41
Cyberpolitics and IPE
Towards a research agenda in the Global South

Maximiliano Vila Seoane and Marcelo Saguier

Introduction

Cyberpolitics is a field where the political, economic and ecological dynamics that shape contemporary international relations are being played out in relation to technological transformations. We are in a moment of transition towards data capitalism[1] that is characterized by the accumulation of capital by few large Internet companies and platforms (Srnicek 2016), based on the extraction, safeguarding, analysis and (ab)use of data for different purposes (Mayer-Schönberger and Cukier 2013). We call *digitalization* the ongoing process of turning every type of interaction into data. Digitalization is a fundamental vector of data capitalism insofar as the organization of production, decisions and identities are increasingly linked to the generation, availability and interaction with large volumes of data (popularly known as big data).

Digitalization has profound implications in terms of new forms of power and asymmetries among the many old and new actors of inter- and transnational politics. In effect, these new technological capabilities are concentrated in few leading Internet companies located in the US and China (McKinsey & Company 2017) and, to a lesser extent, in Canada, Israel, Russia and some European countries. This unequal distribution poses enormous challenges for the development prospects of countries and societies from the Global South, increasing the historical patterns of dependency between technologically advanced countries and the rest. Taking into account that China is one of the main leaders in digitalization, there are also new emerging center-periphery configurations in the Global South marked by striking technological asymmetries. Moreover, the accumulation of data by a few companies severely limits citizens' decisions over their data, facilitating new forms of surveillance and control for commercial and geopolitical purposes, as well as the violation of human rights such as the right to privacy.

Due to these and other problematic aspects of digitalization, it is essential to understand the relationship between politics and the changes produced by the new information and communication technologies. "Internet politics" (Chadwick and Howard 2009) and "cyberpolitics" are terms usually used in the social sciences to refer to the nexus between politics and technological changes. We adopt the prefix "cyber" in line with scholarly convention in the field of International Relations studies (IR). According to Choucri (2012: 4), cyberpolitics "refers to the conjunction of two processes or realities — those pertaining to human interactions (politics)

surrounding the determination of who gets what, when, and how, and those enabled by the uses of a virtual space (cyber) as a new arena of contention with its own modalities and realities." Departing from this broad definition, we focus on the emerging dynamics of cooperation and competition between the key public and private actors that are currently shaping an emerging global political economy of data.

Cyberpolitics is becoming increasingly an area of interest in IR/International Political Economy (IPE) scholarship, mostly in research centers of technologically advanced countries of the Western Anglo-Saxon sphere. The mainstream research agenda on cyberpolitics is largely concerned with cyberwar issues and increasingly also with the study of the political and social significance of data (Madsen et al. 2016; Mahrenbach et al. 2018). To a lesser extent, the intersections between cyberpolitics and development studies is also becoming a site of research interest (Mahrenbach et al. 2018; Schia 2018; Taylor and Schroeder 2015).

In contrast, there is scarce research of cyberpolitics coming from technologically dependent countries and societies in the Global South. Some notable exceptions in Latin America examined novel initiatives that took place in the region, such as the Civil Rights Framework for the Internet in established in Brazil in 2014 and the cooperation agenda in cyberdefense and cybersecurity policies adopted by the Union of South American Nations (UNASUR) in 2012 (Abdenur and da Silva Gama 2015). These landmark initiatives captured the initial drive for research agenda on cyberpolitics for some time. Yet, this incipient literature tends to be largely descriptive, oriented to a policy informed readership, and lacking the conceptual and analytical depth that is needed to fully explore, understand and manage the complex political, economic and developmental implications of the digitalization processes worldwide and in the Global South particularly.

In this chapter we set out to interrogate *what role and implications have the digitalization process in the making of a new global political economy centered on data.*

To address this question in the first section we introduce a theoretical discussion to conceptualize digitalization as the political terrain of cyberpolitics. We draw from concepts of the neo-Gramscian perspectives of International Political Economy and of the field of Science and Technology Studies. In the second section we explore the implications of digitalization in four areas where cyberpolitics is being played out: cybersecurity; governance of digital trade and global finance; human rights and citizenship on the Internet; and the environment–sustainable development nexus. These areas are representative of the main arenas where dynamics of conflict and cooperation between key cyberpolitics actors are laying ground for the construction of digital world orders but are not the only ones. Finally, we conclude with a reflection about the importance of advancing research on cyberpolitics in countries and societies of the Global South.

The main claim of this chapter is that the digitalization process constitutes a set of practices in which relations of production and governance frameworks are being disputed as part of digital word (dis)orders historically specific to data capitalism in the making.

Box 41.1 Main concepts

Digitalization: The ongoing process of turning every type of interaction into data, a fundamental vector of data capitalism insofar as the organization of production, decisions and identities are increasingly linked to the generation, availability and interaction with large volumes of data (popularly known as big data).

Cyberpolitics: According to Choucri (2012: 4), cyberpolitics "refers to the conjunction of two processes or realities – those pertaining to human interactions (politics) surrounding the determination of who gets what, when, and how, and those enabled by the uses of a virtual space (cyber) as a new arena of contention with its own modalities and realities." For International Relations it is important to limit the analysis to actors and processes of cooperation and dispute at the inter- and transnational level.

Socio-technical relations of production: covers the totality of socio-technical relations that engender particular socio-technical forces.

Forms of governance: refers to historically contingent state/society/technology complexes.

Digital World (dis)order: the particular configurations of forces which successively define the problematic of how to organize cyberspace.

Hegemony: a form of dominance where elements of consensus prevail, but that does not exclude elements of coercion.

Socio-technical relations of production, forms of governance and digital world (dis)orders

In this section, we present a theoretical discussion to conceptualize the role of the digitalization; the terrain of cyberpolitics shaped by the dynamics of conflict and cooperation among actors structuring a new global political economy centered on data. To do so we revisit core concepts of the neo-Gramscian perspective of International Political Economy (IPE) in terms of their value and limitations for understanding the digitalization process. Furthermore, in the spirit of establishing bridges between both research traditions we bring in insights from the field of Science and Technology Studies (STS) in the effort to overcome shortcomings of such IPE concepts.

Since the seminal work of Robert W. Cox in the early 1980s the perspective of neo-Gramscian critique of IPE has contributed to understanding the unfolding configurations and forces of state–society relations as historically specific configurations associated with the transformations of global capitalism (Bieler and Morton 2004; Cox 1981, 1987; Cox and Sinclair 1996; Gill 2008). The concepts of *social relations of production*, *forms of state* and *world orders* are core categories of this perspective, which explain the structural relations that emerge as the outcome of dialectical relations between social forces at any given time in history.

