitisation of the current debate compounded by a return of nationalism in the public debate of liberal democracies threatens these promises as well as the very values enshrined in the technical infrastructure and the governance mechanisms associated with the internet. However, this paper argues that some of this securitisation is based on the flawed premise that a fragmented internet with monitored digital borders matching physical ones is more easily defensible.

This paper concludes by recommending questions and characteristics for a global multistakeholder debate, the establishment of FIA, and increased involvement in the development of cyber security policies. Section three outlines how these three recommendations are intertwined and can support each other, namely, questions and characteristics for a global multistakeholder debate that, combined with FIAs and stronger involvement, can better inform policymakers and increase the chances of producing interoperable policy frameworks, thus limiting security-based fragmentation.

Acknowledgements:

For written comments on early drafts, the authors are indebted to Marina Kaljurand, William Drake, Ben Hiller, Henry Rıigas, Aude GØry, Jessica Zucker and Christoph Berlich. An earlier version of this paper was presented at the OSCE-ASEAN Inter-Regional Conference on Cyber/ICT Security.

EMERGING TECHNOLOGIES

09. **Challenges for a New Economy: The Fourth Industrial Revolution**

Logan Finucan

Introduction

New advances in an array of different technologies promise to transform the structure of the economy and the way people live. The so-called "Fourth Industrial Revolution" (4IR) will bring significant progress in productivity, such as in the use of advanced robotics and manufacturing techniques, the Internet of Things (IoT) and machine-to-machine (M2M) connections on a massive scale, autonomous vehicles, and new industrial materials, all powered by artificial intelligence (AI) and pervasive big data analytics. Underpinning this new world will be the mass deployment of cloud computing and the continued growth of the digital economy.

While these transformations will improve human welfare, they are also expected to bring widespread disruption and challenges for workers, society and global macroeconomic policies. Governments need to stand ready to work with all stakeholders to meet these challenges ahead and ease the pain of transition.

A History of Industrial Revolutions

Throughout history, there have been periods when technological and economic progress have advanced in leaps and bounds. While there are different ways to analyse the pace of change over time, most historians and economists identify three major revolutions in recent world history, wherein new technology and new business processes produced dramatic changes in the ways the human race has lived and worked:[1]

FIRST
- Fuelled by refinements in the use of steam power and mechanised production;
- Began in the United Kingdom in the late 18th century;
- Gave rise to the first factories, vastly improved productivity, accelerated urbanisation. Generated new markets for textiles, manufactured goods, coal, iron and steel.

SECOND
- Centred on the application of electricity, the telegraph and telephone, chemical and metallurgical sciences, internal combustion, flight, and assembly line production;
- Began in Western Europe and North America in the late 19th century;
- Enabled mass markets for consumer goods and dramatically accelerated transportation and communication.

THIRD
- Triggered by the invention of electronics, computing and telecommunications systems;
- Began in mid-20th century and is still unfolding in the present day;
- Has transformed the ability of humans to record, process and communicate information, transforming business processes and social relations.

Each of these industrial revolutions built upon the progress of the preceding one, using the previous technological advances as a platform for further innovations. They relied upon exploiting economies of scale inherent in new production technologies to deliver new commodities to the market at ever-lower prices. In the process, these market transformations not only changed the sector exploiting the economy of scale—such as coal,

steel, electricity production, microchips—but also enabled different and entirely new sectors of the economy.

These were massively disruptive processes: the industry transformed and old jobs became obsolete. However, this disruption was offset in the long term by new and previously unforeseen creative forces. Thus, while the invention of the automobile, for example—enabled by the internal combustion engine and the assembly line—meant that "horse-related jobs declined… entirely new jobs were created in the motel and fast-food industries" in addition to new jobs for factory workers and auto mechanics.[2]

The Opportunities of the 4IR

Mass-scale electronics manufacturing markets, widespread connectivity and the advent of cloud computing and big data—all outcomes of the Third Industrial Revolution—have set the stage for the next revolution in human productivity. Various new technologies are emerging that, when applied to the economy and society, promise significant changes. Executive chairman of the World Economic Forum (WEF), Klaus Schwab, who popularised the term and ignited global discussions following his first pronouncements, cumulatively refers to these changes as the "Fourth Industrial Revolution (4IR)."[3]

AI and Machine Learning

Artificial intelligence (AI) promises to extend the reach of computing processing power from routine computational tasks to the realm of reasoning, perception, natural language processing, learning and problem solving. The development and operation of AI is powered by processing and analysis of big data, and will be key to managing the complex tasks and computation associated with many technologies of the 4IR. In several countries, the private sector is investing heavily in AI capabilities and has already commercially deployed some applications.

IoT and M2M Communications

The I2T and M2M communications is a developing system that combines networks of embedded sensors and actuators with remotely located computing and controls; this system may operate with or without human intervention.[4] While not a new concept, applications of IoT systems have exploded with the drop in the cost of sensors, embedded electronics and connectivity. The IoT's applications are vast, from industrial and logistical processes to connected homes, infrastructure, vehicles and utility management.

Advanced Robotics

While industrial robots have been a feature of some industries (particularly the automotive industry) for a long time, more advanced robots (enabled by AI) are expected to play an increasing role in production. Armed with new mobility, reasoning and general intelligence capabilities, they can better substitute human labour in processes that are non-routine and require higher cognitive abilities.

3-D Printing

Also known as additive manufacturing, 3-D printing creates objects by gradually layering materials using computing controlled processes. Recent advances have enabled 3-D printing using various materials, including certain types of polymers, resins, metals and glass. In some cases, combinations of different materials are possible in the same object, enabling devices such as batteries and drones.[5] While currently focused on prototyping, 3-D printing markets are growing rapidly and are increasingly moving into other areas as production volumes grow.

New Materials

Industrial biotechnology and nanotechnology are enabling the development of new fuels and industrial materials. Biotechnology uses new genomic and synthetic biology tools to precisely manipulate an organism's genome, enabling not only biofuels but also bio-based batteries and production of industrial materials. Nanotechnology allows the manipulation

of materials at the nanoscale—approaching the level of individual atoms—in fields as diverse as quantum computing, solar cell production and medical applications, such as artificial tissue and nanoscale medical devices. By making the development process quicker and more precise, these will end trial-and-error material science, allowing materials to have tailor-made properties.

Data and the Cloud Links Them Together

Underpinning all of these technologies is cloud computing. Researching, developing and applying these technologies to business processes require collecting and processing massive amounts of data. Therefore, access to high-quality computing is indispensable. While this would be out of reach for most economic actors if they needed to invest in hardware individually, with economical and on-demand access, cloud computing is a crucial facilitator of the technologies of the 4IR.

Impact on Productivity and Challenges of Transition to the 4IR

The economic impact of the 4IR will be substantial, although the specifics are yet to be worked out. The Organisation for Economic Cooperation and Development (OECD), in a recent report, "Enabling the Next Production Revolution," provides an idea of the potential productivity benefits based on some of the new technologies already being implemented today:[6]

- Improving the quality and accessibility of data by just 10 percent is associated with a 14-percent increase in labour productivity;
- Autonomous logistics applications can increase output by 15–20 percent, lower fuel consumption 10–15 percent, and reduce maintenance costs by eight percent;
- Industrial IoT applications can reduce production costs by 18 percent on average; and
- Using AI to optimise aspects of data centre management reduces energy consumption by 40 percent.[7]

These data are just an early-stagae indication of what new production technologies can do in existing industries. Their full potential—what Schwab feels will be a "supply-side miracle, with long-term gains in efficiency and productivity"—are yet to be charted.[8] Further, the broader economic transformations these gains will trigger will be even greater as the 4IR unfolds, business and society adapt, and new economic sectors emerge.

Indeed, the widespread application of these technologies to the economy will bring major changes to society. Labour markets, social policies and global economics are poised to transform in ways that challenge established ways.

Labour Markets

Non-Routine Work Replaces Routine Work

The rise of automation will transform the types of jobs in the economy. Several studies, such as that by Frey and Osborne, have garnered attention by predicting which categories of employment automation will eliminate, fuelling fears that the 4IR will cost jobs.[9] However, these studies do little to illuminate the jobs that automation will create.

Historical trends cast some light on what this will mean in practice. Analysing over 140 years of census data from England and Wales, one study by Deloitte found that during the previous three industrial revolutions, "routine jobs"—both manual and cognitive—declined. However, this was more than offset by the rise in "non-routine" jobs.[10] A similar study in *The Economist* found the same striking rise in non-routine work in US occupational data from 1983 to 2014.[11] Moreover, Deloitte found, "non-routine cognitive jobs" actually have strong complementarity with technology. Applying new technologies that increased their productivity allowed employees to focus more on non-routine analytical and creative aspects of their jobs. Examining specific categories of work, Deloitte found that while the fastest shrinking jobs over the last several decades included manufacturing and craftwork, and stenography and secretarial positions (routine tasks), the fastest growing categories of work included nursing, teaching and welfare, as well as management consultancy, business analysis, and information technology management (non-routine tasks).

This trend towards more work centring on creativity, cognition, problem solving, non-repetitive tasks and human care, will only continue and accelerate.

Change is the New Normal
While workers will need different skills than they have now, these needs will continue to change. As new technologies are deployed and new markets emerge, business models will evolve rapidly. This will give rise to new categories of work that do not yet exist. Moreover, even when a job category continues to exist, the ways employees perform that job will evolve to be assisted by technology. One survey from the WEF concludes that, on average, skills that are currently not considered crucial to a job will constitute one-third of the core skillset for most occupations by 2020.[12]

Much has been written about the importance of skills in STEM (Science, Technology, Engineering and Math). While these areas must be promoted, equally important is a much broader set of skills. Amid a rapidly changing environment, perhaps the most important thing for workers to have is not so much a specific set of skills, but the capacity to learn new skills as the needs of the labour market change. This means that education should provide a strong basis in areas such as critical thinking, problem solving, communications and general literacy and numeracy, and that more robust systems to foster learning of specific in-demand skills are required.

Societies

Managing Inequality

At the societal level, managing and reducing economic inequality will be critical to ensuring that the 4IR is fully realised and that everyone benefits from its advances.

As automation and digital technologies diffuse throughout the economy, gains accrue fastest to those who create and are able to effectively use those technologies. Evidence in advanced economies to date suggest that this often occurs at the expense of middle-skill workers. Economist David Autor argues that many advanced economies are transitioning to a "barbell-shaped" job market, where automation has "hollowed out" many middle-skill positions in areas of production, sales and administration. While these middle-skill positions become automated, many non-routine but low-skill positions, such as janitorial and food service, remain the same or increase.[13] This poses particular challenges because many of the workers displaced by technology are older and face more difficulties adapting to changing labour market needs.

At the same time, the income premium associated with education and high skills has increased. For workers in the digital economy, such as programmers and software engineers, pay has risen sharply as demand has exploded for the goods and services they produce, leading Klaus Schwab to conclude that "in the future, talent, more than capital, will represent the critical factor of production. This will give rise to a job market increasingly segregated into 'low-skill/low-pay' and 'high-skill/high-pay' segments."[14] Returns to high-skill workers are further amplified by the shortage of available labour with these skills, as businesses are adapting and demanding skills that the workforce is slow to develop.

This differential impact of new technologies undermines the belief that technology and innovation will bring benefits for all. If measures are not taken to ease workers through this transition, the result will be not just slower growth, but greater social and political instability. According to Schwab, "A winner-takes-all economy that offers only limited access to the middle class is a recipe for democratic malaise and dereliction."[15]

Safeguarding Privacy

Privacy, and the need to effectively protect it, will only become more important as our lives become more connected and quantified. Privacy is complex, and the privacy practices that individuals expect vary across culture and contexts.[16] As our lives are increasingly measured and qualified by digital technologies, the risks of transgressions of these norms and expectations—whether malicious or inadvertent—will multiply. Further, AI and big data analytics are enabling new and creative ways to draw insights, potentially deducing sensitive personal information from data that may otherwise seem innocuous.

At the same time, the services that are derived from this explosion of data bring real benefits, both for the individual and society. For the individual, it means better access to information and services that are tailored to meet their specific needs. For society, better solutions can be developed to increase aggregate welfare, such as precision medicine, smart city applications and government resource planning. Gathering and processing large amounts of data, including personal data, is the indispensable raw material for the development, refinement and application of these services.
Therefore, closing off access to personal data is not an option. However, privacy concerns must be addressed adeptly. If people are not assured that their privacy expectations will be respected, they will not participate in new technologies, and this will slow down uptake and development. Thus, the challenge for policymakers is to design legal frameworks for personal data that respect individuals' expectations and empower them without preventing legitimate and productive uses of data.

Human Ethics and AI

The increasing integration of automation and algorithmic decision-making into previously human-controlled processes raise some novel ethical and legal questions.

Autonomous applications and IoT systems have enormous potential to increase human safety. However, there are caveats to this potential. As fully autonomous vehicles with collision avoidance protocols come closer to fruition, some are beginning to consider the so called "trolley problem," a philosophical thought experiment concerning the ethics of deliberately taking one life to save several.[17] In addition to the moral discomfort that arises from resolving such a problem through a pre-programmed decision lacking human empathy, there are also questions of legal liability—specifically, who it should accrue to—when algorithms make decisions that result in damage to property, injury or death.

While the trolley problem is abstract and extreme, forms of AI are being applied to human decisions today in situations that are less extreme but no less troubling in their implications. For example, AI is now being used when considering candidates for a job or university, or an appropriate criminal sentence.[18]

Many countries provide safeguards, such as equal opportunity and non-discrimination protections, that apply to decisions concerning employment and economic opportunity. When a human makes a decision that violates these norms, there is clear responsibility and liability. However, several studies have shown that AI can inadvertently replicate societal biases.[19] Deciding how to assign responsibilities in such a case is less clear, but no less important.

Global Economy

Participation in a Globalised Digital Economy

Because the 4IR is built upon the foundations of data and scale, participation in the global digital economy is key to gaining access to its benefits.

Purchasing the computing capacity to serve the needs of new technologies is too expensive for the vast majority of individuals and businesses. Through resource-pooling and driving down costs through economies of scale, only cloud computing can deliver the massive, ubiquitously available capacity to fill this gap at a price point low enough to be accessible to the widest number of people possible. Moreover, to be economical, cloud networks need the flexibility to operate at a global level.

Thus, participation in the global-scale markets of the digital economy is indispensable. Policies that put up barriers to this—whether intentional or inadvertent—will keep the 4IR technologies out of reach. Traditional trade policies remain as important as ever, given that consumer devices and capital goods remain integral to technologies such as the IoT and robotics. However, digital barriers that choke off cross-border data flows, which can already cause damage to small and medium enterprises, will become an enormous disadvantage as they put the technologies of the 4IR out of reach of all but the largest and wealthiest.

Competition in the Digital Economy

The growth of the digital economy has already begun to raise difficult questions regarding competition. Some have suggested that many data-based business models may constitute monopolies because of the dominance of specific platforms in certain markets.

It is certainly worth asking whether data aggregation creates natural monopolies; that is, industries where the average cost of providing services constantly declines as they increase in scale, making it most efficient for one company to serve the market. Particularly in the digital economy, this can be an outcome of "network effects," wherein using a product or service becomes more valuable when more people use it.

This is easy to understand in the case of social networks. For example, if all of your friends use one specific social network, it is far more attractive to also join that social network, rather than another that is less widely used. This effect is also active (though more subtle) in search engines. The more people use a search engine, the more refined its algorithms can become, providing results that are more relevant to the user. The same effect is visible in the new fields of the 4IR. For example, many IoT networks will work best by integrating with the largest number of devices; precision medicine is optimised by considering population-level data sets; and AI, since it runs on analysing large data sets, is optimised by gaining access to the largest pool of data possible.

