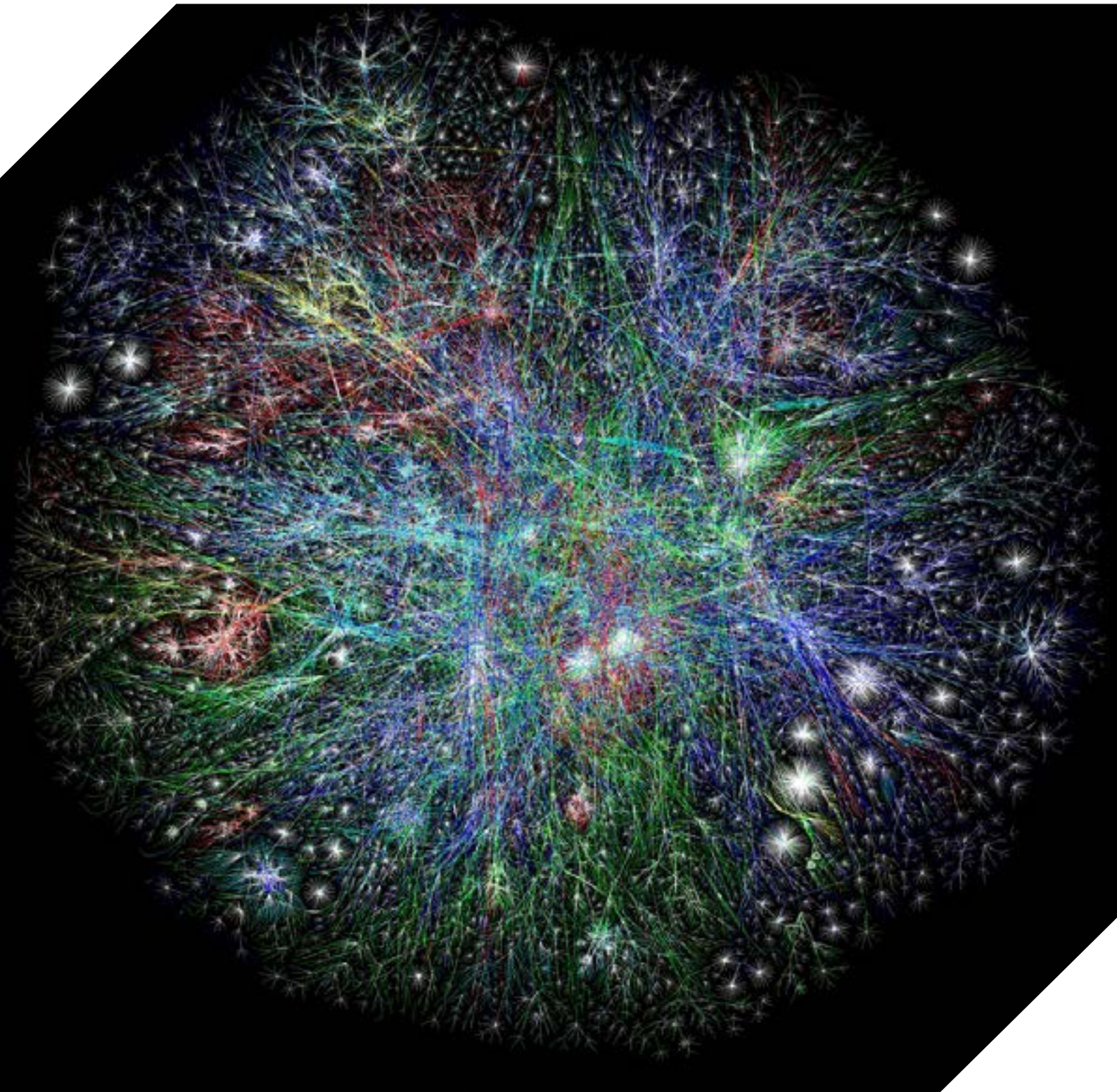
ISPI DOSSIER April 2020

FRAGMENTING THE INTERNET: STATES' POLICIES IN THE DIGITAL ARENA

edited by **Samuele Dominioni, Fabio Rugge**



ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

April 2020

Once upon a time there was a space, the cyberspace, which was a common ground: without boundaries and dominating powers, open to anyone who could connect to it. Less than three decades later, however, the panorama has changed radically. The growing geopolitical importance of cyberspace pulled governments into the digital arena. Their interventions, mostly driven by security imperatives, led to the setting up of boundaries, barriers and other obstacles which are capsizing the very funding principles of the Internet and leading to its "fragmentation". What are the driving forces behind this process? How is the international community responding? And why (and how) do governments create cyber-boundaries?