For example, a possible relation is that antagonisms between different social forces, caused by changes of the social relations of production, can lead to the establishment of hegemony by one class over the rest. Thus, the hegemonic class becomes capable of modifying the forms of state, and if it reaches enough international projection, it can also alter the world order (Cox 1981: 138) which, in turn, conditions the actions of other states. Each conceptual category can be understood heuristically by analyzing the dialectical relationship between ideas, institutions and material capabilities (including technological ones).

The concept of hegemony is central to the definition of *world order* in this IPE perspective. Hegemony here differs from formulations of the Realists school in IR where it is associated with a quality of military supremacy of one state over others. Instead, a neo-Gramscian definition sees

hegemony as a form of domination by a *social force* over others, exercised by the consent of subordinate classes. Their acquiescence to a ruling elite takes place when ideas and values presented by a dominant ruling class are accepted as necessary and universal (when they are naturalized as "common sense"). Through consensus and coercion, dominant ideas, supported by material capabilities and by institutions, act as conditions of legitimacy on which social order is produced and reproduced (Cox 1981; Howson and Smith 2008; Robinson 2005).

Furthermore, as a relational concept, hegemony is always understood in contradiction with counter-hegemonic forces. These contest the legitimacy of a social order is maintained based on unequal relations of domination. Resistances can potentially modify the correlations of power between social forces, resulting in changes of the hegemonic order (Cox 1981: 144). IPE readings of global political economy processes apply the notions of hegemony and counter-hegemonic resistance beyond state-centered analyses. States, international organizations, transnational companies (TNCs) and global social movements are seen as forces that structure and shape the dynamics of neoliberal globalization as a historically specific configuration of world order (Gill 2008).

These IPE concepts provide a starting point to understanding the transformations that digitalization generates in the global political economy of data capitalism. Particularly, the kinds of shifting power relations associated with the prevalence that TNCs (particularly but not only in leading technology sectors) are gaining ideational, material and institutional capacities to appear as legitimate forms of private authority in global governance processes (Fuchs 2013; Hall and Biersteker 2002; Newell and Levy 2002). Nevertheless, these IPE concepts fall short to fully tackle the implications that technology is having in all spheres of human and non-human activity which has direct bearing on the dynamics of conflicts and cooperation that is the focus of cyberpolitics.

Concepts are always the product of a particular historical moment. The neo-Gramscian perspective has evolved in relation to analyses of changes in the world economy associated, first, with imperialism, the post-war international system and, later, with neoliberal globalization and its resistances. The extent to which data technology is imbricated in human and non-human processes at a global scale has no comparison with anything ever experienced, and thus requires new lenses to visualize its unfolding configurations and tensions. In other words, critical IPE concepts need to accommodate conceptually and analytically the mutations of global capitalism towards data-centered processes that are redefining socio-political, ecological and identity relations worldwide.

The understanding of "technology" is critical here. Neo-Gramscian IPE conceives technology as an objective factor influenced by and, at the same time, influencing social forces (Cox 1987: 21). Actors with the greatest "social power" determine the direction of technological change. To illustrate this point, let us think of nuclear technology in war, or the innovative technology applied in industrial processes as examples where the development, access and control of key technologies represent advantages vis a vis countries and economic sectors in terms of capacity to control the use and consequences of such technologies. This view of technology, as an instrument of power, is limited to understand some of the issues raised by digitalization. IPE considers technology as something external and separate from the social; a separation that is being challenged by the growing centrality that data processes have in all spheres of human activity, as much of the literature of Science and Technology Studies (STS) points out.

STS perspectives problematize a simplistic separation between the spheres of the "social" and the "technical." Moving away from instrumental understandings of technology, STS look instead at ontologies that better address the kinds of co-construction relations that take place between human actors and other non-human organisms with technological artifacts (Acuto and

Curtis 2014; McCarthy 2011). One implication of this view of technology is that the belief that the social group with more "power" always determines the direction of technological change is put under question (Bijker et al. 2012; Feenberg 1999; Latour 2005). This is because technology today allows types of agency which cannot be reduced to human decisions alone or else to linear processes; artificial intelligence being the extreme and paradigmatic example of this.

Based on these insights, in what follows we reformulate the IPE concepts that were presented earlier to accommodate a non-instrumental view of technology. We hope this effort enables us to grapple with the question of what role and implications the digitalization process has in the making of a new global political economy centered on data.

First, we refer to *socio-technical relations of production* to examine the networks between humans and other artifacts propitiated by digitalization in contemporary relations of production. Namely, we move beyond a focus on analyses of human actors as separate from technological process. This allows us to study the actions of various devices in our contemporary lives, which seem to act independently or locally, but which are really part of vast global networks of material and human elements. Such networks of human-artifacts are maintained by different practices, can act at a distance and transfer policy decisions through technological designs (Nahuis and van Lente 2008).

Cyberspace is an example of such networks (Deibert et al. 2013; Mueller et al. 2007). Cyberspace includes more than Internet. It also covers all the physical infrastructures of information and telecommunications, codes and protocols for "dialogue" between machines, regulations and norms. In this sense, cyberspace becomes a polycentric and transnational network structure. It raises various questions for the study of cyberpolitics in IR/IPE, such as what power actually means when states are being diminished in their capacities to implement unilateral decisions for the whole network (Choucri 2012) or when technology users can shape the functional boundaries of technology and its originally intended applications. It is also true that cyberspace is entirely built by humans (Betz and Stevens 2011), therefore, its structure is in continuous evolution, as well as the transnational threats it enables and the regulatory frameworks to govern it, which have a marked weakness to keep up to date.

Second, the concept of *forms of state* as originally formulated understands the state bureaucratic apparatus as occupied at a certain historical moment by particular social forces, which can establish multiple configurations of relationships with different social actors, such as companies, the church, media, etc. Besides, these social forces may extend their influence beyond the occupied state in question on a global scale (Bieler and Morton 2004: 87; Cox 1981: 141; Gill 2008). Although this conceptualization is superior to the idea of the state as a unitary structure, it is not enough to understand the growing influence in inter- and transnational politics of different types of actors and non-state networks that multiplied with globalization, such TNCs, networks of activists or terrorists, etc. The specificity of these networks is that they also build horizontal relationships, without necessarily having to control the state in order extend their influence on a global scale (Cox and Schechter 2002; Robinson 2005). This is evident on the Internet, where a wide range of "old" actors coexists with new ones, such as the creation of cyber armies by terrorist organizations or the emergence of transnational technology companies that in a short time accumulated an impressive power and influence worldwide.