Even if these businesses constitute monopolies, it is not clear if they harm consumers or require regulatory intervention. Market power alone is not a problem unless it is abused to gain unfair advantage. Innovative companies that provide free services, such as Facebook and Google, have become nearly ubiquitously used online, despite alternatives that users are free to switch to at any time. They also serve as an invaluable portal for the rest of the digital economy, providing new avenues for individuals, businesses and entrepreneurs to connect with their customers, access and spread information, and engage in commerce. The rapid rise of companies now regarded as monoliths, such as Google and Facebook, as well as more recent digital economy entrants such as Uber or Snapchat, suggests that markets remain fluid, consumers are willing to rapidly switch to new services, and market share alone may not indicate security of position.[20]

Participation of Developing Countries

The capital intensity of these production technologies raises questions of whether developing countries will have the resources to adopt them.

Because of high research and development costs, early deployments of new production technologies are likely to be highly expensive, putting them out of reach of most businesses even in developed countries. As these technologies approach scale, however, costs will decline. Combined with the inherently global nature of the digital economy and the speed of connectivity that globalisation has generated, this provides the opportunity for 4IR technologies to be quickly available to a much wider set of companies around the world. However, this is only true provided government policies do not put up barriers. Just as they are today, factors such as openness to trade, investment and innovation will continue to be crucial to the diffusion of new technologies.[21]

The 4IR may also present particular challenges to the ways that developing countries leverage low-labour costs for industrialisation and development. Nicholas Davis, writing for WEF, observes that since 4IR technologies are more capital than labour intensive, they "may erode the comparative advantage currently enjoyed by many emerging and developing countries, which are focused on labour-intensive goods and services."[22] This may incentivise some production "re-shoring" to developed countries.[23] However, this process—requiring scaling, cost reductions, and large-scale investment—will be lengthy, giving countries time to adjust. Further, even with new, more capital-intensive production methods available, the economics of labour-intensive production methods and trade may remain powerful in many industries and continue to supply rungs on the ladder of development for many.

Recommendations

The 4IR is bringing new opportunities to improve human welfare around the world. However, society will only realise these benefits if it can effectively manage its challenges. To speed and ease the impact of these deep structural transformations, challenges must be approached head on with bold, flexible and inclusive policies.

To accomplish this, governments have an important and complementary role to play alongside the private sector and other stakeholders. There are a few key areas where policymakers should consider action:

1. Enact Comprehensive and Dynamic Workforce Policies
   Workers need assistance to acquire new skills and adapt more quickly to changing conditions. Policy frameworks need to be dynamic and involve a wide range of stakeholders to ensure workers are getting the skills the economy needs.
2. Support Global Data Flows
   A robust digital economy at the global scale, especially cloud markets, is key to 4IR technologies. Governments should work to minimise barriers to cross-border data flows as well as legal conflicts that get in the way of global interoperability.
3. Enable Ubiquitous, Affordable, High-Quality Connectivity for All
   To ensure that the data- and connectivity-based technologies of the 4IR are fully implemented and accessible to everyone, governments need to support robust networks and the investment needed for them to cope with the growth in internet traffic.
4. Build a Business Environment that Fosters Trade, Investment and Innovation
   A welcoming business environment that facilitates investment and innovation will remain as important as ever. So will enabling trade and global engagement, particularly for SMEs, who will best be able to leverage 4IR technologies when they can access global markets.
5. Engage in Dialogue
   There is much that we do not yet understand regarding the technologies of the 4IR and their impact on society. As societies around the world learn to cope with new challenges, policymakers should gauge their responses carefully and engage in dialogue to learn from the experiences of other countries and concerned stakeholders.

10. **Licence in Chains: Could Media Content Be Licensed through Blockchains?**

Meghna Bal

The blockchain is a vast, globally distributed database, which runs on millions of devices and is completely transparent, where anything of value can be privately shared and stored.[1] Intermediaries are no longer the brokers of trust in a transaction. Rather trust is facilitated by a vast network of coders and the immutability of mathematics. This makes it the first intuitive "digital medium for value," just as the internet was the first intuitive "digital medium for information."[2] Blockchain was originally only viewed as an innovation that would transform the financial services industry. Research shows, however, that its usage potential extends far beyond the realm of payments.[3]

One such usage could be within the domain of copyright licensing. Presently, in India, a majority of the licences for media content are issued by copyright societies. Legislators have accorded copyright societies a legal monopoly because they facilitate a reduction in the costs of locating and negotiating with rights holders. Unfortunately, these societies have repeatedly abused their position to the detriment of individual artists and prospective licensees alike. Illustratively, copyright societies have deployed innovative strategies to deny individual artists royalty revenues. Moreover, they have charged exorbitantly high fees for licences of their repertories, a practice that has decimated the online music broadcasting industry in India.[4] Licences are usually issued in blanket form, forcing a prospective licensee to buy the society's entire repertory, even if they only want to acquire a licence for a particular artist. The onerous licensing regime directly impedes the growth of the Media and Entertainment (M&E) industry, a sector that contributes significantly to India's GDP.[5]

The level of disintermediation brought about by blockchain warrants an exploration into whether or not it could serve as a solution for the copyright licensing conundrum in India.

Copyright Licensing: Framework in India

Copyright in India subsists in any "original literary, dramatic, musical and artistic work, cinematograph films and sound recordings."[6] The word "copyright" is not defined by the Copyright Act, 1957. Instead, the Act merely authorises a number of ways in which rights owners may use or exploit their right.[7] The author[8] of a work is typically the first owner of the copyright, unless there is an agreement to the contrary.[9]

There are three types of licences available under the Act: voluntary, statutory and compulsory. Rights holders are free to grant any interest in their works through written licences.[10] Compulsory licences may be granted if works are wilfully held from the public, or for the benefit of disabled individuals, or when the author of the published/unpublished work is either dead or untraceable.[11] Statutory licences are granted to those who wish to make cover versions of sound recordings, those who desire to broadcast literary and musical works and sound recordings, and those who wish to publish translations of any literary or dramatic works in any language.[12] Until very recently,[13] the Copyright Act had tasked the Copyright Board—a quasi-judicial body—with the duty of issuing compulsory licences and deciding royalty rates for statutory licences.[14]

Copyright Societies

For certain types of licensing, individual management of rights was considered unviable. For instance, an author could not contact every single radio or television station to negotiate licences and remuneration for the use of his/her works. Conversely, it was not practical for a

broadcasting organisation to seek specific permission from every author for the use of every copyrighted work. The impracticability of managing these activities individually—both for the owner of rights and for the user—created the need for collective management organisations. In India, collective rights management is facilitated by copyright societies. These entities have a legal monopoly for issuing licences for literary, dramatic, musical and artistic works integrated in cinematograph films or sound recordings.[15] Copyright societies typically acquire the rights for a large repertory of works from copyrights holders and license them to users for a fee.[16] The proceeds are then distributed amongst their members. Ordinarily, there can be only one copyright society for any given class of works. A copyright society must exist under the collective control of the authors and other owners of copyright whose rights it administers.[17] Members must have equivalent control over the workings of the society, and there should be no bias favouring certain members (typically larger players, such as music labels) over others. Copyright societies can only issue licences if they are registered with the central government. Any person aggrieved with their tariff scheme may approach the Copyright Board with a complaint. These structural safeguards were meant to prevent copyright societies from abusing their dominant position.

Before the amendment of the Copyright Act in 2012, the registered copyright societies administering rights in India were as follows:[18]

- The Indian Performing Rights Society Limited (IPRS): The IPRS administered all rights with respect to the underlying works in a sound recording, such as the lyrics and the music itself.
- Phonographic Performance Limited (PPL): The PPL administered rights for sound recordings.
- Indian Singers Rights Association (ISRA):[19] The ISRA represented singers and works to protect their performance rights under the Act.
- The Indian Reprographic Rights Organization (IRRO): The IRRO represented the rights of owners of literary works.

Issues with the Current System

Theoretically, the introduction of a compulsory collective licensing scheme had the dual advantage of furthering social welfare and promoting economic efficiency.[20] Collective rights management fostered social policy goals by insulating authors against exploitation by publishers and other firms of the copyright industry.[21] Moreover, economies of scale enabled larger collecting societies to be more competitive due to the low marginal cost associated with the management of an additional work.[22] Thus, it makes sense for these entities to operate like natural monopolies. Where several collecting societies compete for rights holders, rights holders would probably choose the larger collecting society, since it could "distribute the fixed costs on more" people.[23] The distribution of costs allows individual right holders to save on fees deducted from the royalties collected by the society.[24]

Unfortunately, many copyright societies are now being used as corrupt conduits by larger players, such as music labels, to exploit individual artists and restrict them from earning revenues for their work. In 2010, a delegation of aggrieved artists filed a complaint with the Human Resources and Development ministry about the IPRS neglecting to pay out royalties.[25] The complaint stated that the IPRS withheld some INR 25 crore in royalty payments because many individual members refused to sign a letter that ceded their rights to the publishers and ousted individual authors from executive positions within the society.[26] Further, an investigation in 2011 revealed that the IPRS and the PPL agreed that the PPL would collect royalties on ringtones.[27] The PPL predominantly consisted of large music producers, while the IPRS also included individual authors, such as lyricists and composers. The agreement effectively denied lyricists and composers crores of rupees in royalties due from the use of their works as ringtones.[28]

A sound recording typically encompasses two or three types of rights: one for the recording itself, one for the underlying musical score, and (if the song has words) one for the lyrics.[29] As different societies administer these variegated rights, a prospective licensee will have to negotiate with all of them to broadcast any content.

The 2012 amendment brought in some changes to stem the tide of iniquity rising within copyright societies. It gave authors more control over the administrative and operational

working of societies. All extant societies were required to re-register with the government after the amendments were passed. The IPRS and the PPL—both failed to secure registration—claimed that their registration was pending inquiry and was not explicitly cancelled. The absence of any contradictory clarification from the government allowed the IPRS and the PPL to exploit the nebulous milieu surrounding their registration status and continually extract royalties from unwitting business owners.

Blockchain and Smart Contracts

The blockchain is a decentralised transparent ledger of transaction records.[30] It is shared by and accessible to all network nodes, monitored by everyone, and owned and controlled by no one. The blockchain is updated by miners: coders who apply a mathematical formula to transaction information, converting it into a string of arbitrary numbers and letters known as the "hash."[31] The blockchain is not used to store the file itself; rather, it stores details about the file, such as who created it and what is in it.[32] The blockchain first gained notoriety as the technology underpinning Bitcoin: a cryptocurrency that enabled otherwise unrelated parties to transact safely and securely over the internet without the oversight of a trusted third party. The Bitcoin blockchain was a seminal breakthrough in computer science as it solved a longstanding issue with digital cash: the double-spend problem.[33] Until blockchain cryptography, digital cash was like any other digital asset: infinitely replicable.[34] Without a central intermediary, such as PayPal or a bank, there was no way to confirm whether a certain batch of digital money had already been spent or not.[35]

The blockchain overcame this dependency by enabling the creation of an immutable, time-stamped record of mathematically validated transactions.[36] This new model of "trustless transactions" eliminated the process inefficiencies concomitant with intermediaries such as banks. Further, the blockchain was essentially a registry that tracked details about ownership. Thus, it enabled users to track a certain asset's chain of provenance.[37] Each block in the blockchain contains the hash of the preceding block within its own header, creating a chronological chain of blocks going back to the genesis block.[38] This enables the blockchain's application potential to extend well beyond the scope of digital wallets.

One such application is a "smart contract." A smart contract is a contract that can automatically enforce itself. It does not require third-party intervention to enforce its terms and stipulations.[39] Unlike a traditional legal contract which is written in a language, a smart contract is written in code.[40]

Smart contracts were first conceptualised in 1994 by Nick Szabo and remained a theoretical construct till the advent of the blockchain, which allowed for the automatic execution of code.[41] Smart contract code is stored on the blockchain at a particular address, which is ascertained when the contract is placed on the blockchain.[42] When the event prescribed on the contract occurs, "a transaction is sent to that address" and the network executes the script's operational code "using the data sent with the transaction."[43]

Just as Bitcoin allowed for trustless payment transactions, blockchain-enabled smart contracts allow for common legal problems to be solved in a way that diminishes the need for trust. An example of a basic smart contract on the blockchain is inheritance that becomes available upon the death of a parent. A transaction can be created that sits on the blockchain and goes uninitiated until a specified time or the triggering of certain future events. To set up the condition for inheritance, a program can be written to scan the online death registry and pre-specified online obituaries to verify the parent has died. When the smart contract confirms the death, the funds are automatically sent to the intended recipient.

How will this work in the case of a digital recording of a song? Say the musical data that makes up a particular song—along with related information such as the identity of the lyricist, the singer, and the background musicians—are uploaded on a blockchain. Listeners can access the track by paying a small fee (currently, only through the cryptocurrency Ethereum). A smart contract can be written up to ensure that as soon as the payment is made for the track, a percentage[44] of that amount is paid, in real time, to each individual who worked on the track.

Smart Licensing and its Advantages

Licensing through smart contracts could offer several advantages over the current system. It will not only allow for reliable attribution for claims of authorship, but also enable the tracking of provenance, and permit flexible pricing and terms of use.[45] Smart contracts could also allow for royalties to be paid out through "fast, frictionless micropayments" with minimal transaction costs.[46]

Blockchain technology enables the digitisation and secure storage of information on digital assets, allowing users to track and identify the ownership and location of a particular asset.[47] Hashing prevents the use of any computer algorithm to back-compute this information into the original content, creating a unidirectional cryptographic channel that allows content creators to prove authorship.[48] Moreover, it allows them to prove that authorship existed at a given point in time without revealing the actual contents of the work. Illustratively, the company Ascribe allows graphic artists to lay claim to their work by creating a temporal record of when the work was created and giving it a unique identity.[49] While this might not prevent the illegal upload of recordings to streaming platforms, it will ensure proper acknowledgement of the artists and rights holders.[50] This also allows for the acknowledgement of sessions musicians and background engineers, individuals often overlooked in credit formats under online streaming.[51] In addition to allowing parties to hold assets of value, blockchain technology enables users to transfer these assets on their own terms without the interference of liaisons.[52]

Smart contracts further allow for autonomous pricing mechanisms. Rights holders have the freedom to structure pricing for their content in any way they want.[53] They may even make it free to a particular demographic or on a given day of the year, and have the freedom to include other individuals, such as a photographer or a charity, in the payment scheme.

Smart contracts enable royalty distribution in real time.[54] Instead of passing through intermediaries, revenue from a stream or download could be distributed automatically between rights holders, according to an apportionment already agreed upon, as soon as a track is downloaded or streamed.[55] Further, micropayments, traditionally thought unfeasible for online transactions due to the high transaction costs can easily be made through cryptocurrencies.[56] This is relevant given how content is priced in the digital realm. It also opens the door for electronic "tipping" for content.[57]

In addition to governing how a particular piece of content is priced, smart contracts can also cover how the content is used.[58] For instance, a rock group may allow a school band to use a track without charging them. Information such as a terms of service agreement and contact details could be embedded on the track, which would significantly ameliorate the process of tracking down artists.[59]

It is decidedly difficult for independent artists to raise funds without the support of a record label. Despite the proliferation of crowdfunding platforms, artists are generally unable to figure out how to price their content in a way that will raise some profits for them.[60] The transparency proffered by blockchains allows investors to monitor artist returns closely, thereby encouraging capital investment in this field.[61]

Challenges to Adoption

Though this technology offers a host of benefits to the M&E industry in general, several legal, regulatory and environmental barriers stand in the way of its adoption. Platforms built on the blockchain are not particularly user-friendly. While public keys may be shared with others private keys must be kept secret.[62] Private keys are not particularly easy to remember as they comprise a long string of random numbers and letters.[63] However, a number of backup avenues are open to users including writing it down on a piece of paper and keeping it in a secure location.[64] Cryptocurrencies are also decidedly difficult to generate and their usage is rare, especially within a country like India. It will be hard to generate a high volume of revenue through their use. Projects such as Imogen Heap's "Mycelia" are facing this exact issue with revenue generation.

The level of transparency brought about by the blockchain could pose a problem for labels and publishers, as some information could be business-sensitive.[65] Companies and copyright societies will only adopt this technology if they are confident that it will boost their appeal

amongst artists and users.[66] Transparency may create issues for artists as well. Illustratively, artists who do not enjoy a fair amount of fame might wish to be seen as more well-off than they are whereas major stars might want to seem worse-off, so that fans are not discouraged from spending money on their work.[67] However, there are a number of platforms available that offer differing levels of transparency, suited to the different requirements in the market. For instance, on Dot Blockchain Music, anything beyond the limited data required to acknowledge who worked on a particular track—for instance, its time of publishing—is kept confidential to users.[68] Thus, it is certainly possible for artists and managers to be able to view the value chain without disclosing the information to prospective users.[69]

It is highly probable that intermediaries like copyright societies will remain, however revenue shares may favour artists more. Copyright societies, for instance, could utilise the blockchain to verify data and resolve disputes.[70] Even if their administrative role is supplanted by the blockchain, they will still play key role in negotiating on behalf of artists.[71]

Finally, there is the question of data integrity.[72] What will happen if erroneous information is uploaded onto an immutable ledger?[73] While corrections are possible, it is unclear how disputes would be resolved or received, given the lack of governance and experience of regulators and judicial officers with this technology.[74] Further, the recent amendment to the Finance Bill, which transfers the Board's responsibilities to the Intellectual Property Appellate Board (IPAB), will bring its own set of problems. It is uncertain whether the members of the IPAB will have the requisite competence to handle matters pertaining to copyright. The amendment states that the central government will decide, among other things, the terms of office and the salaries of the members of the IPAB. This brings it in direct contravention with the doctrine of separation of powers (as the IPAB is a judicial body) and, subsequently, a number of judicial rulings on the subject. The fact that the information and broadcasting ministry is looking to set up its own copyright board, to oversee IP issues within the M&E industry, further obfuscates things.

Licensing content through blockchain technology offers considerable advantages. It can bring about a more transparent value chain for content, a dramatic increase in the speed and transparency of royalty payments, and a considerable boost to artistic control. However, copyright societies cannot be done away with completely (at least in the immediate future). They are too deeply embedded in the creative ecosystem and are necessary for eschewing the transaction costs associated with IP. These societies can, however, use the blockchain to do away with the shroud of opacity they currently operate under. Glimmers of this new paradigm can already be seen in the United States, where three American copyright societies are currently working on a blockchain solution aimed at thwarting piracy. The platform will endeavour to create a tangible connection between the time music is created and the time it is consumed. Newer Indian licensing entities such as Novex Communications[75] are well placed to start something similar in India. The hybrid of blockchains and traditional licensing entities could be the dawn of a truly democratised licensing regime: one that benefits all stakeholders involved and works in tandem with the pace of the new digital economy.

11. **Applications and Policy Considerations for AI in Cyber Security and Public Services**

Ryan Johnson and Seha Yatim

The Fourth Industrial Revolution (4IR) will be marked by the universal adoption of cyber-physical systems, Artificial Intelligence (AI), the Internet of Things, and robotics, many of which are already being deployed. But how can the complex interrelationships between these technologies be managed, as well as the disruption they are likely to cause? AI will be necessary to make full use of the benefits of the 4IR, monitoring services for usage security, and performance. This essay analyses the direction these ongoing technological developments will take, and recommends policies for states to adopt so their citizens can take full advantage of them.

In framing this essay, the authors focus on AI that performs specific tasks, a category under which most AI applications and research falls today. General purpose AI, which tends to be depicted in movies as a technology that is as intelligent or even more superior than humans, is still a long way from materialising; it is difficult to project its potential influence.

AI will have a huge impact on cyber security and public services, helping societies become more efficient, secure and innovative.[1] However, the adoption of AI can be impeded by distrust, a lack of understanding or fear of security breaches. Whether data protection, privacy or trustworthiness of data, meeting the security expectations of users will be a significant factor in whether or not the use of AI will become ubiquitous. While these concerns have been around since the dawn of the digital age, AI will rely ever more on data hygiene and will, therefore, cause the exponential growth of threats to individual privacy.

Cyber security and e-services are two key areas in AI where policy can help promote adoption and social change. To develop AI programs geared towards social gains, governments should work with all stakeholders to set policies that ensure AI technologies are developed in parallel to public interests and must take advantage of innovations in cyber security and e-services that AI can bring. Policy and regulatory structures will need to adapt to the countries' own requirements to maximise the benefits of this revolutionary technology.

AI in Cyber Security

AI is poised to challenge current cyber security structures, if not upend them altogether. Applications for AI in cyber security range from cryptography to data protection and detection and management of vulnerabilities.

Cryptography driven by AI may produce some of the most novel and complex cryptographic designs, as found by researchers at Google's AI research platform, Google Brain. They asked two AI systems to send encrypted messages to each other, while a third AI attempted to decrypt them. The research revealed that the two neural networks evolved over time and became so proficient at encrypting messages that the third AI was not able to decrypt their communications.[2] While still at an early stage, this will almost certainly grow into a major field of research. Beyond the difficulty of deciphering their messages, understanding the algorithms and architecture being used will become even more challenging. This will make academic and industry review more difficult, and will drive new techniques for evaluation.

The same forms of AI that are developing their own cryptography can also look for vulnerabilities across systems, programs and network architectures. Combining the speed of

distributed computing with techniques developed by AI will enable software companies to find many more vulnerabilities and potential software hazards before shipping products, and once found, speed up patching, which will reduce cyber threats. It is not hard to imagine the companies currently offering software "fuzzing," which tests the integrity of security systems by overwhelming them with huge amounts of random data, adopting AI to offer always-on AI testing of systems.

As with any kind of cyber security technology, however, there will inevitably come a time when AI will be harnessed for malicious acts, either by states or criminal elements. As systems become more secure, the human element will increasingly be the preferred attack vector. Yampolskiy predicts, "In the near future, as AI systems become more capable, we will begin to see more automated and increasingly sophisticated social engineering attacks."[3] Society needs to think about the implications now, and determine what safeguards and backups are needed to ensure the resilience of the digital world.

AI can be part of the solution. The recent WannaCry ransomware attack showed how the integration of AI into the NHS's cyber security defences allowed the threat to be identified and contained within minutes.[4] National governments are already adopting AI as part of their defensive cyber security practices. The Scottish government has implemented a commercially available machine-learning program that monitors the network and uses probabilistic mathematics and special algorithms to learn about the network it is defending and the attackers it faces. Using the tool, the Scottish government has improved its ability to detect insider and external threats in real time, vastly reducing the damage it faces from cyber attacks.[5] With sensitive data more secure, governments can offer more and deeper e-services at a lower risk threshold.

AI is poised to revolutionise cyber security by improving the skills of both the attacker and the defender. While the use of AI in attacks is concerning, the opportunity to utilise AI to conduct better real-time monitoring and reactions, as well as continuously searching for vulnerabilities in systems even after they are deployed, will build user confidence significantly in an increasingly digital world.

AI in Public Services

Government efficiency is often a subject of consternation. With AI, this may be history. A study by Deloitte revealed that the US government can free up to 30 percent of its workforce's time within five to seven years through AI.[6]

Programs that run on AI could improve public service efficiency in several ways: (i) split a task to allow AI to handle simpler tasks while humans supervise or take on more complex and high-value tasks; (ii) remove repetitive tasks completely by leaving them to AI; and (iii) augment employees with AI-driven tools for more efficient results.

AI is built on data analytics and heuristics that allow smart decision modelling. From the massive amounts of data collected, AI programs can highlight the "whats, wheres and whens" of materials and events, generating fixed data points. The ideal smart city can pinpoint how busy trains are at what time and at which stations, which roads are congested and where responses are needed, right down to which street lights will need replacement.

A pilot test on the use of AI in traffic signals in Pittsburgh, Pennsylvania showed encouraging results, reducing travel time by 25 percent and lowering emissions by 21 percent.[7] In a country such as the United States, which loses $121 billion to congestion and emits 25 billion kg of carbon dioxide emissions every year, the potential savings are appealing.

Healthcare is another area that could benefit from AI. Viral outbreaks, such as the Middle East Respiratory Syndrome and Severe Acute Respiratory Syndrome have had enormous economic impacts. As the world becomes increasingly globalised, viral outbreaks move much faster and become harder to detect or control. AI can play an important role in predicting and potentially stemming the spread of the next outbreak, even in prevention, by running algorithms to predict potential sources of viruses and clusters which may need greater attention.[8]

The applications of AI in public services are broad. Governments around the world have set

targets and aim to create smart cities; from India's Smart Cities Mission to develop 100 citizen-friendly cities to China's implementation of technology and data solutions in 200 cities, and the US Department of Transportation's $165-million investment in smart-city solutions.[9]

How Safe is AI?

The merits of AI do not discount the fact that AI can bring challenges, such as privacy encroachment or biased algorithms. Privacy is understandably one of the top concerns when it comes to the use of data-hungry AI programs. When AI programs are left to make autonomous decisions, they may become biased due to unintentional side-effects of algorithms or the unconscious biases of programmers. As data streams used by AI applications merge and affect each other, in ways that may not always be transparent to the users or data subjects, these issues will become more important to address in both application programming and contracts.

For instance, when an AI system uses past hiring data to learn what is a "good" hire, it may reinforce biases towards a person's name, hobby, age and race.[10] This raises ethical questions about how to enable the gains of automation without removing all human controls. sers and data subjects will also need to understand the role that AI may have in making important, even life-changing, decisions.

Further complicating this picture is the idea that these increasingly large, interwoven, streams of data will be high-value targets for cyber criminals, meaning that assurances on the security of the data (its confidentiality, integrity and availability) will be key to the industry's success. Given that data on individuals is more valuable when it has more data about that individual, big data sets that link financial, health, employment and other categories will require great protection.[11] As is often the case, law and policy will forever be a few steps behind the technological development, meaning that technical solutions will need to incorporate security issues that policymakers may not yet be aware of.

Therefore, while AI has potential in cyber security and public services, the speed of adoption depends on governments and industry creating trust among end users. Industry will have to take the lead in shaping the application of AI in ways that consider cultural and behavioural norms as well as customer needs. Governments will need to strike a balance in policies that do not stifle innovation or potential societal benefits while still protecting the public.

Policy Recommendations for AI Safety

AI Safety is a broad field of research that explores ways to mitigate existing and potential risks posed by AI. Stakeholders in government, industry, civil society and the technical community see great promise in AI Safety to address natural apprehensions about the development of AI. To align AI development with the public interest, this essay makes the following recommendations to governments:

Ensure Policies Prioritise Safety and security

AI decision-making models may raise concerns among citizens over whether their privacy is compromised and whether AI can be trusted to make autonomous decisions. For instance, when AI trawls large data sets, who decides which information is private? If a university acceptance process is automated by AI, can it be guilty of bias? Therefore, it is important that governments build policy frameworks for AI decision-making models that prioritise security and safety as fundamental.

Promote Cyber Security Best Practices

Governments play a key role in promoting best practices that improve security while fostering innovative solutions, such as voluntary, risk-based mechanisms for product design, testing and roll-out. At the same time, a report by the Commission on Enhancing National Cybersecurity has highlighted the need for incentives to encourage the adoption of cybersecure practices.[12] Incentives can range from tax relief and public recognition programmes, to protection from liability. Governments can delve into more research on identifying the optimal way to incentivise businesses to adopt best practices and improve their network security.

Promote AI Norms through Private–Public Dialogues

As governments develop policies around AI and its implications, establishing a dialogue process between private and public sectors is key. Such dialogues can be steered towards developing norms regarding AI applications, and definitions that will steer AI policy development. The dialogue can involve cross-regional stakeholders so that more comprehensive norms or guidelines can be developed for AI technologies that are often used by multiple economies.

Integrate AI into Cyber Security Systems

While cyber attacks today are often automated, many organisations still rely on traditional, manual methods to identify and stem the attacks. As a result, weeks or months can pass before an attack is detected. To move at the same speed as automated cyber attacks, governments and organisations can integrate AI into their cyber security systems to analyse large amounts of data efficiently. An AI security program that audits and interrogates programs can quickly identify potential threats to citizens' data or government systems, and it may even be programmed to shut down hostile programs if necessary.

Invest in industry R&D Partnerships

In many economies, AI R&D is spearheaded by the private sector or academia. However, governments that invest in R&D on behalf of the public sector or SMEs can create a multiplier effect for the economy. For example, the Chinese government, which has a deep interest in AI, has contributed an undisclosed amount to a deep learning lab that will be led by Baidu,[13] while the Japanese government is investing an estimated 100 billion yen (about $882 million) over the next 10 years on a new industry–government–academia project to develop AI technology.[14] By leveraging AI expertise in the private sector and academia, governments can apply it to improve public services or even extend the knowledge to SMEs to create an inclusive environment.

Conclusion

AI has tremendous potential use for societal good. From a cyber security perspective, AI could open a new era in enhanced security. Likewise, new and innovative government services can transform the role of the state and meet the needs of 21st-century citizens. Stakeholders should promote policies that promote the benefits and avoid the pitfalls associated with AI. While governments take the lead and set the rules of play to cultivate AI Safety, it is crucial that all stakeholders contribute to AI Safety from their particular areas of expertise.

12. **Predatory Data: Gender Bias in Artificial Intelligence**

Vidisha Mishra and Madhulika Srikumar

Introduction

Bias in algorithmic decision-making was discovered at least 20 years ago when researchers[1] studied one of the first online flight booking websites in the US and found that the website favoured one airlines over the rest (i.e. American Airlines, which sponsored the website).[2] Algorithms—opaque and hidden—feed on a data diet selected by the developer. In turn, they reflect the biases found in the data. There has been a sharp increase in the amount of data generated as social media and e-commerce become more pervasive. With computers boasting increased capabilities in processing this data, and algorithms getting smarter too, machines learn faster and pick up more from human interests and interactions, resulting in the twin phenomena of machine learning and deep learning

Machine learning, a subset of artificial intelligence (AI), optimises most of one's online usage: from powering web searches to voice-activated personal assistants. Since a lot of data generation is a social phenomenon these days through interactions on social media and political discourse online, AI agents are attuned to human mannerisms, opinions and even biases. AI is described as the development of computer systems that can perform in ways that would typically require a level of human intelligence as a means of aiding their human counterparts. Studies suggest that the gendered nature of AI programming is now well-established: it has its roots in the same traditional social constructions where masculinity or femininity of language is determined by preconceived notions of what it means to be masculine or feminine.[3]

Jack Clark's 2016 article[4] calling out the AI community for having a "sea of dudes" problem relied on an aside involving the Gates. At a tech conference where Bill Gates celebrated the promise of AI, calling it nothing short of the "holy grail," Melinda Gates chose to take a cautionary tone and called attention to the lack of women participation in the creation and development of AI agents. As organisations strive to make diversity a priority, when recruiting employees or assembling panels for conferences (spawning the derisive term, manels), lacking gender diversity in AI can affect not only how the technology evolves but also the impact it has on users, unwittingly or not. While "gender and technology" has long been identified as a point of contention as early as in the beginning of mankind, when technical skills were considered integral to shaping masculinities,[5] "gender of technology" and "gender in technology" are assuming prominence now, and rightly so. As humans teach machines to become intelligent, to imitate human beings, the threat of reinforcing existing biases becomes a real concern, either through sexualising AI or through unequal representation of sexes during creation, leading to deployment of AI that is biased against women.