Likewise, a standard definition of global governance focuses on the set of rules, norms and practices that include both the state as well as private and social actors as relevant stakeholders in global agenda issues. Such a mainstream view of global governance stresses the plurality of actors in processes of deliberation, decision-making and policy implementation and practices. Cox refers to "nebuleuse" to the constellation of actors in transnational networks that exercise governance functions and authority in an age of global capitalism (Cox and Schechter 2002).

However, global governance and nebuleuse both retain a vision of the "political" that has no technological dimension in its conception of agency-structure and power. Alternatively, we propose that governance is also carried out through technologies, such as algorithms (Ziewitz 2015). Therefore, we refer to *forms of governance* as historically contingent state/society/technology complexes which captures such diverse types of configurations.

Finally, taking into account that digitalization is the main driver of data capitalism, it is more precise to refer to *digital world orders* instead of world orders. We are interested in the dynamics of conflict and cooperation that take place in cyberspace. We question the idea of an order in cyberspace, suggesting that "disordered" conditions are likely without this meaning a situation of conflict ridden global processes. In this sense, we propose that the notion of "order" underpinning neo-Gramscian perspectives of IPE needs to be revisited, since it suggests stable and homogenous properties that are too rigid to make sense of more fluid, decentered, contested global processes of co-construction relations between human actors and other non-human organisms with technological artifacts.

In this discussion we have tried to show that the changes that digitalization produces in an emerging global political economy of data are not easily captured by instrumental views of technology and its correlates in other core concepts of critical IPE. What is needed is conceptual lenses that provide insights into the difficult issues and questions raised by data technologies. We are at a historical time when new forms of state-society-technology complexes are being established. Conceptualizing these transformations are inevitably a challenging task, particularly in the field of international relations studies where technology has received little attention (Mayer et al. 2014).

Cyberpolitics in the contours of digital world (dis)orders

Drawing on the theoretical discussion introduced in the previous section, here we explore the implications of digitalization in the global political economy of data in relation to cybersecurity; governance of digital trade and global finance; human rights and citizenship on the Internet; and the environment–sustainable development nexus. These areas are not comprehensive of all domains where data technologies are generating policy and research debates. Nor are the issues and debates presented in each case all that can be said about them. Nevertheless, these areas are strategic arenas where cyberpolitics is drawing new boundaries in defining agendas, actors' alliances and governance arrangements/practices. In these areas, the pathways for future digital world (dis)orders are being disputed.

Cybersecurity

Digitalization has changed significantly the agendas and practices of international security. This changes the global political economy as high-tech companies gain unprecedented weight in security and defense policies. Cybersecurity is the general term most used in relation to the defense against potential threats and/or attacks on the Internet and the protection of computer systems. However, its meaning has come to be associated with strategic military perspectives as was incorporated into a securitization discourse (Dunn Cavelty 2007), displacing the civilian interpretation of the term.

The US military was pioneer in the adaptation to the opportunities that digitalization opened for defense industry and military applications. This was determinant in the securitization of the cybersecurity agenda. In 2009 the US created its Cyber Command dependent on the National Security Agency (NSA) to carry out defensive and attack operations. Then, in 2011 the Pentagon classified cyberspace as a new field of war, along with traditional ones (air, space, sea and land).

The North Atlantic Treaty Organization (NATO) followed in 2016. Therefore, and referring to the theoretical discussion of the previous section, the focus of the mainstream literature on cybersecurity is on the analysis of military and intelligence state agencies, high-tech information companies and other related organizations. These are key actors, or socio-technical forces, driving of cybersecurity processes.

Furthermore, the debates in the cybersecurity literature reflect a "problem solving" approach (Cox 1981) to the potential risks posed by new technologies. The primary concern of scholarly production is to contribute to US capacities to maintain technological superiority and hence support its standing as a global power, which includes neutralizing risks and threats. Issues of great importance are the prospects of attack and deterrence techniques. The prospects of a cyberwar taking place is subject of intense debate (Junio 2013; Lynn III 2010; Rid 2012).

Those convinced of cyber-weapons risks often repeat well-known Realist perspective analyses, accusing countries such as China or Russia of being threats to the world order. Such is the case of Adam Segal (2013), who asserts that China, in order to reach the peak in technological development of its industries, supports systematic cyber-espionage campaigns against US companies and state agencies to steal their intellectual property and other valuable strategic data. In the same vein, Russia is credited with sophisticated "hybrid warfare" attack, which often involves a mixture of cyber-attacks, disinformation campaigns and the use of camouflaged soldiers, as in the cases of Estonia, Georgia, Ukraine and the United States in 2016.

From the perspective of international security, the malware known as StuxNet (Kello 2018) became a milestone in the study of cybersecurity, because it exemplifies the danger of cyber-weapons. It was allegedly created by the intelligence services of the US and Israel and was used in 2010 to sabotage the computer systems of the Natanz nuclear power plant in Iran. The original feature of StuxNet is that it was designed to attack the software that controls industrial processes, and specifically nuclear centrifuges, without resorting to a conventional military attack. In addition to the malware's source code causing considerable physical damage, it also infected other organizations using systems similar to those of the Iranian nuclear power plant. This generated consternation in the community dedicated to cybersecurity because of the risk of causing major damage beyond its initial military objectives.

The risks of cyber-attacks are particularly high in "critical infrastructures." This imprecise concept covers all types of industry or sectors that are critical for the normal functioning of societies, be it civil or military (e.g., banks, social security databases, electric power plants, transportation, etc.) (Deibert et al. 2013). These are no longer mere prospective scenarios. Several incidents demonstrated the damage that cyberattacks[2] can cause in contemporary societies in the process of digitalization. The recent global attack of WannaCry ransomware caused considerable physical damage by paralyzing the systems of companies, government departments, hospitals and individuals around the world. This malware was supposedly created by North Korean hackers based on leaks of cyber-weapons developed by the NSA.

Like all hegemony, order on the Internet is also based on a dimension of consensus-based cooperation. In effect, the US is the driver of the multistakeholder model for Internet governance,[3] which is believed to be a more democratic model than others. Decision processes includes states, firms, civil society organizations, international organizations and technical communities, among others. However, it is no secret that the main Internet governance companies and organizations are generally located in the USA. Therefore, the ideas and interests of these organizations have a superior influence to those of other countries in the development of the Internet and in the processes of digitalization. Hence, the promise of the multistakeholder model, despite its democratic intention, does not alter significantly the power dynamics that privileges the role of states and TNCs particularly those of the US (Carr 2014).

The most emblematic example of this trend is the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit organization based in Los Angeles, charged until 2016 with administering Internet domain names directly on behalf of the US Department of Commerce. For years, this was the cause of a dispute with initiatives from other countries that sought to transfer this responsibility to the United Nations Organization, in order to avoid the prevalence of US preferences over those of other countries, a tension that persists despite recent changes at ICANN (Jackson 2018).

Although the US and its coalition of socio-technical forces retain the leadership in the construction of a hegemony in data capitalism, it is not exempt from counter-hegemonic challenges (Ebert and Maurer 2013). One example of this is the criticisms about the abuse of the surveillance and control facilitated by data technologies following Edward Snowden's revelations. This former NSA agent exposed mass cyber-surveillance programs of the US and its allies in cooperation with transnational technology companies, revealing deep contradictions with the discourse of a free and democratic Internet that emanates from Western countries. The public outcry caused by these revelations did not produce changes in surveillance practices. Instead, the leaks paved the way for public policies that legalized such practices (Pohle and Van Audenhove 2017).

In this scenario, China indirectly accuses the US of having a "cyber hegemony" on the Internet, for not respecting the "cyber sovereignty" of other states. Based on this reading, it is not surprising that China uses its growing economic and technological capabilities to compete with the US on a par in terms of cybersecurity, electronic surveillance, and more recently, artificial intelligence and 5G technologies.

Another example of this counter-hegemonic competition is the establishment of rules to govern conflicts in cyberspace (Finnemore and Hollis 2016). The proposals of the Shanghai Cooperation Organization to limit the use of cybercrimes go in that direction. Yet, these proposals have not prospered due to US opposition on the grounds that such rules would limit freedom of expression and its ability to perform cyber-attacks (Maurer 2011). In response to these initiatives, NATO's Cooperative Cyber Defense Centre of Excellence developed two versions of the Tallinn Manual, written to adapt and internationalize its interpretation of international law for conflicts in cyberspace.

Governance of digital trade and global finance

Digitalization changes relations of production by modifying global trade and finance leading to a transition to digital economies. The governance of these key areas of the global political economy are critical arenas between competing actors.

Global data value chains have different types of actors, though the most influential ones are the companies based in the US (Amazon, Apple, Facebook, Gmail and Microsoft) and in China (Alibaba, Baidu and Tencent). These companies have a privileged position in the new configurations of a global political economy centered on data. They have structural power, which is derived from the increasing dependence that conventional international trade of goods and services has from "digital trade."

"Digital trade" refers to the set of transactions carried out through web portals and new forms of communication. Data transactions differ from the exchange of products or services, since there is no consent or payment for their cross-border flow, and yet they remain essential and of enormous value for data capitalism. The increase in cross-border data flows and automation (e.g., algorithms and robotics) accelerates international trade of goods and services (López-González and Jouanjean 2017).

Moreover, digitalization has enabled the expansion of global value chains that rest on deterritorialized forms of work that would be unthinkable without innovations in the data technology. New modalities of work are facilitated by the provision of services in the "cloud" that allows access to documents, emails and all types of data from various devices and in any moment that can be accessed via the Internet. These facilitate remote distance coordination between production units located in different parts of the world as well as the management to international trade logistics.

The pivotal role that TNCs in data technology sectors have in the global value chains has been characterized as the consolidation as the new monopolies of the twenty-first century. A form of transnational "privatized public infrastructure" (Plantin et al. 2016) is leading the development of new forms of production in the digital era and is partly responsible for their negative effects in terms of human rights and developmental. This has led to a debate about the need to have effective global regulatory instruments to avoid market concentration, tax evasion (Aaronson 2015) and complicity in human rights violations around the world.

Voices contrary to regulation claim that monopolistic concentration in digital sectors is necessary to offer global goods that would otherwise be difficult to produce. This position informs the lobbying practices of US companies in the US and in the European Union aimed at ensuring that the rules of the digital economy and digital trade are in tune with their interests. Likewise, the anti-regulation positions seek to prevent other states from implementing restrictions on the free flow of data across borders (e.g., data localization requirements in the countries where they operate), because they consider such policies as a restriction to freedom of access to the Internet.

In contrast, positions favorable to regulatory measures hold that they are essential state instruments to ensure that digitalization can be conducive to development-oriented policies, as well as consistent with national sovereignty rights. In short, what is at stake is the dispute over different forms of governance of digital trade, an area of the global economy that places additional strains on the state digital development strategies.

Equally, the actors and governance challenges of the global financial system are being changed by the emergence of FinTech. Cryptocurrencies, such as Bitcoin, are one of the most recent cases of new technological innovations in the sector, but not the only ones. These digital currencies are based on blockchain technology (De Filippi and Wright 2018), which allows to protect and exchange value in encrypted, decentralized and transnational networks.

Different actors are part of these new cryptocurrencies networks, such as technologists, investors, fans, citizens, but also money launderers and other criminals from around the world, promoting a new way of realizing and speculating with financial transactions. In its most radical expression, these new digital forms of exchanging value are inspiring the creation of "nations without borders", such as BitNation, as well as the implementation of smart contracts, which exemplifies the looming forms of algorithmic-decentralized governance.

According to Campbell-Verduyn and Goguen (2017) these processes of decentralization have a direct impact on the dominant intermediaries of global finance (e.g., companies such as JP Morgan, central and private banks). Their control capacities are being loosened by such new structures of money and value flows, causing new dilemmas for the stability of the global financial system and for efforts to curb money laundering. States and companies have responded by seeking to appropriate blockchain technology in an attempt to reverse their loss of control in global finances. In short, blockchain exemplifies the emergence of a new form of transnational governance, which has the potential to alter significantly the digital world order.

Human rights and citizenship on the Internet

The digitalization of contemporary societies is causing multiple impacts on preexisting ideas and practices on human rights and citizenship. Infringement to citizen's rights to privacy is one of the main problems associated with digitalization. Indeed, cybercrime (Holt and Bossler 2014) and the excessive use of devices capable of producing thorough electronic traces of our interactions with other humans and machines, allows companies to generate precise profiles on consumption, political preferences, spatial displacements, etc. (Ball et al. 2012) of its users, limiting citizens' online privacy. State security and intelligence agencies believe that the collection of these large databases – in collaboration with the private sector – is essential to avoid contemporary threats, such as terrorism or organized crime. These practices are justified on the grounds that citizens need not fear from the analysis of data or metadata[4] if they have nothing to hide. However, following Snowden's revelations about the indiscriminate and disproportionate use of espionage capabilities by the US in collaboration with other states, the arguments used to justify massive electronic surveillance are seriously questionable (Bernal 2016).