First, gender of tech. While men write lines of code, AI is female. Digital assistants like Apple's Siri, Amazon's Alexa, and Microsoft's Cortana are all designed as hyper-intelligent yet servile female chatbots.[6] There is a California-based company, RealDoll, that is set to unveil a $15,000-hyper realistic silicon sex doll named Harmony; it is expected to lead to exponential growth in the decade-old sex tech industry that is already worth $30 billion.[7] Realistic sex-robots like Harmony will become common within a decade.[8]

Then there is gender in tech. The shortage of women and other minorities in developing teams has resulted in the (mostly unintentional[9]) creation of AI biased by design, replicating existing gender and racial prejudices. Google had to apologise after a flawed algorithm tagged photos of people of colour as "gorillas."[10] Infamously, when Microsoft introduced their Twitter 'millennial' chatbot, Tay, she quickly adapted to using hateful, xenophobic, and

sexually offensive language due to her self-learning capabilities and the ready availability of biased data. Given that the chatbot was introduced with the tag-line, "the more you talk, the smarter Tay gets," it is not surprising that she adapted to her male-dominated ecosystem where abuse is a well-documented problem.[11] The experience highlighted two issues: first, that women's participation and, consequently, data sets from women are highly limited in most online media forums; and second, that the inability of Tay's developers to foresee this obvious outcome may be attributed to the lack of diversity in the development of the technology.

Gender of AI

In the last decade, conversations on gender-fluidity and post-genderism have gained more traction. However, a majority of AI applications are still anthropomorphic and perpetuate outdated binaries. For instance, digital assistants like Siri, Cortana, and Alexa are modeled after efficient and subservient female secretaries: they undertake functions historically given to women for low pay such as scheduling appointments, looking up information, and generally easing work-related communications.[12]

While the assignment of female characteristics to a majority of assistive AI personalities may seem innocuous, it can have serious implications. First, given the deficit of women in leadership roles, the persistent gender wage gap, and gaps in labour-force participation, gendering digital assistants can reinforce the links between women and subjugation.[13] Voices of disembodied, supportive AI tend to be female as both men and women find them warmer, more conversational and less threatening.[14] On the other hand, AI in movies, which is often portrayed as powerful, is predominantly male. A study of 77 major AI characters in 66 movies between 1927 and 2015 found that barring three examples, all characters were gendered. A total 57 out of these were found to be male while only 17 were female.[15] These representations matter because they reinforce subconscious bias.

Second, it has been reported that female-sounding assistive chatbots regularly receive sexually charged messages. It was recently cited that five percent of all interactions with Robin Labs, whose bot platform helps commercial drivers with routes and logistics, is sexually explicit.[16] The fact that the earliest female chatbots were designed to respond to these suggestions deferentially or with sass was problematic as it normalised sexual harassment.[17] A 2016 study published in JAMA Internal Medicine found that that smartphone assistants such as Siri, Google Now and S Voice were inefficient in responding to statements like, "I was raped" and "I was abused." It was discovered that only Cortana could give the users links to sexual assault helplines.[18] This again highlights that AI is being designed less with female consumers in mind.

The upside is that some technology companies have begun acknowledging these gaps. Recently, Siri was updated to provide more compassionate and helpful advice in response to users' questions about rape, suicide and abuse.[19] Further, digital assistants are also being made more gender-ambiguous. For instance, Cortana's response to "Are you a girl?", is "No. But I'm awesome like a girl." Further, there is growing realisation within the tech community that AI personalities need not be gendered, or even human. For instance, MasterCard's Kai and Samsung's Bixby are gender-neutral, while evidence suggests that people can, and do, bond with non-human technology like with Sony Aibo Robot dogs in Japan.[20]

While these developments are encouraging, it comes alongside the development of hyper-realistic and highly feminised sexbots such as Harmony and "Mark 1" modelled after actress Scarlett Johansson.[21] Presently, considerable money, time and expertise is being spent on the development of AI customised to male preferences at the cost of objectifying the female body and without taking ethical and societal ramifications into consideration. These developments point towards two main concerns: what the implications will be if people begin to mistreat robots with female traits who never say no, and how the normalisation of this behaviour will impact real women and gender relations. The sexually explicit messages received by female digital assistants already demonstrate the possible mistreatment of AI. However, the current enthusiasm for humanising AI tends to ignore the implications of people with gendered ideas creating technologies that conform to gender norms and then perpetuate existing stereotypes.[22] Moving ahead, it is important to address uncomfortable questions such as: How will sexual relations with female robots—who do not or cannot say no—impact the idea of consent and rape? Will violent behaviour with these robots be acceptable? Or as philosopher Blay Whitby puts it, "How would you feel about your ex-boyfriend getting a robot that looked exactly like you, just in order to beat it up every night?"[23]

Gender Bias in Data

While sexism perpetuated by AI can seem like a concern for the distant future, it is already impacting society in insidious ways. Researchers at Carnegie Mellon University in 2015 found that the Google search engine was less likely to show ads of highly paid jobs to women as compared to men.[24] When a 2016 study explored word embeddings that are used to train AI systems that handle language, such as chatbots and recommendation algorithms, it discovered that data mining algorithms associated jobs like philosopher, captain, warrior and boss with maleness while top results for "she" were homemaker, nurse and receptionist.[25]

Word embeddings are essentially algorithms that assign numbers to words based on how the words are popularly used online, to make them machine-readable. The words "flower" and "candy" would be assigned numbers associated with other pleasant objects or emotions, while "death" or "greed" would be closer to things that are generally perceived as unpleasant. Most computer programs rely on word embeddings, such as the feed on a social media site, search engines and programs that target ads.

Machine-learning algorithms, according to studies, have identified "cold" and "sassy" as female characteristics while "guru" and "cocky" are considered male.[26] As a result of the data that the computer relies on—mostly biased against women—the AI replicates the same prejudice against women found online and offline, and propagates stereotypes. If an organisation were to write up a program to recruit a computer programmer using AI—the AI agent would associate the word "programmer" to a man and would throw up a male candidate. If the example was turned on its head and the AI was programmed to look for a nurse, the machine would respond with a female candidate.

Biases creeping into these seemingly neutral systems can be dangerous as they are hard to identify. Algorithms are commonly perceived to be gender-neutral but have been found to exacerbate existing biases: women cannot apply for high prestige jobs if they do not see them being advertised. This is because the lack of women in these jobs reinforces the illusion that women are more suited for administrative roles, resulting in the algorithm not displaying traditionally "male-suited" job positions to females, making it a chicken and egg problem.

This situation is tricky to address as Google is simply a window into organised data- most of which is inherently biased and over which Google has no control. In the US, where the police departments are increasingly using data-driven risk-assessment tools for "predictive policing" and crime prevention, biased data sets can lead to these softwares perpetuating racial prejudice by over-surveilling and over-policing traditionally poorer, non-white neighbourhoods while ignoring wealthier, white neighbourhoods. If such digital discrimination is allowed to go unchecked, it can become a part of everyday logic and algorithmic systems, in turn solidifying existing social hierarchies.[27]

It is clear that data-driven AI reflects the values of its creators. The onus thus lies on its creators to be vigilant about inclusivity and "de-bias" data sets that drive these algorithms. This is as much about actively overcoming prejudice as it is about avoiding lazy coding. A team of researchers from Microsoft and Boston University in 2016 came up with a technique to de-bias word embeddings by teaching the algorithm to disassociate words with genders.[28] For some words, however, the scientists instructed the algorithm to retain the relationship: a "mother" or a "sister" must be identified as female. This to ensure that health advertisements or opportunities for women can still be targeted towards them.

However, there are some technical issues with de-biasing, mainly that it may lead to the elimination of a lot of useful data. Also, de-biasing can lead to change in nature of data, which in turn can result in poor machine learning/artificial intelligence models. This can happen because de-biasing may leave out a lot of data that is important for training such models, or it may lead to data sets becoming different from the real-world data being present on the internet. Therefore, it is important that AI bots be trained on data that they are going to encounter in the real world for them to be effective. As de-biasing may lead to poorly trained AI systems, at present there seems to be a situational trade-off between making sure that AI is not sexist and at the same time giving it data sets that allow it to be effective in use.

Gender in AI

In its 2016 Report, the White House's Office of Science and Technology Policy called the

shortage of women and other minorities "one of the most critical and high-priority challenges for computer science and AI."[29] The report acknowledged the role of the government in the growth of AI, through investment in research and development of a skilled and diverse workforce. The latter to ensure that the processes behind AI account for justice, fairness and safety and not allow for the developers' biases to creep in, whether intentional or not.

A 2014 study by Gartner, an IT research and advisory corporation, found that only 11.2 percent of technology leadership jobs in Europe, Africa and the Middle East were occupied by women.[30] The corresponding percentage for Asia stood at 11.5 percent, while it was 13.4 percent in Latin America and 18.1 percent in North America. Globally, women are disturbingly underrepresented in STEM (the fields of Science, Technology, Engineering and Mathematics). Women's average representation in AI and robotics research is worse, the percentage of women in AI research in commercial industries has been quoted to be as abysmal as 5 percent.[31] This lack of diversity results in the absence of crucial inputs and insights in the development of AI and makes it susceptible to learning stereotypes. Experts consider today's greatest existential risks—all spawning from advanced technologies, such as nuclear weapons and nanotechnology—to also include artificial superintelligence.[32] Torres argues that for humanity to overcome these risks, we need the smartest people working to solve the problem and that includes women.[33]

Experts have noted that technology and gender are both socially constructed, and one cannot be understood without the other.[34] The association of technology with masculinity, Bray notes, can be found in daily experiences of gender, historical narratives, employment practices, and the design of new technologies since technology is seen as the "driving force of progress."[35] This is evident, as Torres summarises, when women are said to be less inclined towards certain fields due to a lack of visible role models, expectations of family care, discrimination at workplaces, and finally the perception that women would be less suitable for certain disciplines, that they would be better at professions that focus on "people" rather than "things."[36]

The lack of gender diversity in AI is troubling as it would have serious implications on how the technology develops. Engineers play an important role in evaluating designs, ensuring that the system is not biased and is accountable. In the above example where the developer writes the code for finding resumes for a programmer position in a company, the developer has to make sure that the algorithm is not biased against female applicants. This is a huge responsibility to bestow on the creators since detecting biases beforehand may be difficult. Word embeddings act as dictionaries that programmers plug into different applications: a developer would have to be diligent before using a hand-me-down word embedding. And as engineers de-bias data and "train" algorithms, ascribing values to words, creators are at a position to incorporate ethics into the architecture of the AI. If robots are learning from humans, the engineers must be diverse to ask the right questions. Studies have proven, for instance, that the collective intelligence of a group vastly improves if women are involved.[37]

The culture in Silicon Valley—hosting some of the companies that work at the forefront of AI—has also been under the scanner in the past year. The technology sector ranks amongst the lowest in gender diversity.[38] The former Uber employee's take on the sexism prevalent in the industry brought the issue to limelight once again,[39] with some describing Silicon Valley as plain "awful" to women.[40] Studies have shown that women in tech leave their jobs at twice the rate that men do.[41] Women are asked to do things that men would not have to do; they do not have the same opportunities as their male counterparts.[42] As Silicon Valley gains fame for its "white bro" culture[43]—one where those with boorish behaviour are said to rule the roost—companies are in a drive for diversity, seemingly desperate to increase the number of their female employees. Commentators, on the other hand, point out that that these companies instead hire women in non-technical positions to display parity. This when tech companies with higher gender diversity across roles have been proved to be more profitable than the rest.[44]

Initiatives such as the Partnership for AI—established by Google, Amazon, IBM and others at the cutting edge of the technology—have recognised that in the absence of baseline ethics and common standards in AI, research and commercial use of AI cannot advance. The thematic pillars for the partnership are transparent and accountable AI, and social and societal influence of AI.[45] The AI Now symposium, an initiative led by female researchers that studies the impact of AI on society, identified specific problem areas such as limitations in access to data resources and the difficulty in assessing algorithms.[46] The grouping has recommended diversifying and broadening access to resources such as data sets and training by making the field more inclusive and including more opportunities for people to participate in AI development and deployment.[47] To address accountability in algorithms, the group

recommended establishing mechanisms involving notification to users who are subject to automated decision-making and providing opportunities for redressal.

Conclusion

As patriarchy and prejudice become encoded in machines, fighting bias in data and deployment through increasing diversity in AI research will become important. As machine learning permeates every aspect of people's lives, AI is no longer a mere object of science fiction. Take the recent United Nations-supported summit in Geneva, "AI for Good." that focused on the potential of using AI technologies for achieving the Sustainable Development Goals by 2030. Participants recognised that complex development challenges faced by countries like India cannot be solved simply by the conventional linear approach. AI can aid and transform India's health and nutrition as well as education sectors. For instance, the Centre for Study of Science, Technology and Policy is presently working on a project in Karnataka that is attempting to use AI-based systems to improve delivery of child nutrition programmes. Image-recognition techniques are being developed to help in early identification of stunted growth, epidemics and other health issues.[48] However, for these solutions to be truly effective, the data sets must be free of bias and the development, inclusive.

In India, the legal sector is gradually embracing AI, which is expected to improve speed and efficiency by automating tasks such as document drafting, undertaking legal research and due diligence. Similarly, new-writing bots are now functioning in the world of journalism. In both cases, AI will autonomously generate output by identifying story angles based on algorithms with "built-in" criteria. When cases involving sexual violence and their portrayal in traditional news media are already under scrutiny, it is important to question how male-hegemonic data sets will impact future news stories and liability of sexual assault and other areas that require greater gender sensitivity. Data sets will suffer from a lack of representation when only 29 percent of internet users and 28 percent of mobile phone owners in India are women, making access to basic ICT services and infrastructure critical.

Eric Berridge, the CEO of Bluewolf, earlier this year, called AI the perfect partner to increase gender diversity in organisations, to use AI as an accountability layer to identify bias in areas like hiring and promotion.[49] Companies, for instance, are already using AI to study how job descriptions can encourage female applicants. Words such as "dominant" and "ninja" in job profiles have deterred women from applying before. Companies are looking at changing their language to appeal to a larger audience: a welcome move when companies list "always be hustlin" as a core value.[50] With the growing momentum around using AI to increase accountability in existing sectors, the code itself must be made accountable first.

ENDNOTES

01

1. See, e.g.
   "U.S.-ROK-Japan Experts Meeting on Cybersecurity of Critical Infrastructure," Media Note, US Department of State, 19 December 2016, https://2009-2017.state.gov/r/pa/prs/ps/2016/12/265783.htm; and UK Chancellor of the Exchequer Philip Anthony Hammond, Speech at Microsoft "Future Decoded" Conference, 1 November 2016, https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy, accessed 28 April 2017.

2. An institutionalised riot system involves "calculated and deliberate actions by key individuals, the conveying of messages, recruitment of participants, and other specific types of activities, especially provocative ones, that are part of a performative repertoire." Paul R. Brass, "Development of an Institutionalised Riot System in Meerut City, 1961 to 1982," Economic and Political Weekly, 30 October 2004, http://www.paulbrass.com/files/Epwarticle.pdf, accessed 28 April 2017. Also available in print form.

3. Malaysian Minister of Home Affairs Ahmad Zahid Hamidi, Response to a question in the Parliament of Malaysia, Hansard, 25 May 2015, 3.

4. For an interesting take on how social media killed the poison-pen letter, see Syed Nazri, "The dying art of the surat layang," New Straits Times, 6 December 2016, http://www.nst.com.my/news/2016/12/194787/dying-art-surat-layang, accessed 28 April 2017.

5. Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security, 7 October 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national, accessed 29 April 2017.
   "Grizzly Steppe: Russian Malicious Cyber Activity," Joint Analysis Report by the Department of Homeland Security and the Federal Bureau of Investigation, 29 December 2016, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf, accessed 29 April 2017.