This is not a new issue in international relations. Already in the 1990s Der Derian (1990) identified the strategic role of surveillance to discipline and normalize behaviors of others. Yet, in data capitalism the variety, speed and volume of data (big data) that states and companies can obtain from entire populations certainly constitutes a new phenomenon. That is to say, the current coercive practices of cyber-espionage and cyber-surveillance of major powers have confirmed, and even exceeded, the wildest speculations and concerns of previous decades.

The regulation of increasingly powerful Internet TNCs in terms of their impacts on economic, political and social rights consists of a great challenge in an age of data capitalism. Companies have the ability to make decisions at a distance through algorithms that are often not transparent (DeNardis and Hackl 2015) generating impacts on the working conditions of their users. Many of these companies coordinate the offer of their digital products and services globally, without necessarily operating physically in offshore jurisdictions, generating considerable disruptions in sectors that until recently were immune to digitalization.

The most striking example is Uber's incursion in the transport sector, whose rapid global expansion was accompanied by a disdain to comply with local regulations in the countries where it operates, causing conflicts with national labor regulations and trade unions that see workers' rights threatened and with states that have a limited capacity to regulate the company. Another recent landmark is that of the scandal of the firm Cambridge Analytica, which revealed how Facebook's lax data protection policies at the time paved the way for the collection and manipulation of its users' personal data to distribute political propaganda in different elections (such as in those in the USA, Argentina, Kenya and the United Kingdom).

The growing centrality of TNCs in offering all types of products and services is having significant impacts in terms of citizenship. Identities are increasingly mediated by algorithms and data that circulate in private and transnational Internet platforms with the effect of influencing the interactions that users may have (Jackson 2018). For instance, social media algorithms show their users content that corroborates their cultural, economic, political, etc. preferences, in order to retain them on the platform. This generates the so-called echo chambers effect, since users mostly access content that confirms their beliefs, limiting exposure to other positions, and possibly impoverishing the necessary debate in democratic contexts (Helbing et al. 2017).

In turn, this phenomenon can facilitate the distribution of "fake news", which might shape the construction of political identities in ways in need of further research (Lazer et al. 2018). Likewise, another characteristic of these new mediations is that a large section of users are in jurisdictions different from those of origin of these companies, putting under pressure the

traditional idea of citizenship based on our belonging to a nation-state in geographical terms. For these reasons, Isin and Ruppert (2015) invite us to think about the digital citizen as someone who claims rights, both of existing and new ones, and can be useful to investigate the novel and changing contours of digital and transnational citizenship in an era of data capitalism.

The impacts of digitalization on human rights and citizenship are changing relations of production and forms of governance. This has led to human rights organizations such as Amnesty International and Human Rights Watch to incorporate these issues into their agendas. Likewise, new transnational organizations specialized in digital rights were created, such as Privacy International, which contest what they consider to be unethical production practices of several Internet companies. It is also true that some of the Internet TNC are adopting—albeit slowly—cryptography in their services (e.g., WhatsApp), which make it difficult for third parties to access the content of messages, but which also limit state sovereignty in regulating the content through such channels (Buchanan 2016).

Finally, several states are legislating over the Internet and the use of data. On the one hand, initiatives to reform data protection laws stand out, such as the General Regulation of Data Protection of the European Union. These grant basic rights to users about their data and assigns responsibilities to organizations that collect and process data, although without reducing all the asymmetries between these two types of actors. On the other hand, other states are implementing policies of censorship, control and "nationalization" of the Internet, which challenge the multistakeholder model of governance (Deibert 2015).

Environment–sustainable development nexus

Big data techniques to collect real time information about the human–environment nexus are revolutionizing the science, politics and economics of adaptation and mitigation to climate change (Ford et al. 2016) and sustainable development. While digitalization presents opportunities it also poses risks for environmental and sustainable development policies related to the issue of ownership and potential uses of biological and environmental data.

The so-called "Fourth Industrial Revolution" is presented as an opportunity to tackle many of the world's current environmental problems (climate change, pollution, depletion of fishing stocks, toxins in rivers and soils, waste on land and oceans, loss of biodiversity and deforestation, etc.). New technologies are enabling societal shifts by having an effect on economics, values, identities and possibilities for future generations. This industrial revolution, unlike previous ones, is underpinned by the established digital economy and is based on rapid advances in artificial intelligence (AI), the Internet of Things, robots, autonomous vehicles, biotechnology, nanotechnology and quantum computing, among others. It is characterized by the combination of these technologies, which are increasing speed, intelligence and efficiency gains (World Economic Forum 2018).

The applications of big data technologies like AI and others enable new possibilities for monitoring environmental changes, such as changes in soil composition, water quality, patterns of species movements, to mention a few examples. Access to big data on the environment is critical for adequate policy and environmental governance responses. In particular, to devise informed mechanisms and processes of impact assessment on socio-ecological systems. This is relevant to understand the scale, intensity and direct/indirect impacts of climate change, resource-based industries (agriculture, mining, aquiculture, fishing, forestry, energy, etc.) and infrastructure projects (hydroelectrical, transport, irrigation infrastructures, etc.) (Gerlak et al. 2019).

Moreover, other technologies such as blockchain are also opening new possibilities for different approaches to environmental governance. Blockchain technology is being used in

forest protection (Howson et al., 2019), and as a mechanism for smart contracts to register the ownership of environmental resources or the traceability of products, among others (Chapron 2017). This decentralized technology, where no single user can control the entire information structure, is proving a viable option to managing the problems associated with lack of trust between stakeholders connected to different aspects of environmental governance.

Digitalization of environmental data also presents some difficult issues such as the unequal conditions in terms of influence, advantages and power related to access to this information. Private ownership of environmental data favors economic concentration in leading actors in natural resource sectors. Likewise, in the internet platforms that provide the technologies to generate and manage environmental data by different users. Big data technologies make it possible to estimate more accurately the availability of biological and natural resources. It becomes a strategic commodity, as access to this technology translates into commercial advantages. It can also encourage illicit economic activities such as biopiracy, which consist in the commercial exploitation of animals, plants, microorganisms and other natural resources (Lucchi 2013).

The weight of environmental big data is not only related to the fact that only leading economic sectors can access and control information. It also depends on the generation of artificial barriers that limit the use of data by other states and actors who cannot pay for them (such as public policy decision makers in less resourceful states, researchers and the public in general). Restricted public ownership or access to environmental data undermines efforts to democratize the management, protection, and/or rational and sustainable use of natural and biological resources.