6. See, e.g.
   Case Concerning the Military and Paramilitary Activities against Nicaragua (Nicaragua v. United States of America), International Court of Justice, 27 June 1986, http://www.icj-cij.org/docket/?p1=3&p2=3&case=70&code=nus&p3=4; and Dov H. Levin, "Partisan electoral interventions by the great powers: Introducing the PEIG Dataset," Conflict Management and Peace Science, 19 September 2016.

7. FireEye, Digital Bread Crumbs: Focusing Seven Clues To Identifying Who's Behind Advanced Cyber Attacks, 2014, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-digital-bread-crumbs.pdf, accessed 29 April 2017.
   Nicholas Tsagourias, "Cyber attacks, self-defence and the problem of attribution," Journal of Conflict and Security Law 17, no. 2 (2012): 229–44.
   "State Responsibility for Cyber Operations: International Law Issues," Event Report, British Institute of International and Comparative Law, 9 October 2014, https://www.biicl.org/documents/380_biicl_report_-_state_responsibility_for_cyber_operations_-_9_october_2014.pdf?showdocument=1, accessed 29 April 2017.

8. Richard A. Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What to do about It (Ecco/Harper Collins, 2010), 249. Cf. Marco Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations," Texas International Law Journal 50, no. 2 (2015): 233-73.

9. Roscini, op. cit.

02

1. See http://news.nationalpost.com/news/canada/canadian-politics/electoral-fraud-did-take-place-in-2011-federal-vote-but-it-didnt-affect-outcome-judge-rules.

2. See https://www.theguardian.com/politics/2016/apr/22/barack-obama-brexit-uk-back-of-queue-for-trade-talks.

3. See, e.g. https://en.wikipedia.org/wiki/French_constitutional_referendum,_1800.

4. See https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0.

5. See Thucydides, The Peloponnesian War.

6. See http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/27/opm-attack-hack-china-cybersecurity-personal-data-suspect-espionage-verifiable-/29341789/; and https://www.the-american-interest.com/2015/06/16/former-cia-head-opm-hack-was-honorable-espionage-work/.

7. See generally Federalist Papers.

8. See, e.g. "Briefing: Cyber Espionage," Jane's Defence Weekly, 9 November 2015.

9. See https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

10. James R. Clapper, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, 12 March 2013.

11. See https://sg.finance.yahoo.com/news/Anonymous-exposes-visitors-afpsg-2809071407.html; and http://asia.nikkei.com/Business/Trends/Hackers-turn-stock-advisers-as-Anonymous-targets-China-Inc?page=1.

12. See http://www.af.mil/News/Article-Display/Article/127729/operation-achilles-leaflet-airdrop-delivers-message-to-taliban/.

13. See https://www.wired.com/2016/08/twitter-says-suspended-360000-suspected-terrorist-accounts-year/.

14. See https://www.britannica.com/topic/Bolshevik; and http://www.historytoday.com/richard-cavendish/bolshevik-menshevik-split.

15. See http://news.nationalgeographic.com/2016/06/iceland-greenland-name-swap/. See also https://www.scientificamerican.com/article/proof-on-ice-southern-greenland-green-earth-warmer/.

16. See https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.f575e36dfcd2.

17. See http://www.reuters.com/article/us-usa-election-facebook-idUSKBN1380TH.

18. See Protocol Additional to the Geneva Conventions of 12 August 1949; and Relating to the Protection of Victims of International Armed Conflicts (hereinafter Protocol 1), Article 37, 8 June 1977.
See also Protocol 1, Article 39.

19. Protocol 1, Article 39(3).
See also Protocol 1, Article 37(2).

03

1. Consultation Note on Model for Nation-wide Interoperable and Scalable Public Wi-Fi Networks, Telecommunications Regulatory Authority of Italy, November 2016.

2. "The Digital India programme is a flagship programme of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy." See http://www.digitalindia.gov.in/.

3. Cf. United Nations General Assembly 2030 Agenda, A/RES/70/1, "Transforming our world: The 2030 Agenda for Sustainable Development," https://sustainabledevelopment.un.org/post2015/transformingourworld.

4. "Consultation Paper on Proliferation of Broadband through Public Wi-Fi Networks," Telecommunications Regulatory Authority of India, July 2016.

5. "The role of ICT in advancing growth in least developed countries - Trends, challenges and opportunities," International Telecommunication Union, Geneva, Switzerland, 2011.

6. Gordon A. Gow and Jennifer Parisi, "Pursuing the Anonymous User: Privacy Rights and Mandatory Registration of Prepaid Mobile Phones," Bulletin of Science, Technology and Society 28, no. 1 (February 2008): 60–68.

7. "Mandatory registration of prepaid SIM cards Addressing challenges through best practice," GSM Association, April 2016, http://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf.

8. Prashant Iyengar, "IP Addresses and Expeditious Disclosure of Identity in India," Centre for Internet and Society, 22 August 2011, http://cis-india.org/internet-governance/front-page/ip-addresses-and-identity-disclosures, accessed 14 April 2017.

9. Kevin P. Donovan and Aaron K. Martin, "The rise of African SIM registration: The emerging dynamics of regulatory change," First Monday 19, no. 2–3 (February 2014), http://journals.uic.edu/ojs/index.php/fm/article/view/4351/3820.

10. "GSMA, The Mandatory Registration of Prepaid SIM Card Users a White Paper," GSM Association, November 2013, http://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_WhitePaper_MandatoryRegistrationofPrepaidSIM-Users.pdf.

11. Nicola Jentzsch, "Implications of Mandatory Registration of Mobile Phone Users in Africa," DIW Berlin Discussion Paper No. 1192, 1 March 2012, https://ssrn.com/abstract=2017490.
12. Note that causality may run in the reverse: in countries where mobile competition is diverse, it may be that the mobile industry carries a sufficiently strong political voice to get an audience for their reluctance to administrative requirements, especially if they lack an evidential base.

13. Internet Service Providers Association of India, Response to TRAI Consultation Note on "Model for Nation-wide Interoperable and Scalable Public Wi-Fi Networks," 2016, http://www.trai.gov.in/sites/default/files/ISPAI_15_Nov_2016.pdf.

14. Association of Unified Telecom Services Providers India, Response to the TRAI's Consultation Note on "Model for Nationwide Interoperable and Scalable Public Wi-Fi," December 2016, http://www.trai.gov.in/sites/default/files/AUSPI_15_Nov_2016.pdf.

15. Internet and Mobile Association of India (IAMAI), Submission on TRAI Note on "Model for Nationwide Interoperable and Scalable Wi-Fi Networks," December 2016, http://www.trai.gov.in/sites/default/files/IAMAI_15_Nov_2016.pdf.

16. See supra note 1.

17. Stefano Maffei and Isabella Merzagora Betsos, "Crime and Criminal Policy in Italy:

Tradition and Modernity in a Troubled Country," European Journal of Criminology 4, no. 4(2007): 461–82, 1477–3708.

18. Riccardo Pelizzo, "Nihil Novi Sub Sole? Executive Power, the Italian Parlamento and the 'War on Terror'," The Journal of Legislative Studies 15, no. 2–3 (September 2009): 277–93.

19. Silvia B‹isi, "To be or not to be (anonymous)? Riflessioni in tema di libertà e controllo," Centro Nexa su Internet and Società, Politecnico di Torino, 2011, 28, https://nexa.polito.it/nexafiles/anonimato-in-rete.pdf, accessed 20 April 2017.

20. Ibid., 28.

21. Ibid., 36.

22. Ibid., 29.

23. Ibid., 30.

24. Andreas Kornelakis, "Inclusion or Dualization? The Political Economy of Employment Relations in Italian and Greek Telecommunications," British Journal of Industrial Relations 0007–1080 (June 2016): 385–408.

25. Ibid.

26. Cf. Commission Directive 90/388/EEC of 28 June 1990 on competition in the markets for telecommunications services, and follow-up EU level initiatives such as the first ePrivacy directive of 1997, the telecommunications package of 2002, the new ePrivacy directive of 2002 and revised telecommunications package of 2009.

27. Cf. EU Commission Digital Score Board, https://ec.europa.eu/digital-single-market/en/digital-scoreboard.

28. See, e.g. Contributions to European legislative processes or enforcement processes by ETNO (European Telecommunications Network Operator's Association), ECTA (European Competitive Telecommunications Association), DFMonitor or FTTH Council.

29. Eco (Verband der Internetwirtschaft e.V.), "Großes Potenzial von WLAN in Deutschland bislang ungenutzt," Survey Report, 4 November 2014, https://www.eco.de/2014/pressemeldungen/eco-studie-zeigt-grosses-potenzial-von-wlan-in-deutschland-bislang-ungenutzt.html.
An English-language summary of the report is available at https://international.eco.de/2014/press-releases/eco-study-shows-great-potential-of-wi-fi-in-germany-so-far-untapped.html.

30. All translations from the Italian are by the author.

31. Alessandro Gilioli, "Carta dei cento per il libero Wi-Fi," L'Espresso, 26 November 2009, http://gilioli.blogautore.espresso.repubblica.it/2009/11/26/la-carta-dei-cento-per-il-libero-wi-fi/, accessed 16 April 2017.

32. Alessandro Gilioli, "Wi-Fi: anche Pisanu Ł contro il decreto Pisanu," L'Espresso, 3 December 2009, http://gilioli.blogautore.espresso.repubblica.it/2009/12/03/wi-fi-anche-pisanu-e-contro-il-decreto-pisanu/, accessed 16 April 2017.

33. Raffaele Mastrolonardo, "A new dawn for wi-fi: Why using a public network in Italy no longer means showing your passport," ZDNet, 6 September 2013, http://www.zdnet.com/article/a-new-dawn-for-wi-fi-why-using-a-public-network-in-italy-no-longer-means-showing-your-passport/, accessed 16 April 2017.

34. Alessio Beltrame, "Italia Wi-fi, ecco il progetto del governo per connettere il Paese," Corriere Comunicazioni, 2 December 2016, http://www.corrierecomunicazioni.it/digital/44754_italia-wi-fi-ecco-il-progetto-del-governo-per-connettere-il-paese.htm, accessed 16 April 2017.

35. Internet@Italia 2014 L'uso di Internet da parte di cittadini e imprese, Istituto Nazionale di Statistica (Roma: Fondazione Ugo Bordino, 2015), http://www.istat.it/it/files/2015/12/Internet@Italia2014.pdf, accessed 20 April 2017.

36. "Consultation Paper on Proliferation of Broadband through Public Wi-Fi Networks," Telecommunications Regulatory Authority of India, July 2016.

37. Regulation No. 820-1/2008-DS Pt.II, "Instructions under the Internet Service License regarding provision of Wi-Fi Internet services under delicensed frequency band," Department of Telecommunications, Government of India, 23 February 2009, http://www.dot.gov.in/sites/default/files/Wi-%20fi%20Direction%20to%20ISP%2023%20Feb%2009_3_0.pdf?download=1.

38. See, e.g. "Analysis: Data Protection in India - Getting It Right," 27 April 2017, https://cis-india.org/internet-governance/news/inforisk-today-april-26-2017-suparna-goswami-varun-haran-analysis-data-protection-in-india-getting-it-right/.

39. Arun Mohan Sukumar, "The national security case against Aadhaar," Observer Research Foundation, March 2017, http://www.orfonline.org/research/the-national-security-case-against-aadhaar/.

04

1. "Asia Marketing Research, Internet Usage, Population Statistics and Facebook Information," Internet World Stats, 2016, http://www.internetworldstats.com/asia.htm.

2. "Cisco Visual Networking Index: Forecast and Methodology, 2015-2020," Cisco, 2016, http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf.

05

1. The title is a quote from the campaign "WagesForFacebook.com," founded by Laurel Ptak, a professor at New York City's New School. Last accessed 6 September 2017.

2. "India worst hit by Petya in APAC, 7th globally: Symantec," Economic Times, 29 June 2017 http://economictimes.indiatimes.com/tech/internet/india-worst-hit-by-petya-in-apac-7th-globally-symantec/articleshow/59367013.cms.

3. "After Petya, WannaCry attacks, experts say India vulnerable to cyber attacks/http," The Financial Express, 29 June 2017, www.financialexpress.com/industry/after-petya-wannacry-attacks-experts-say-india-vulnerable-to-cyber-attacks/740350/.

4. Aadhaar is a 12-digit unique-identity number issued to Indian residents based on their biometric and demographic data. The data is collected by the Unique Identification Authority of India (UIDAI). Over 99 percent of Indians aged 18 and above had been enrolled for Aadhaar.

5. "Information Security Practices of Aadhaar (or lack thereof): A documentation of public availability of Aadhaar numbers with sensitive personal financial information," Centre for Internet and Society, 16 May 2017, https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1.

6. Alexa is an intelligent personal assistant developed by Amazon. It is capable of voice interaction, music playback, making to-do lists, setting alarms, streaming podcasts, playing audio books, and providing weather, traffic and other real-time information, such as the news. Siri is the intelligent personal assistant part of Apple's operating system.

7. "Facebook's failure: did fake news and polarized politics get Trump elected?" The

Guardian, 10 November 2016, https://www.theguardian.com/technology/2016/nov/10/facebook-fake-news-election-conspiracy-theories.

8. "The Rising Connected Consumer in Rural India," Boston Consultancy Group, 10 August 2016, https://www.bcgperspectives.com/content/articles/globalization-customer-insight-rising-connected-consumer-rural-india/.

9. "The addiction that's worse than alcohol or drug abuse," BBC News, 10 April 2017, http://www.bbc.com/capital/story/20170417-the-addiction-thats-worse-than-alcohol-or-drug-abuse.

10. India stack refers to a series of connected systems that allow people to store and share their data. These could include bank statements, medical records, birth certificates or tax filings. It includes Aadhaar information, an Aadhaar Payments Bridge System, which essentially turns an Aadhaar number into the person's financial address, and a consent layer to share personal data such as health records and financial transactions with a bank, insurer, employer or university for a limited time for a specific purpose.

11. Julia Angwin, Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance (New York: Times Books, 2014).

12. "Metadata Investigation: Inside Hacking Team," Share Foundation, 29 October 2015, https://labs.rs/en/metadata/.

13. E. Alex Jung, "Wages for Facebook," Dissent Magazine, Spring 2014, https://www.dissentmagazine.org/article/wages-for-facebook.

14. Matt Thompson, "Advertising That Exploits Our Deepest Insecurities," The Atlantic, 28 June 2017, https://www.theatlantic.com/technology/archive/2017/06/advertising-that-exploits-our-deepest-insecurities/532038/.

15. Adam Tanner, "Different Customers, Different Prices, Thanks To Big Data," Forbes, 26 March 2014 https://www.forbes.com/sites/adamtanner/2014/03/26/different-customers-different-prices-thanks-to-big-data/#149e3b0e5730.

16. Michael Fertik, "The Rich See a Different Internet Than the Poor," Scientific American, 1 February 2013, https://www.scientificamerican.com/article/rich-see-different-internet-than-the-poor/.

17. Lazzarato, quoted in E. Alex Jung, op. cit.

18. wagesforfacebook.com

19. "Where is the World's Data being stored," Mozy-Dell Inforgraphics, http://mozy.com/infographics/where-is-the-worlds-data-stored/.

20. Rob Crossley, 'Where in the World is my data, and How Secure is it?" BBC News, 9 August 2016, http://www.bbc.com/news/business-36854292.

21. "Indian business prepares to tap into Aadhaar, a state-owned fingerprint-identification system," The Economist, 24 September 2016, https://www.economist.com/news/business/21712160-nearly-all-indias-13bn-citizens-are-now-enrolled-indian-business-prepares-tap.

22. Mathew Jenkin, "Tablets out, imagination in: the schools that shun technology," The Guardian, 2 December 2015, https://www.theguardian.com/teacher-network/2015/dec/02/schools-that-ban-tablets-traditional-education-silicon-valley-london.

23. Jules Suzdaltsev, "There's a Social Network That Costs $9,000 to Join," Vice, 17 September 2014, https://www.vice.com/en_us/article/vdpqmx/this-guy-is-creating-a-facebook-for-rich-people-917.

24. Adrian Chen, "The Labourers that keep dick pics and beheadings out of your Facebook

feed," Wired, 23 October 2014, https://www.wired.com/2014/10/content-moderation/.

06

1. For further analysis, see Thomas Rid, "Cyberwar and Peace," Foreign Affairs 92, no. 6 (2013): 77–87.

2. Michael Schwirtz and Joseph Goldstein, "Russian Espionage Piggybacks on a Cybercriminal's Hacking," The New York Times, 12 March 2017, https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html?_r=0, accessed 15 March 2017.

3. Garrett M. Graff, "Inside the Hunt for Russia's Most Notorious Hacker," Wired Magazine, 21 March 2017, https://www.wired.com/2017/03/russian-hacker-spy-botnet/, accessed 25 March 2017.

4. Michael Corkery and Matthew Goldstein, "North Korea Said to Be Target of Inquiry Over $81 Million Cyberheist," The New York Times, 22 March 2017, https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html, accessed 25 March 2017.
5. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," Journal of Strategic Studies 38, no. 1-2 (2015): 33.

6. "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," The United States Department of Justice, 15 March 2017, https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions, accessed 6 April 2017.

7. See, e.g. "German media: cyber attack carried out on Bundestag," DW, 15 May 2015, http://www.dw.com/en/german-media-cyber-attack-carried-out-on-bundestag/a-18452770; "France fights to keep Macron email hack from distorting election," Reuters, 6 May 2017, http://www.reuters.com/article/us-france-election-idUSKBN1820BO.
8. "Security and international cooperation dominate today's cyber policy landscape," Journal of Cyber Policy 1, no. 1 (2016): 134.

9. "Fact Sheet: President Xi Jinping's State Visit to the United States," The White House of President Barack Obama, 25 September 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states, accessed 6 April 2017.

10. Scott Warren Harold, Martin C. Libicki and Astrid Stuth Cevallos, Getting to Yes with China in Cyberspace (Santa Monica, CA: RAND Corporation, 2016), 87, https://www.rand.org/pubs/research_reports/RR1335.html.

11. Jason Healey and Barry Hughes (2016) quoted in Carl Bildt and Gordon Smith, "The one and future Internet," Journal of Cyber Policy 1, no. 2 (2016): 152.

12. "'Avalanche' Network Dismantled in International Cyber Operation," Europol, 1 December 2016, https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation, accessed 6 April 2017.

13. Rid and Buchanan, "Attributing Cyber Attacks," 25.

14. "Cyber attacks: EU ready to respond with a range of measures, including sanctions," Council of the European Union, 19 June 2017, http://www.consilium.europa.eu/press-releases-pdf/2017/6/47244660913_en.pdf, accessed 23 July 2017.

15. See, e.g. "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say," The New York Times, 6 July 2017, https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html; "Hackers target Irish energy networks amid

fears of further cyber attacks on UK's crucial infrastructure," The Independent, 15 July 2017, http://www.independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html.

16. "CommuniquØ from the G20 Finance Ministers and Central Bank Governors Meeting Baden-Baden, Germany, 17-18 March 2017," G20, 18 March 2017, http://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/g20-communique.pdf;jsessionid=60A482D741862F3F01EFD61050EE0BAD?_blob=publicationFile&v=3, accessed 23 July 2017.

17. Bildt and Smith, "The one and future Internet," 152.

18. HM Government, "National Cyber Security Strategy 2016 to 2021," 63 [online], 1 November 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, accessed 8 April 2017.

19. Global Commission on Internet Governance, "One Internet," Centre for International Governance Innovation, The Royal Institute for International Affairs and Chatham House, 2016, https://www.ourinternet.org/report, accessed on 20 March 2017.

20. Joseph S. Nye Jr., "Will the Liberal Order Survive?" Foreign Affairs 96, no. 1 (2017): 16.

07

1. Lene Hansen and Helen Nissenbaum, "Digital disaster, cyber security and the Copenhagen School," International Studies Quarterly 53 (2009): 1161.

2. See for example: Ian Loader and Neil Walker, Civilizing Security (Cambridge: Cambridge University Press, 2007); Rita Abrahamsen and Michael Williams, Security beyond the State: Private Security in International Politics (Cambridge: Cambridge University Press, 2011); Joakim Berndtsson and Christopher Kinsey, eds., The Routledge Research Companion to Security Outsourcing (London: Routledge, 2016); Rita Abrahamsen and Anna Leander, eds., Routledge Handbook of Private Security Studies (London: Routledge, 2016).

3. Abrahamsen and Williams, Security beyond the State.

4. Ibid., 119.

5. Max Weber, The Vocation Lectures. Science as a Vocation/Politics as a Vocation (Cambridge, Indianapolis: Hackett Publishing, 2004/1919).

6. Janice Thomson, Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe (Princeton: Princeton University Press, 1994).

7. Michael Williams, "Global security assemblages," The Routledge Handbook of Private Security Studies, eds. Rita Abrahamsen and Anna Leander (London: Routledge, 2016), 131.

8. Ibid., 131.

9. Ian Loader, "Plural Policing and Democratic Governance," Social and Legal Studies 9 (2000): 323.

10. Kathleen Eisenhardt, "Agency theory: An assessment and review," Academy of Management Review 14 (1989): 57-74.

11. Madeline Carr, "Public-private partnerships in national cyber-security strategies," International Affairs 92 (2016): 43-62.

12. Ibid., 44.

13. See e.g. David Garland, The Culture of Control. Crime and Social Order in Contemporary Society (Chicago: The University of Chicago Press, 2001), 124, who speaks of a strategy of responsabilisation.

14. Cited in Shane Harris, @War: The Rise of the Military Industry Complex (Boston and New York: Houghton Mifflin Harcourt, 2014), 167.

15. Benoit Dupont, "Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime," Crime, Law and Social Change 67 (2017): 97–116.

16. Ibid., 107.

17. Ibid., 112.

18. For an overview, see Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, eds., Access Denied: The Practice and Policy of Global Internet Filtering (Cambridge, Massachusetts: MIT Press, 2008); Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, eds., Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace (Cambridge, Massachusetts: MIT Press, 2010); Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, eds., Access Contested. Security, Identity, and Resistance in Asian Cyberspace (Cambridge, Massachusetts: MIT Press, 2011).

19. Ethan Zuckerman, "Intermediary Censorship," Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace, eds. Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (Cambridge: MIT Press, 2010).

20. Dennis Broeders, The Public Core of the Internet. An International Agenda for Internet Governance. (Amsterdam: Amsterdam University Press, 2015), 70.

21. Center for Cyber and Homeland Security, Into the Gray Zone. The Private Sector and Active Defense Against Cyber Threats (Washington: George Washington University, 2016), 10.

22. Juan Zarate, "The Cyber Financial Wars on the Horizon: The convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response," in Cyber Enabled Economic Warfare: An Evolving Challenge, ed. Samantha Ravich (Washington D.C.: Hudson Institute, 2015), 111.

23. Center for Cyber and Homeland Security, op. cit., 28.

24. Jeremy Rabkin and Ariel Rabkin, "Hacking back without cracking up," Series paper no. 1606, Hoover Institution, Stanford University, 2016, 8–9.

25. Wyatt Hoffman and Ariel Levite, Private Sector Cyber Defense. Can Active Measures Help Stabilize Cyberspace? (Washington D.C.: Carnegie Endowment for international Peace, 2017).

26. Ibid., 37.

27. Dennis Broeders, Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance, (Breda: The Netherlands Defence Academy, 2014), 42–43.

28. Ashley Deeks, "Confronting and Adapting: Intelligence Agencies and International Law," Virginia Law Review 102 (2016): 599– 685.

29. Vijay Padmanabhan, "Cyber warriors and the Jus in Bello," International Law Studies 89 (2013): 291–92.

30. Vincent Boulanin, "Cyber security and the arms industry," SIPRI Yearbook 2013: Armaments, Disarmament and International Security (Oxford University Press: Oxford, 2013), 223.

31. Richard Godfrey, Jo Brewis, Jo Grady and Chris Grocott, "The private military industry and neoliberal imperialism: mapping the terrain," Organization 21 (2014): 106–125; Elke Krahmann, States, Citizens and the Privatization of Security (Cambridge: Cambridge University Press, 2010).

32. Jospeh Nye Jr., "Deterrence and dissuasion in Cyberspace," International Security 41 (2017): 65–66.

33. Padmanabhan, "Cyber warriors," 291; see also: Sean Watts, "Combatant Status and Computer Network Attack," Virginia Journal of International Law 50 (2010): 391–447.

34. Aaron Ettinger, "The mercenary Moniker: Condemnations, contradictions and the politics of definition," Security Dialogue 45 (2014): 188.

35. For a detailed analysis see: Tim Maurer, "'Proxies' and Cyberspace," Journal of Conflict and Security Law 21 (2016): 383–403.

36. Scott Applegate, "Cybermilitias and Political Hackers – Use of Irregular Forces in Cyberwarfare," IEEE Security and Privacy (2011): 19.

37. Alexander Klimburg, "Mobilising cyber power," Survival 53 (2011): 41–60.

38. Nir Gazit, "State-sponsored Vigilantism: Jewish Settlers' Violence in the Occupied Palestinian Territories," Sociology 49 (2014): 440–41.

39. Maurer, op. cit., 395.

40. Joseph Nye Jr., "The regime complex for managing global cyber activities," Global Commission on Internet Governance, Paper Series 1 (2014).

08

1. Expanding Participation and Boosting Growth: The Infrastructure Needs of the Digital Economy," World Economic Forum, March 2015.

2. "World Development Report 2016: Digital Dividends," World Bank, 2016.

3. Alexander Klimburg and Hugo Zylberberg, Cyber Security Capacity Building: Developing Access (NUPI, September 2015).

4. William J. Drake, Vinton G. Cerf and Wolfgang Kleinwächter, "Internet Fragmentation: An Overview," World Economic Forum, January 2016.

5. "Internet" means "internetworks": several networks connected to each other through interoperable standards.

6. A good example of such governance mechanism is found in the principle of subsidiarity as used in the EU. As written in the Article 5 of the Lisbon Treaty: "Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and insofar as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level. The institutions of the Union shall apply the principle of subsidiarity as laid down in the Protocol on the application of the principles of subsidiarity and proportionality. National Parliaments ensure compliance with the principle of subsidiarity in accordance with the procedure set out in that Protocol." For more information, see "Protocol on the Application of the Principles of Subsidiarity and Proportionality," Official Journal of the European Union, no. C310 (2004): 619, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:310:0207:0209:EN:PDF.

7. William Audureau and Soren Seelow, "Comment fonctionnent les blocages de sites jihadistes en 7 questions," Le Monde, 17 March 2015, http://www.lemonde.fr/pixels/

article/2015/03/17/les-premiers-blocages-administratifs-de-sites-djihadistes-en-7-questions_4594952_4408996.html.

8. "Germany approves plans to fine social media firms up to €50m," The Guardian, 30 June 2017, https://www.theguardian.com/media/2017/jun/30/germany-approves-plans-to-fine-social-media-firms-up-to-50m.

9. Cyrus R. Vance Jr., François Molins, Adrian Leppard and Javier Zaragoza, "When Phone Encryption Blocks Justice," New York Times, 12 August 2015, https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html.

10. Natasha Lomas, "We want to limit use of e2e encryption, confirms UK minister," TechCrunch, 5 June 2017, https://techcrunch.com/2017/06/05/we-want-to-limit-use-of-e2e-encryption-confirms-uk-minister/.

11. S.S. Wimbledon Case, Permanent Court of International Justice, 1923.

12. Track 1.5 refers to diplomatic dialogues where participants represent governments, academia or companies.

13. Michael Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017).

14. The debate around the layers forming cyberspace is still very much active, with many convincing and competing models. Since this debate is not the primary focus of our paper, we adopted a simple four-layer model. Given the heavy emphasis on policy analysis, this model ensures a clear distinction of cyber security components that are affected through cyber security policymaking. The development of this framework was informed and influenced by other approaches, such as: David Clark's four-layer approach (David Clark, "Characterizing cyberspace: past, present and future," MIT CSAIL, 2010); Laura DeNardis' multistakeholder governance analysis (Laura DeNardis, "One Internet: An Evidentiary Basis - for Policy Making on Internet - Universality and Fragmentation," Global Commission on Internet Governance, Paper Series No. 38, 2016); Yochai Benkler's three-layer model (Yochai Benkler, Wealth of Networks: How Social Production Transforms Markets and Freedom (Princeton: Yale University Press, 2000)); Kevin Werbach's four-layer model (Kevin Werbach, "A Layered Model for Internet Policy," Journal on Telecommunications and High Tech Law 1, no. 37 (2002)); and Ron Deibert's national policy analysis (Ron Deibert, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," Canadian Defence and Foreign Affairs Institute, 2012).

15. However, further progress within UNGGE seems unlikely after the recent failure to find consensus for the latest version of a report. See Adam Segal, "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?" Net Politics, Council on Foreign Relations, 29 June 2017, https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

16. See OSCE Permanent Council, "Decision No. 1039: Development Of Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies," 909th Plenary Meeting PC Journal, no. 909, agenda item 2, OSCE (April 2012); OSCE Permanent Council, "Decision No. 1106 Initial Set Of Osce Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies," 975th Plenary Meeting PC Journal, no. 975, agenda item 1, OSCE (December 2013); Ministerial Council, "Draft Decision On OSCE Efforts Related To Reducing The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies," MC.DD/7/16/Rev.3 7, OSCE (December 2016).

17. This notion was developed at the National Science Foundation around 2008. See, e.g. Helen Gill, A Continuing Vision: Cyber-Physical Systems (Carnegie Mellon University: 2008), https://www.ece.cmu.edu/~electriconf/2008/PDFs/Gill%20-CMU%20Electrical%20Power%202008%20-%20%20Cyber-Physical%20Systems%20-%20A%20Progress%20Report.pdf.

18. One outlier that is worth mentioning is the EU since it has its own Commissioner for Digital Economy and Society. Moreover, national privacy authorities exist within EU member states.

19. Nick Wingfield and Cecilia Kang, "Microsoft Wins Appeals on Overseas Data Searches," New York Times, 14 July 2016, https://www.nytimes.com/2016/07/15/technology/microsoft-wins-appeal-on-overseas-data-searches.html.

20. See the DTE database published by ECIPE, "Digital Trade Estimates Project Database," ECIPE. http://ecipe.org/dte/database/.

21. See the full text of the regulation: "Regulation (EU) 2016/679 of the European Parliament and of the Council," Official Journal of the European Union L119 (2016): 1, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

22. See the full text of the Act: "Investigatory Powers Act of 2016," legislative.gov.uk, http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

23. See Joseph A. Cannataci, "Report A/HRC/34/60 of the Special Rapporteur on the right to privacy," Human Rights Council, www.ohchr.org/Documents/Issues/Privacy/A_HRC_34_60_EN.docx.

24. Lillian Ablon, Martin C. Libicki and Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," RAND Corporation, 2014.

25. "The 9/11 Commission Report," National Commission on Terrorist Attacks upon the United States, 2004.

26. "IBM Security Services 2014 Cyber Security Intelligence Index," IBM Global Technology Services, 2014, https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.

27. Harold Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter and Daniel Weitzner, "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," DSpace@MIT, 2015, https://dspace.mit.edu/handle/1721.1/97690.