In fact, the booming market of companies providing big data services for the natural resource industries is in direct tension with states' goal of advancing opportunities for public access to information and participation in decisions concerning the environment (as contained in the Agenda 2030 of the Sustainable Development Goals, as the follow up of the 1992 UN Summit on Sustainable Development in Rio). Due to these criticisms, an open data movement has emerged as a counter-hegemonic socio-technical force advocating the notion of data as a public good (Leonelli 2013). Ensuring public access and control over environmental data is essential for the democratization of environmental governance.

Private ownership and control of environmental data contributes to creating conditions for the diffusion of a market-based approach to global environmental governance. Companies that have access to this technology are being presented as key stakeholders in bringing about effective responses to the environmental crisis and as means to realizing the aspirations of sustainable development. This is part of a narrative of eco-efficiency and environmental modernization that currently disputes the meanings and contents of an evolving discourse of "sustainable development." Companies that muster data technologies are seen to be best capable of responsibly managing resources with sustainability criteria. Let us think of the notion of "responsible mining" in relation to technology providing means of managing contamination risks and water usage in mining practices, or the evolving notion of an "intelligent agriculture" as the paradigm of efficient use of soil and water relying on big data and AI. In fact, this technological element can be seen as a more recent development of a longer process of building a narrative of "corporate responsibility" as a discursive strategy to offset regulatory demands stemming from mounting criticisms to business involvement in ecological destruction and human rights violations (Saguier 2012).

These ideas have a pretence to serve as part of a hegemonic consensus on which to structure global governance arrangement for the environment based on a market-based approach that has business actors as driving agents of change. Internet and high-tech companies have a pivotal role here since they command a neuralgic component of the value chains in resource-based

sectors. Reflexions about alternative policy pathways to address the environmental crisis and the challenges of sustainable development challenges, which do not involve the determining role of business, are simply foreclosed or minimized from the global agenda (Saguier and Brent 2017).

The politics of environmental governance involve also state–company coalitions that dispute a share of the enormous market that the climate crisis opened for business investments. Germany and China are prime examples of states that have articulated solid alliances with private and public companies (Beveridge and Kern 2013; Wang et al. 2014) with great influence in shaping the politics of global environmental governance in terms of agenda setting, securing commercial contracts and investing in international legitimacy. Their global leadership in "green production" and renewable energy sectors are also explained by the disengagement of the US from the climate agenda under the Donald Trump government and of Brazil under Jair Bolsonaro.

Conclusions

In this chapter we set out to interrogate what role and implications the digitalization process has in the making of a new global political economy centered on data. To explore this theme, we reviewed the emerging issues, actors and processes in four strategic arenas of cyberpolitics. In these arenas we discussed ways in which digitalization is generating changes in the relations of production, governance and configurations of socio-technical forces that are currently disputing the direction of potentially different pathways towards world orders in cyberspace.

The challenges and dilemmas raised by digitalization are already a priority on the agenda of major powers and other transnational actors but remain marginal in the research communities of Global South countries and societies. In the effort to contribute to a research agenda on these issues we identify a few preliminary conclusions.

In terms of cybersecurity, we find that IR/IPE scholarship is mostly oriented to maintaining the hegemony of countries and Western social forces (led by US companies, security and defense agencies) on the Internet, both in terms of new forms to carry out cyberwar, as in elaborating norms and institutions that defend the neoliberal order of Internet Governance. The boundaries between public and private spheres in the security and defense sectors are increasingly blurred as the leading private high-tech companies have a leading role and influence in this industry and in public sector decisions and capabilities.

With respect to the governance of digital trade and global finance, we identify two opposite patterns. On the one hand, from the side of digital trade, there is a process of concentration in few TNCs from the US and China, which gives them excessive market power. This creates new ways of producing value, but also new governance challenges and questions about what type of data capitalism will prevail on the Internet. On the other hand, in terms of global finance, blockchain technology initiated an opposite process of decentralization, which threatens not only incumbent actors in charge of financial transactions, but also the global financial structure. That is, IPE perspectives on cyberpolitics can shed light on the new patterns of organization and regulation of trade, production and finance in the digital era.

Similarly, changes in the forms of production fostered by digitalization are generating new challenges in terms of human rights and citizenship practices and identities. These are being addressed by different states and civil society organizations in disparate ways. Nascent citizen movements have begun to contest and counteract the growing concentration of data that is (mis)used for security, commercial and political purposes. However, the extent to which such bottom-up forces can open up spaces of democratization and pluralization in the sphere of cyberpolitics is yet to be seen. Nonetheless, it is certain that citizen movements will tend to have

growing influence as the awareness of the implications of new technologies gradually coalesce into new social demands and political agendas in different countries.

Finally, we highlight the challenges that emerge in relation to environmental data being considered a private versus a public good. Similarly, we mentioned the potential of new forms of decentralized environmental governance based on blockchain technology, but also a centralizing trend towards concentrated companies in the high tech and extractive sectors having growing authority and material leverage in environmental governance. This trend is inscribed in the efforts of countries like China and Germany to influence global environmental governance, based on innovations achieved at the national level through digitalization. What is crucial is to understand the shifting configurations of power involved in the construction of an environment–sustainable development nexus where technology places a pivotal role.

Notwithstanding the particular issues raised in these four arenas of cyberpolitics, we also argued that we face conceptual challenges in the effort to make sense of the implications of digitalization. In this respect, we proposed to go beyond instrumental understandings of technology as the only possible readings of the political and economic implications of the use of new data technologies. Although instrumental use will always be relevant to consider, our warning is to avoid assuming uncritically ideas of technological determinism; whereby actors' possession of technology translates necessarily into power.

Instead, we suggest to see social and technological spheres as co-produced. This means that what is relevant is to pay attention to technology designs as immanent of, and imbricated in, social contexts marked by dynamics of conflict and cooperation between socio-technical forces. Namely, seeing social contexts as constitutive of technology and not as mere backgrounds. That is to say, the particular designs of technology (its functional capability) are manifestations of specific relations between such forces and interests. This suggests that new data technologies are also being appropriated and adapted by different actors beyond the intent for which it was originally designed. This complicates power assumptions that rely on a conflated relation between actor's agency and technology control. In this chapter we cited some examples that illustrate trends of cyberpolitics as dimensions of decentered agency.

Notwithstanding the potential openings that cyberpolitics offers for exploring alternative uses of technology, for most other countries today it is not an exaggeration to say that they are under a kind of "digital imperialism." Although Snowden's revelations intensified tensions between the US and the European Union in terms of data protection, it has not led to significant changes. This is a hegemonic order in which that most data-dependent countries accept and rarely question. An order characterized by new forms of digital control, concentrated in a few transnational social actors that have increasing influence over data of varied kinds (personal, biological, environmental, military, etc.), is enabling the fine-grained surveillance of populations in ways that were impractical a few years ago.