28. Laura DeNardis, "One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation," Global Commission on Internet Governance, July 2016.

29. Dennis Broeders, "The public core of the Internet. An international agenda for Internet governance," WRR, 2015.

09

1. For a further analysis of this tripartite division, albeit from a "techno-pessimist" perspective, see Robert Gordon, "Is U.S. Economic Growth Over? Faltering Innovation Confronts the Six Headwinds," National Bureau of Economic Research Working Paper Series, August 2012, http://www.nber.org/papers/w18315.pdf.

2. David Autor, "Automation and Anxiety: Will smarter machines cause mass unemployment?" The Economist, 25 June 2016, https://www.economist.com/news/special-report/21700758-will-smarter-machines-cause-mass-unemployment-automation-and-anxiety.

3. For a fuller discussion of the 4IR, see Klaus Schwab, The Forth Industrial Revolution (New York: Crown Business, 2016), https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab. For a deeper examination of specific 4IR technologies referenced, see "Enabling the Next Production Revolution: The Future of Manufacturing and Services – Interim Report," OECD, June 2017, https://www.oecd.org/mcm/documents/Enabling-the-next-production-revolution-the-future-of-manufacturing-and-services-interim-report.pdf.

4. Jeffrey Voas, "NIST Special Publication 800-183: Networks of 'Things'," United States National Institute of Standards and Technology, July 2016, http://dx.doi.org/10.6028/NIST.SP.800-183.

5. Jeremy Faludi, Natasha Cline-Thomas and Shardul Agrawala, "3D printing and its environmental implications," The Next Production Revolution: Implications for Governments and Business, ed. Alistair Nolan, OECD, 10 May 2017, http://dx.doi.org/10.1787/9789264271036-en.

6. Alistair Nolan, ed., Enabling the Next Production Revolution, OECD, 10 May 2017, http://www.oecd.org/sti/ind/next-production-revolution.htm.

7. Sources various, cited in Alastair Nolan, "The next production revolution: Key issues and policy proposals," The Next Production Revolution: Implications for Governments and Business, ed. Alistair Nolan, OECD, 10 May 2017, 30, http://dx.doi.org/10.1787/9789264271036-5-en.

8. Klaus Schwab, "The Fourth Industrial Revolution: What It Means and How to Respond," Foreign Affairs, 12 December 2015, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

9. Frey and Osborne make particularly extreme predictions of the impact of automation; see Carl Benedikt Frey and Michael A. Osborne. "The Future of Employment: How Susceptible are Jobs to Computerisation?" Oxford University, 17 September 2013, http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

10. Ian Stewart, Debapratim De and Alex Cole. "Technology and people: the great job-creating machine," Deloitte, December 2014, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-technology-and-people.pdf.

11. "Automation and Anxiety: Will smarter machines cause mass unemployment?" The Economist, 25 June 2016, https://www.economist.com/news/special-report/21700758-will-smarter-machines-cause-mass-unemployment-automation-and-anxiety.

12. "The Future of Jobs: Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution," World Economic Forum, January 2016, http://www3.weforum.org/docs/WEF_FOJ_Executive_Summary_Jobs.pdf, 3.

13. Quoted in David Rotman, "Technology and Inequality," MIT Technology Review, 21 October 2014, https://www.technologyreview.com/s/531726/technology-and-inequality/.

14. Klaus Schwab, "The Fourth Industrial Revolution: What It Means and How to Respond," Foreign Affairs, 12 December 2015, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

15. Ibid.

16. Hellen Nissenbaum, "A Contextual Approach to Privacy Online," Daedalus, the Journal of the American Academy of Arts and Sciences 140, no. 4 (Fall 2011), https://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf.

17. Tanay Jaipuria, "Self-driving cars and the Trolley problem," Medium, 23 May 2015, https://medium.com/@tanayj/self-driving-cars-and-the-trolley-problem-5363b86cb82d.

18. "State v. Loomis," Harvard Law Review, 10 March 2017, https://harvardlawreview.org/2017/03/state-v-loomis/.

19. Matthew Hutson, "Even artificial intelligence can acquire biases against race and gender," Science, 13 April 2017, http://www.sciencemag.org/news/2017/04/even-artificial-intelligence-can-acquire-biases-against-race-and-gender.

20. For a nuanced discussion of data and competition issues, see Ania Thiemann and Pedro

Gonzaga, "Big Data: Bringing Competition Policy to the Digital Era – Background note by the Secretariat," OECD Directorate for Financial and Enterprise Affairs Competition Committee, 27 October 2016, https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf.

21. "Enabling the Next Production Revolution: The Future of Manufacturing and Services – Interim Report," OECD, June 2017, 25, https://www.oecd.org/mcm/documents/Enabling-the-next-production-revolution-the-future-of-manufacturing-and-services-interim-report.pdf.

22. Nicholas Davis, "What is the fourth industrial revolution?" World Economic Forum, 19 January 2016, https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/.

23. Jae-Hee Chang and Phu Huynh, "ASEAN in Transformation: The Future of Jobs At Risk of Automation," International Labour Organization, July 2016, 2, http://www.ilo.org/public/english/dialogue/actemp/downloads/publications/2016/asean_in_transf_2016_r2_future.pdf.

10

1. Don Tapscott and Alex Tapscott, "The Impact of Blockchain Goes Beyond Financial Services," Harvard Business Review, 10 May 2016, https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services.

2. Ibid.

3. Ibid.

4. Times News Network, "Onerous licensing regime killing legal digital music," The Times of India, 20 February 2014, http://timesofindia.indiatimes.com/business/india-business/Ford-India-focusing-on-non-metro-markets/articleshow/30691347.cms.

5. "Media and Entertainment Industry," IBEF, June 2017, https://www.ibef.org/industry/media-entertainment-india.aspx.

6. The Copyright Act, 1957, S. 13.

7. The Copyright Act, 1957, S. 14.

8. According to S. 2(d) of the Act, an "author means, – (i) in relation to a literary or dramatic work, the author of the work; (ii) in relation to a musical work, the composer; (iii) in relation to an artistic work other than a photograph, the artist; (iv) in relation to a photograph, the person taking the photograph; (v) in relation to a cinematograph film or sound recording, the producer; and (vi) in relation to any literary, dramatic, musical or artistic work which is computer generated, the person who causes the work to be created."

9. The Copyright Act, 1957, S. 17.

10. The Copyright Act, 1957, S. 30.

11. The Copyright Act, 1957, Ss. 31, 31A and 31B.

12. The Copyright Act, 1957, Ss. 31C, 31D and 32.

13. The Government of India recently notified certain amendments to the Finance Bill, 2017, which transferred the responsibilities of the Copyright Board to the IPAB. The IPAB was constituted under the Trade Marks Act, 1999, and already deals with appeals against orders of the Registrar of Trademarks, the Registrar of Geographical Indications, and the Controller of Patents.

14. The Copyright Act, 1957, S. 11.

15. The Copyright Act, 1957, S. 33.

16. Balaji Subramanian, "Updating Indian Copyright Law," Seminar, no. 687 (November 2015), http://www.india-seminar.com/2016/687/687_balaji_subramanian.htm.

17. Ibid., supra 12.

18. Indian Copyright Office, Copyright Societies.
19. ISRA was incorporated in 2013 under S. 25 of the Companies Act, 1956.

20. Josef Drexl, Copyright, Competition, and Development, Report, Max Planck Institute for Intellectual Property and Competition Law, 2013, http://www.wipo.int/export/sites/www/ip-competition/en/studies/copyright_competition_development.pdf.

21. Ibid.

22. Ibid.

23. Ibid.

24. Ibid.

25. Prashant Reddy, "Breaking down the basics of the Javed Akhtar-IPRS royalty dispute," Spicy IP (June 2011), https://spicyip.com/2011/06/breaking-down-basics-of-javed-akhtar.html.

26. Ibid.

27. Ibid., supra 16.

28. Ibid., supra 16.

29. The Copyright Act, 1957.

30. For a more detailed account of how the blockchain technology works, please see: Nikolei M. Kaplanov, "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation," Temple University Legal Studies Research Paper, March 2012, https://ssrn.com/abstract=2115203 or http://dx.doi.org/10.2139/ssrn.2115203.

31. Ibid.

32. Melanie Swan, Blockchain: Blueprint for a New Economy (Sebastopol: O'Reilly, 2015), 60–80.

33. Ibid.

34. Ibid.

35. Ibid.

36. Ibid.

37. Ibid.

38. Ibid.

39. Ibid.

40. BBVA Research, "Smart contracts: the ultimate automation of trust?" Digital Economy Outlook, 2015, https://www.bbva.com/en/wp-content/uploads/2016/11/Digital_Economy_Outlook_Oct15_Cap1.pdf

41. Ibid.

42. Ibid.

43. Ibid.

44. As agreed upon by the owner of the copyright and the rest of the artists working on the track.

45. Marcus O'Dair, "The Networked Record Industry: How Blockchain could transform the consumption and monetisation of recorded music," Nemode, March 2016, http://www.nemode.ac.uk/wp-content/uploads/2012/12/ODair-The-networked-record-industry-REPORT-1.pdf.

46. Ibid.

47. Ibid.

48. Ibid.

49. Trent McConaghy and David Holtzman, "Towards an Ownership Layer for the Internet," Ascribe GmbH, June 2015.

50. Marcus O'Dair, "The Networked Record Industry: How Blockchain could transform the consumption and monetisation of recorded music," Nemode, March 2016, http://www.nemode.ac.uk/wp-content/uploads/2012/12/ODair-The-networked-record-industry-REPORT-1.pdf.

51. Ibid., supra 30.

52. Marcus O'Dair, Music on the Blockchain (London: Middlesex University, 2016).

53. Marcus O'Dair, "The Networked Record Industry: How Blockchain could transform the consumption and monetisation of recorded music," Nemode, March 2016, http://www.nemode.ac.uk/wp-content/uploads/2012/12/ODair-The-networked-record-industry-REPORT-1.pdf.

54. A. Wright and P. De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," Working paper, http://ssrn.com/abstract=2580664, accessed 17 December 2015.

55. Ibid.

56. Ibid.

57. Ibid.

58. Ibid.

59. Marcus O'Dair, Music on the Blockchain (London: Middlesex University, 2016).

60. Ibid.

61. Ibid.

62. Ibid.

63. Ibid.

64. Ibid.

65. Ibid.

66. Ibid.

67. Ibid.

68. Dot Blockchain Music, http://dotblockchainmusic.com/.

69. Ibid.

70. Marcus O'Dair, Music on the Blockchain (London: Middlesex University, 2016).

71. Ibid.

72. Ibid.

73. Ibid.

74. Ibid.

75. Novex Communications is a content distributor in India that is the official assignee for all content created by major Indian production houses and record companies. As such, it offers public performance licences for all the content produced by these entities. For more information, please see: http://www.novex.in/public-performance-licenses/.

11

1. Satya Ramaswamy, "How Companies Are Already Using AI," Harvard Business Review, 14 April 2017. https://hbr.org/2017/04/how-companies-are-already-using-ai.

2. Martín Abadi and David G. Andersen, "Learning to Protect Communications with Adversarial Neural Cryptography," Cornell University Digital Library, https://arxiv.org/abs/1610.06918.

3. Roman V. Yampolskiy, "AI is the Future of Cybersecurity, for Better and for Worse," Harvard Business Review, 8 May 2017, https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse.

4. Darktrace, "NHS Agency Successfully Fought Back WannaCry Ransomware with Darktrace," Symantec, 12 May 2017, https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware.

5. Darktrace, "Case Study: The Scottish Government," Darktrace, N.D., https://www.darktrace.com/resources/cs-scottish-government.pdf.

6. Deloitte, "Artificial Intelligence in Government," Wall Street Journal CIO Journal, 31 May 2017, http://deloitte.wsj.com/cio/2017/05/31/artificial-intelligence-in-government/.

7. Parchi Patel, "Pittsburgh's AI Traffic Signals Will Make Driving Less Boring," IEEE Spectrum, 17 October 2016, http://spectrum.ieee.org/cars-that-think/robotics/artificial-intelligence/pittsburgh-smart-traffic-signals-will-make-driving-less-boring.

8. Emily Singer, "Decoding Flu Viruses Before an Outbreak," Quanta Magazine, 29 August 2013, https://www.quantamagazine.org/decoding-flu-viruses-before-an-outbreak-20130829/.

9. BI Intelligence, "The US is Investing $165 Million Into Smart City Solutions," Business Insider, 15 October 2016, http://www.businessinsider.com/the-us-is-investing-165-million-into-smart-city-solutions-2016-10/?IR=T.

10. Hannah Devlin, "AI programs exhibit racial and gender bias, research reveals," The Guardian, 13 April 2017, https://www.theguardian.com/technology/2017/apr/13/ai-programs-exhibit-racist-and-sexist-biases-research-reveals.

11. “A Global Black Market for Stolen Personal Data,” Trend Micro, last modified N.D., https://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/global-black-market-for-stolen-data/.

12. Commission on Enhancing National Cybersecurity, “Report on Securing and Growing the Digital Economy,” National Institute of Standards and Technology, 1 December 2016, https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

13. Sam Shead, “The Chinese Government is Funding a New Lab from China’s Most Powerful AI Company,” Business Insider, 23 February 2017, http://www.businessinsider.com/baidu-artificial-intelligence-lab-funded-by-chinese-government-2017-2/?IR=T&r=SG#8yHtX7PjX2gqZZWh.99.

14. Masaaki Demura, “Researchers to Develop Japanese-Style AI,” Nikkei Asian Review, 14 September 2016, http://asia.nikkei.com/Tech-Science/Tech/Researchers-to-develop-Japanese-style-AI.

12

1. Batya Friedman and Helen Nissenbaum, “Bias in Computer Systems,” ACM Transactions on Information Systems 14, no. 3 (July 1996): 330–347.

2. Osond Osaba and William Welser, “The Risks of Bias and Errors in Artificial Intelligence.”

3. “Nurture vs. Nature – The Sexist Nature of Artificial Intelligence,” Shout Out, 26 November 2016, https://shoutoutjmu.com/2016/11/.

4. Jack Clark, “Artificial intelligence has a ‘sea of dudes’ problem,” Bloomberg, 27 June 2016, https://www.bloomberg.com/professional/blog/artificial-intelligence-sea-dudes-problem/.

5. Francesca Bray, “Gender and Technology,” Annual Review of Anthropology 36 (2007): 37–53.

6. Vidisha Mishra and Samir Saran, “AI replicating same conceptions of gender roles that are being removed in real world,” The Economic Times, 17 June 2017, http://blogs.economictimes.indiatimes.com/et-commentary/ai-replicating-same-conceptions-of-gender-roles-that-are-being-removed-in-real-world/.

7. Tabi J. Gee, “Why female sex robots are more dangerous than you think,” The Telegraph UK, 5 July 2017, http://www.telegraph.co.uk/women/life/female-robots-why-this-scarlett-johansson-bot-is-more-dangerous/.

8. Ibid.

9. Ansgar Koene, “Algorithmic Bias – Addressing Growing Concerns,” IEEE Technology and Society Magazine, June 2017, http://ieeexplore.ieee.org/document/7947257.

10. Alistair Barr, “Google Mistakenly Tags Black People as ‘Gorillas,’ Showing Limits of Algorithms,” The Wall Street Journal, 1 July 2015, https://blogs.wsj.com/digits/2015/07/01/google-mistakenly-tags-black-people-as-gorillas-showing-limits-of-algorithms/.

11. Davey Alba, “Twitter Is Running Out of Time to Get Real About Fighting Abuse,” WIRED, 22 July 2016, https://www.wired.com/2016/07/twitter-running-time-get-real-fighting-abuse/.

12. Monica Nicklesburg, “Why is AI female? How our ideas about sex and service influence the personalities we give machines,” GeekWire, 4 April 2016, https://www.geekwire.com/2016/why-is-ai-female-how-our-ideas-about-sex-and-service-influence-the-personalities-we-give-machines/.

13. Ibid.

14. “Nurture vs. Nature – The Sexist Nature of Artificial Intelligence,” Shout Out, 26 November 2016, https://shoutoutjmu.com/2016/11/26/24246/.

15. Tyler Schnoebelen, “The gender of artificial intelligence,” Crowdflower Blog, 11 July 2016, https://www.crowdflower.com/the-gender-of-ai/.

16. Michael J. Coren, “Virtual assistants spend much of their time fending off sexual harassment,” Quartz, 25 October 2016, https://qz.com/818151/virtual-assistant-bots-like-siri-alexa-and-cortana-spend-much-of-their-time-fending-off-sexual-harassment/.

17. Jacqeline Feldman, “The Bot Politic,” The New Yorker, 31 December 2016, http://www.newyorker.com/tech/elements/the-bot-politic.

18. Tony Whitfield, “‘Siri, I was raped’: Study finds smartphone assistants unable to respond to help in a crisis,” Mirror, 15 March 2016, http://www.mirror.co.uk/tech/siri-raped-study-finds-smartphone-7559389.

19. Rhiannon Williams, “Siri update offers support for rape victims and suicide questions,” The Telegraph UK, 4 April 2016, http://www.telegraph.co.uk/technology/2016/04/04/siri-update-offers-support-for-rape-victims-and-suicide-question/.

20. Sophie Lord, “Gender and artificial intelligence: The five laws of branding AI,” Landor, 15 June 2017, https://landor.com/thinking/gender-and-artificial-intelligence-the-five-laws-of-branding-ai.

21. Tabi J. Gee, op. cit.

22. Laurie Penny, “Why do we give robots female names? Because we don’t want to consider their feelings,” NewStatesman, 22 April 2016, http://www.newstatesman.com/politics/feminism/2016/04/why-do-we-give-robots-female-names-because-we-dont-want-consider-their.

23. Tabi J. Gee, op. cit.

24. Byron Spice, “QUESTIONING THE FAIRNESS OF TARGETING ADS ONLINE,” Carnegie Mellon University, 7 July 2015, http://www.cmu.edu/news/stories/archives/2015/july/online-ads-research.html.

25. Tolga Bolukbasi et al., “Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings,” Advances in Neural Information Processing Systems, 2016, https://arxiv.org/pdf/1607.06520v1.pdf.

26. Byrd Pinkerton, “He’s Brilliant, She’s Lovely: Teaching Computers To Be Less Sexist,” NPR, 12 August 2016, http://www.npr.org/sections/alltechconsidered/2016/08/12/489507182/hes-brilliant-shes-lovely-teaching-computers-to-be-less-sexist.

27. Kate Crawford, “Artificial Intelligence’s White Guy Problem,” The New York Times, 25 June 2016, https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html.

28. In a recent paper, they’ve shown that if you tell the algorithms to ignore certain relationships, they can extrapolate outwards.

29. “Preparing for the Future of Artificial Intelligence,” Executive Office of the President National Science and Technology Council Committee on Technology, October 2016, https://obamawhitehouse.archives.gov/blog/2016/10/12/administrations-report-future-artificial-intelligence.

30. Samuel Gibbs, “Women in technology: no progress on inequality for 10 years,” The

Guardian, May 2014, https://www.theguardian.com/technology/2014/may/14/women-technology-inequality-10-years-female.

31. Jenny Darmody, "Are robots sexist? The danger of the lack of women in AI," Silicon Republic, 8 March 2017, https://www.siliconrepublic.com/people/robots-sexist-women-in-ai.

32. Phil Tores, "The Collective Intelligence of Women Could Save the World," Future of Life Institute, 13 June 2016, https://futureoflife.org/2016/06/13/collective-intelligence-of-women-save-world/.

33. Ibid.

34. M. Lohan and W. Faulkner, "Masculinities and technologies: some introductory remarks," Men Mascul 6 (2004): 319–329.

35. Francesca Bray, op. cit.

36. Supra n. 32.

37. Massachusetts Institute of Technology, "Collective intelligence: Number of women in group linked to effectiveness in solving difficult problems," Science Daily, 2 October 2010, https://www.sciencedaily.com/releases/2010/09/100930143339.htm.

38. "Women Employees Boost the Bottom Line for Tech Firms," Morgan Stanley, 3 May 2017, https://www.morganstanley.com/ideas/gender-diversity-tech-companies.

39. Susan Fowler, "Reflecting On One Very, Very Strange Year At Uber," Susan J. Fowler, 19 February 2017, https://www.susanjfowler.com/blog/2017/2/19/reflecting-on-one-very-strange-year-at-uber tore.

40. Liza Mundy, "Why Is Silicon Valley So Awful to Women?" The Atlantic, April 2017, https://www.theatlantic.com/magazine/archive/2017/04/why-is-silicon-valley-so-awful-to-women/517788/.

41. Catherine Ashcraft, Brad McLain and Elizabeth Eger, "Women in Tech: The Facts," National Center for Women and Information Technology, 2016, https://www.ncwit.org/sites/default/files/resources/womenintech_facts_fullreport_05132016.pdf.

42. Ibid.

43. Laura Colby, "Why So Few Women Break Through Tech's Bro Culture," Bloomberg, 2 June 2017, https://www.bloomberg.com/news/articles/2017-06-02/why-so-few-women-break-through-tech-s-bro-culture-quicktake-q-a.

44. "Thematic Pillars," Partnership on AI, https://www.partnershiponai.org/thematic-pillars/.

45. Ibid.

46. Madeline Elish, Solon Barocas, Aaron Plasek and Kadija Ferryman, "The AI Now Report, The Social and Economic Implications of Artificial Intelligence Technologies in the Near-Term," AI Now, 22 September 2016, https://artificialintelligencenow.com/media/documents/AINowSummaryReport_3_RpmwKHu.pdf.

47. Ibid.

48. Anshu Bharadawaj and Jai Asundi, "Using AI to achieve development goals," LiveMint, 12 July 2017, http://www.livemint.com/Opinion/VPfXlEDCtQVaGARCw4ZLRM/Using-AI-to-achieve-development-goals.html.

49. Eric Berridge, "AI Is The Perfect Partner To Achieve Gender Diversity," HuffPost, 14 April 2017, http://www.huffingtonpost.co.uk/eric-berridge/ai-gender-diversity_b_15956924.html.

50. Julia Wong, “Uber’s ‘hustle-oriented’ culture becomes a black mark on employees’ rØsumØs,” The Guardian, 7 March 2017, https://www.theguardian.com/technology/2017/mar/07/uber-work-culture-travis-kalanick-susan-fowler-controversy.

AUTHORS

Amelia Andersdotter

Amelia represents ARTICLE 19 in its work on human rights in WiFi standards at the IEEE, and in its monitoring work of HTTP status code 451. She has worked with internet policy advocacy since 2006. As a member of the European Parliament she worked on sectoral regulations promoting competition and interplay between technical and legal standards, as well as copyright reform. She now does policy research in the field of consumer rights in technology, privacy and data protection as well as IT security policies and continues to be an avid supporter of open standards and open software. She holds a BSc in Mathematics from the University of Lund, with an additional two years of studies in business law.

Chelsey Slack

Chelsey Slack works as a policy officer on cyber defence with the International Staff at NATO. She provides advice and supports the development and implementation of NATO's cyber defence policy. Previously, she worked at the Canadian Foreign Ministry focusing on conflict prevention. Chelsey earned a Master's Degree of Philosophy in International Relations from the University of Cambridge where she wrote her thesis on state behaviour in cyberspace. She studied as a Hansard Scholar at the London School of Economics and at the Institut d'Études Politiques de Lyon in France.

Dennis Broeders

Dennis Broeders is professor of Technology and Society at the Department of Public Administration and Sociology of the Erasmus University Rotterdam and a senior research fellow at the Dutch Scientific Council for Government Policy (WRR), an advisory body to the Dutch government within the Prime Minister's department. His research broadly focuses on the interaction between technology and policy, with specific areas of interest in cyber security governance, internet governance, surveillance and Big Data. He recently published the books, 'The public core of the internet: towards a new international agenda for internet governance' (2015, Amsterdam University Press) and 'Exploring the boundaries of Big Data' (ed., 2016, Amsterdam University Press).

Elina Noor

Elina Noor is Director, Foreign Policy and Security Studies, ISIS Malaysia. She was previously a key team member of the Brookings Institution's Project on US Relations with the Islamic World in its formative years post-September 11, 2001 and before that, did research on weapons of mass destruction terrorism at the Center for Nonproliferation Studies, Monterey Institute of International Studies in Washington, DC. Her policy interests include US-Malaysia bilateral relations, cyber warfare and security, radicalisation and terrorism, and major power relations. Her commentaries have appeared in local and foreign media, including *The New Straits Times, BFM, the New York Times, and Al-Jazeera.* She currently serves on the Global Commission on the Stability of Cyberspace.

Hugo Zylberberg

Hugo Zylberberg is a Cyber Fellow at Columbia University's School of International and Public Affairs where he coordinates the Tech & Policy Initiative. He studied Computer Science, Economics and Public Policy. He is also affiliated with the Chair on Values and Policies of Personal Data at Institut Mines-Télécom and the Castex Chair of Cyber Strategy in Paris, and

is Deputy Chair of the Research Advisory Group of the Global Commission on the Stability of Cyberspace. His research focuses on data protection, internet fragmentation, the digital transformation and international security issues.

Logan Finucan

Logan supports the implementation of advocacy strategies of several leading ICT clients including device manufacturers, electronic and network service providers, and satellite operators. He regularly provides analysis on key markets in the Asia-Pacific region, supports campaigns to shape spectrum management policies, and dispenses advice on the US legislative process. Areas of expertise include international trade regulations, data protection laws, internet governance, and multilateral processes.

Madhulika Srikumar

Madhulika Srikumar is a Junior Fellow with ORF's Cyber Initiative. A lawyer by training, she works at the intersection of policy, law and technology -- specifically how the law can act as both a safeguard against, and enabler of emerging technologies. Her current work focuses on the effect of technology on evolving societies, specifically the role of technology in urban mobility, capacity building for law enforcement, and bias in algorithmic decision-making.

Meghna Bal

Meghna Bal is a Junior Fellow with ORF's Cyber Initiative. A lawyer by training, her discursive interests span the gamut of issues related to technology policy. Her current research centres around Blockchain Technology, Artificial Intelligence, and Intellectual Property-related issues in India. Before foraying into policy studies, she played professional golf.

Michael Khoo

Michael Khoo is an Associate Research Director at TRPC, having first joined the company in 2011. He is a graduate of the University of Sydney, where he spent a year and graduated with a Master's degree in Political Economy. His overseas education has exposed him to the various schools of economic thought, many in contrast to that of mainstream orthodox economics today. Michael finished his Bachelor of Arts in Economics at the National University of Singapore. His research interests include video gaming, intellectual property rights, social media, and next-gen devices. He sees ICT as an integral part of the fabric of society today, particularly in promoting democracy and development.

Nikolas Ott

Nikolas Ott is a Mercator Fellow of International Affairs at the Mercator Program Center for International Affairs (Stiftung Mercator). His research focuses on how international legal norms and confidence-building measures help reduce conflict in cyberspace. During this fellowship, he worked at the Cyber Defence Section of the North Atlantic Treaty Organization (NATO), the NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) and the Transnational Threats Department of the Organization for Security and Co-operation in Europe (OSCE). He holds an MA in Law and Diplomacy from The Fletcher School of Law and Diplomacy (Tufts University) and BA in Political Science from Freie Universität Berlin.

Peter Lovelock

Peter Lovelock is Director of the Technology Research Project Corporate (TRPC), an IT and telecommunications-based think-tank with offices in Singapore, Hong Kong and China. He brings more than 25 years' experience in telecoms, technology and media to these undertakings, including regulatory assessments, implementation and execution projects, and due diligence and market entry strategic guidance projects throughout Asia. Dr. Lovelock is a strategic adviser to the Yellow Pages group, the ADB, and ICANN, as well as a senior

adviser to Microsoft, and sits on the board of the International Institute of Communications (IIC). TRPC provides Executive Director and Secretariat support to the Asia Cloud Computing Association (ACCA), among others.

Ryan Johnson

Ryan Johnson leads Access Partnership's cybersecurity public policy practice. He consults on international issues for a range of clients on information and communications technology policy. He has worked on internet governance issues for some years, primarily in developing countries in Africa, Latin America and South Asia. Before joining Access Partnership, he worked for Neo Globe Consulting, where he managed market research, policy advocacy, and new market entry activities, and focused on cybersecurity, data protection and cryptography. He has advised various Latin American governments on their digital agendas, national cybersecurity strategies and electronic-crime laws.

Sean Kanuck

Sean Kanuck is an attorney and strategic consultant who advises governments, financial institutions, law firms, and entrepreneurs. He is also Chair of the Research Advisory Group of the Global Commission on the Stability of Cyberspace. Sean served as the first National Intelligence Officer for Cyber Issues from 2011 to 2016. He came to the National Intelligence Council after a decade of experience in the Central Intelligence Agency's Information Operations Center, including both analytic and field assignments. In his Senior Analytic Service role, he was a contributing author for the 2009 White House Cyberspace Policy Review, an Intelligence Fellow with the Directorates for Cybersecurity and Combating Terrorism at the National Security Council, and a member of the United States delegation to the United Nations Group of Governmental Experts on international information security. Prior to government service, Sean practiced law with Skadden Arps in New York, where he specialised in mergers and acquisitions, corporate finance, and banking matters.

Seha Yatim

Seha works with the Access Partnership team in Asia to help technology clients navigate the regulatory and policy environment in the region. She develops policy briefs and reports on various technology topics including FinTech, mobile, payments, big data and artificial intelligence. Prior to joining Access Partnership, Seha worked for the world's largest package delivery company on trade issues, as well as the Singapore government on foreign manpower policies and labour trafficking issues. Seha holds a Master of Science in International Relations from the S. Rajaratnam School of International Studies, and a Bachelor of Business Management from the Singapore Management University.

Urvashi Aneja

Urvashi Aneja is Research Fellow at the Observer Research Foundation, where she writes on the governance and sociology of emerging technologies, and India's development partnerships across the global south. She is also Associate Professor at the Jindal School of International Affairs and Founding Director of Tandem Research.

Vidisha Mishra

Vidisha Mishra is a Junior Fellow at the Observer Research Foundation, New Delhi and a Fellow at the German Development Institute's Managing Global Governance Academy 2017, Bonn, Germany. Vidisha is also a part of the UN Working Group on Youth and Gender Equality for the Commission on the status of Women (CSW), a member of the Women 20 (W20) Network 2017 and the Think 20 (T20) Digital Economy Task Force 2017. She read politics, international studies, and gender in development for her Undergraduate and Graduate degrees from the University of Warwick and the London School of Economics, respectively.

CyFy 2016 saw the participation of nearly 130 experts from 44 countries along with 10 governmental delegations. Last year, the conference hosted dialogues on sentient technologies, cyber norms, affordable and universal digital access, and regional governance architectures for managing the digital economy. This year, the Digital Debates captures some of these conversations and more, exploring the complex and evolving relationship between cyberspace and global politics. Cyber policy practitioners from around the world discuss issues including norm-building for information insecurity; frameworks for cyber governance; regulation of digital economy and the promise and perils of emerging technologies. Digital Debates is an integral part of CyFy: The India Conference on Technology, Security and Society, the annual internet policy conference organised by the Observer Research Foundation. CyFy 2017 was held from October 3-4 in New Delhi, India.