Despite these trends, academic interest in cyberpolitics and digitalization is rather scarce in countries and regions that experience such new digital dependencies. We consider this problematic for two reasons. First, strategically, without some exceptions, researchers in the Global South are not thinking about how to deal with these new digital challenges, leaving such countries and societies even more vulnerable on initiatives of extra-regional actors. Second, by neglecting cyberpolitics and digitalization in the Global South, academics are missing the opportunity to expand our understanding of these processes by incorporating the national and/or regional specificities that that could extend IR/IPE research scholarship beyond the usual Western-centric paradigms.

The discussion we proposed in this chapter hopes to make a contribution in this direction. Although the issues and topics addressed are not the only ones where research is needed, we

think that they are at least the indispensable ones to move forward in a collective and interdisciplinary way. At the same time, we must not lose sight of the importance of critical engagements with cyberpolitics research. The greatest challenge of all is to contribute to avoid, or at least manage, the worst elements of digitalization, as well as position alternatives to those preferred by the most powerful actors of data capitalism.

Notes

1 Researchers often use "digital capitalism" in the literature; however, we chose data capitalism, because it makes a clear reference to the central resource that this form of capitalism accumulates: data.
2 When speaking of "cyber-weapons", analysts refer to malware, which is a concept that includes software with malicious purpose that seeks to provoke some kind of damage in other systems or software. There are several types of malware, among them: worms, ransomware, rootkits, trojans and viruses.
3 It should be noted that in this section our observations are limited to the intersection between cybersecurity and Internet governance, and not to all the other connotations that tend to be discussed under the latter term, particularly in the context of the Internet Governance Forum.
4 Metadata refers to data about data, such as the telephone numbers that a specific line was contacted. Although such metadata does not expose the content of the communications, it reveals the network of contacts of the spied line, very valuable intelligence information.

Bibliography

Aaronson, S. 2015. Why trade agreements are not setting information free: the lost history and reinvigorated debate over cross-border data flows, human rights, and national security. *World Trade Review* 14(4): 671–700.

Abdenur, A. and Da Silva Gama, C. 2015 Triggering the norms cascade: Brazil's initiatives for curbing electronic espionage. *Global Governance* 21(3): 455–474.

Acuto, M. and Curtis, S. (eds.) 2014. *Reassembling International Theory: Assemblage Thinking and International Relations*. Basingstoke, UK: Palgrave Macmillan.

Ball, K., Haggerty, K. and Lyon, D. (eds.) 2012. *Routledge Handbook of Surveillance Studies*. Routledge International Handbooks. New York, USA: Routledge.

Bernal, P. 2016. Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy* 1(2): 243–264.

Betz, D. and Stevens, T. 2011. *Cyberspace and the State. Toward a Strategy for Cyber-Power*. London, UK: Routledge.

Beveridge, R. and Kern, K. 2013. The Energiewende in Germany: Background, developments and future challenges. *Renewable Energy Law and Policy Review* 4(1): 3–12.

Bieler, A. and Morton, A. 2004. A critical theory route to hegemony, world order and historical change: neo-Gramscian perspectives in international relations. *Capital & Class* 28(1): 85–113.

Bijker, W., Hughes, T. and Pinch, T. (eds.) 2012. *The Social Construction of Technological Systems*. Anniversary edition. Cambridge, Massachusetts, USA: The MIT Press.

Buchanan, B. 2016. Cryptography and sovereignty. *Survival* 58(5): 95–122.

Campbell-Verduyn, M. and Goguen, M. 2017. The mutual constitution of technology and global governance: Bitcoin, blockchains, and the international anti-money-laundering regime. In: *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*. London, UK: Routledge.

Carr, M. 2014. Power plays in global internet governance. *Millennium: Journal of International Studies* 43(2): 640–659.

Chadwick, A. and Howard, P. 2009. *Routledge Handbook of Internet Politics*. London, UK: Routledge.

Chapron, G. 2017. The environment needs cryptogovernance. *Nature* 545(7655): 403–405.

Choucri, N. 2012. *Cyberpolitics in International Relations*. Cambridge, Massachusetts, USA: The MIT Press.

Cox, R. 1981. Social forces, states and world orders: Beyond International Relations Theory. *Millennium. Journal of International Studies* 10(2): 126–155.

Cox, R. 1987. *Production, Power, and World Order: Social Forces in the Making of History*. New York, USA: Columbia University Press.

Cox, R. and Schechter, M. 2002. *The Political Economy of a Plural World: Critical Reflections on Power, Morals and Civilization*. RIPE series in: Global Political Economy. London, UK: Routledge.
Cox, R. and Sinclair, T. 1996. *Approaches to World Order*. Cambridge, UK: Cambridge University Press.
De Filippi, P. and Wright, A. 2018. *Blockchain and the Law: The Rule of Code*. Cambridge, Massachusetts, USA: Harvard University Press.
Deibert, R. 2015. The geopolitics of cyberspace after Snowden. *Current History* 114(768): 9–15.
Deibert, R., Rohozinski, R. and Crete-Nishihata, M. 2013. Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war. *Security Dialogue* 43(1): 3–24.
DeNardis, L. and Hackl, A. 2015. Internet governance by social media platforms. *Telecommunications Policy* 39(9): 761–770.
Der Derian, J. 1990. The (s)pace of international relations: Simulation, surveillance, and speed. *International Studies Quarterly* 34(3): 295–310.
Dunn Cavelty, M. 2007. Cyber-terror – looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics* 4(1): 19–36.
Ebert, H. and Maurer, T. 2013. Contested cyberspace and rising powers. *Third World Quarterly* 34(6): 1054–1074.
Feenberg, A. 1999. *Questioning Technology*. Abingdon, Oxon, UK: Routledge.
Finnemore, M. and Hollis, D. 2016. Constructing norms for global cybersecurity. *The American Journal of International Law* 110(3): 425–479.
Ford, J., Tilleard, S., Berrand-Ford, L., Araos, M., Biesbroek, R., Lesnikowski, A., MacDonald, G., Hsu, A., Chen, C. and Bizikova, L. 2016. Big data has big potential for applications to climate change adaptation. *Proceedings of the National Academy of Sciences of the United States of America* 113(39): 10729–10732.
Fuchs, D. 2013. Theorizing the power of global companies. In: Mikler, John, ed. *Handbook of Global Companies*. Chichester: Wiley-Blackwell: 77–95.
Gerlak, A., Saguier, M., Mills-Novoa, M., Fearnside, P. and Albrecht, T. 2019. Dams, Chinese investments, and EIAs: A race to the bottom in South America? *Ambio* 49(1): 154–164.
Gill, S. 2008. *Power and Resistance in the New World Order*. 2nd ed. New York, USA: Palgrave Macmillan.
Hall, R. and Biersteker, T. 2002. *The Emergence of Private Authority in Global Governance*. Cambridge, UK: Cambridge University Press.
Helbing, D., Frey, B. and Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., van den Hoven, J., Zicari, R.V. and Zwitter A. 2017. Will democracy survive big data and artificial intelligence? *Scientific American* 25, February.
Holt, T. and Bossler, A. 2014. An assessment of the current state of cybercrime scholarship. *Deviant Behavior* 35(1): 20–40.
Howson, P., Oakes, S., Baynham-Herd, Z. and Swords, J. 2019. Cryptocarbon: The promises and pitfalls of forest protection on a blockchain. *Geoforum* 100: 1–9.
Howson, R. and Smith, K. (eds.) 2008. *Hegemony: Studies in Consensus and Coercion*. Routledge Studies in Social and Political Thought. New York, USA: Routledge.
Isin, E. and Ruppert, E. 2015. *Being Digital Citizens*. London, UK: Rowman & Littlefield.
Jackson, S. 2018. A turning IR landscape in a shifting media ecology: The state of IR literature on New Media. *International Studies Review* 21(3): 518–534.
Junio, T. 2013. How probable is cyber war? Bringing IR theory back in to the cyber conflict debate. *The Journal of Strategic Studies* 36(1): 125–133.
Kello, L. 2018. *The Virtual Weapon and International Order*. New Haven, Connecticut, USA: Yale University Press.
Latour, B. 2005. *Reassembling the Social. An Introduction to Actor-Network Theory*. New York, USA: Oxford University Press.
Lazer, D., Baum, M., Benkler, Y., Berinsky,A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J. and Zittrain J. L. 2018. The science of fake news. *Science* 359(6380): 1094–1096.
Leonelli, S. 2013. Why the current insistence on open access to scientific data? Big data, knowledge production, and the political economy of contemporary biology. *Bulletin of Science, Technology & Society* 33(1–2): 6–11.
López-González, J. and Jouanjean, M. 2017. *Digital Trade: Developing a Framework for Analysis. OECD Trade Policy Paper 205*: OECD.
Lucchi, N. 2013. Understanding genetic information as a commons: From bioprospecting to personalized medicine. *International Journal of the Commons* 7(2): 313–338.

Lynn III, W. 2010. Defending a new domain: The Pentagon's cyberstrategy. *Foreign Affairs* 89(5): 97–108.
Madsen, A., Flyverbom, M., Hilbert, M. and Rupert, E. 2016. Big Data: Issues for an international political sociology of data practices. *International Political Sociology* 10(3): 275–296.
Mahrenbach, L., Mayer, K. and Pfeffer, J. 2018. Policy visions of big data: Views from the Global South. *Third World Quarterly* 39(10): 1861–1882.
Maurer, T. 2011. *Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-security*. Cambridge, Massachusetts: Belfer Center for Science and International Affairs, Harvard Kennedy School.
Mayer, M., Carpes, M. and Knoblich, R. (eds.) 2014. The global politics of science and technology: an introduction. In: *The Global Politics of Science and Technology*. Berlin: Springer-Verlag: 1–35.
Mayer-Schönberger, V. and Cukier, K. 2013. *Big Data. A Revolution That Will Transform How We Live, Work and Think*. New York, USA: Houghton Mifflin Hartcourt Publishing Company.
McCarthy, D. 2011. The meaning of materiality: Reconsidering the materialism of Gramscian IR. *Review of International Studies* 37(3): 1215–1234.
McKinsey & Company 2017. *Artificial Intelligence: The Next Digital Frontier?* Discussion Paper. McKinsey Global Institute. Available at: www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx.
Mueller, M., Mathiason, J. and Klein, H. 2007. The Internet and global governance: Principles and norms for a new regime. *Global Governance* 13(2): 237–254.
Nahuis, R. and Van Lente, H. 2008. Where are the politics? Perspectives on democracy and technology. *Science, Technology & Human Values* 33(5): 559–581.
Newell, P. and Levy, D. 2002. Business strategy and international environmental governance: Towards a neo-Gramscian synthesis. *Global Environmental Politics* 2(4): 84–101.
Plantin, J., Lagoze, C., Edwards, P.and Sandvig. C. 2016. Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society* 20(1): 293–310.
Pohle, J. and Van Audenhove, L. 2017. Post-Snowden Internet policy: Between public outrage, resistance and policy change. *Media and Communication* 5(1):1–6.
Rid, T. 2012. Cyber war will not take place. *The Journal of Strategic Studies* 36(1): 5–32.
Robinson, W. 2005. Gramsci and globalisation: From nation-state to transnational hegemony. *Critical Review of International Social and Political Philosophy* 8(4): 559–574.
Saguier, M. 2012. Peoples' tribunals in Latin America. In: Reed, D., Utting, P. and Mukherjee-Reed, A. (eds) *Business Regulation and Non-State Actors: Whose Standards? Whose Development?* Abingdon, UK: Routledge: 250–265.
Saguier, M. and Brent, Z. 2017. Social and solidarity economy in South American regional governance. *Global Social Policy* 17(3): 259–278.
Schia, N. 2018. The cyber frontier and digital pitfalls in the Global South. *Third World Quarterly* 39(5): 821–837.
Segal, A. 2013. The code not taken: China, the United States, and the future of cyber espionage. *Bulletin of the Atomic Scientists* 69(5): 38–45.
Srnicek, N. 2016. *Platform Capitalism*. Cambridge: Polity Press.
Taylor, L. and Schroeder, R. 2015. Is bigger better? The emergence of big data as a tool for international development policy. *GeoJournal* 80(4): 503–518.
Wang, Z., He, H. and Fan, M. 2014. The ecological civilization debate in China. The role of ecological Marxism and constructive postmodernism—Beyond the predicament of legislation. *Monthly Review* 66(6): 37–59.
World Economic Forum. 2018. Harnessing Artificial Intelligence for the Earth. *Fourth Industrial Revolution for the Earth Series:* REF 030118. Available at: www3.weforum.org/docs/Harnessing_Artificial_Intelligence_for_the_Earth_report_2018.pdf.
Ziewitz, M. 2015. Governing algorithms: Myth, mess, and methods. *Science, Technology & Human Values* 41(1): 1–14.