** Samuele Dominioni is a Research Fellow at the ISPI Centre on Cybersecurity, in partnership with Leonardo.*
** Counselor Fabio Rugge is Head of ISPI's Centre on Cybersecurity, in partnership with Leonardo.*

An Internet That Divides

Fabio Rugge
ISPI

Looking at the ongoing militarization of the Internet, one could rephrase Rousseau's famous incipit to The Social Contract: "Internet was born free and everywhere it is in chains". In fact, the Internet is increasingly militarizing, and cyberspace has become the domain of choice for destabilising campaigns and hostile activities that would be unsustainable in the conventional domain.

Given the absence of a superordinate authority, the Internet has often been portrayed as anarchical in nature. Supporting this idea is the fact that cyberspace offers an unprecedented platform for humankind to interact globally with complete disregard for political borders and power politics. Moreover, the Internet allows public opinion a much greater control of governments' doings, new forms of social protests, and empowers communities outside of the mainstream media. As such, one cannot but sympathize with Barlow's ode to a cyberspace outside of states' control, in his 1996 Declaration of the Independence of Cyberspace: "Governments of the Industrial World, you weary giants of flesh and steel, I

Counselor **Fabio Rugge** is Head of ISPI's Centre on Cybersecurity, in partnership with Leonardo. He is a diplomat currently working as Head of the Office in charge for NATO and Security and Politico-Military Issues, Directorate General for Political Affairs and Security, Ministry of Foreign Affairs and International Cooperation.

come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."

In reality, however, Rousseau's quixotic "State of Nature" is fictional just as much as Barlow's alleged "statelessness" of the Internet. Whoever remembers the movie "War Games" from 1983 will know how, since the very beginning, the cyber domain was understood to be intrinsically insecure and yet increasingly critical in supporting even the most sensible tasks. Before the term "cyberspace" even existed, it was clear that its security was going to be crucial in military operations and that the distinction between what is "cyber" and what is "real" was going to be increasingly difficult to grasp. States had therefore an interest in Internet's security from the outset, and their involvement only grew over time: the more the confidentiality, integrity and availability of data prove essential for national security, the more urgent it becomes for states to enhance their national cyber power, intended as the ability to achieve desired results in and through cyberspace while denying strategic, tactical and operational advantages to the adversaries. Hence the ongoing "militarization" of the Internet, by which we refer both to the struggle of sovereign states to assert their prominence in cyberspace vis-à-vis all non-state actors that populate cyberspace, and to the increasing relevance of military considerations in shaping national approaches to the stability of cyberspace.

This ongoing militarization, regrettably, is proving how much Barlow was wrong, and it is not making cyberspace any safer. In fact, quite the opposite: the more cyber power becomes an essential enabler of sovereignty, the more cyberspace develops as a contested domain where each player's quest for greater security translates, at the systemic level, into a more unpredictable and volatile security environment. Cyberspace is ubiquitous: it is the nervous system that connects and increasingly enables the political, strategic, military, informative, economic, financial, industrial and infrastructural dimensions on a personal, local, national, transnational and international level. This entanglement and the growing complexity of these interdependencies multiply the risk of cross-domain escalations: a cyber-attack on critical civilian infrastructures or military command and control centres, or a major cyber-enabled information warfare campaign, could (in an admittedly unlikely but not impossible scenario) escalate into a concrete threat to strategic nuclear stability.

Efforts to develop globally recognized norms of responsible state behaviour in cyberspace have so far had little success, and optimists about their prospects should probably think twice, as the nature of cyberspace poses significant stumbling blocks to the development of an agreed-upon international framework. This has immediate consequences both on the stability of cyberspace and on the actual privacy and freedoms that Internet users may enjoy. Just like the emergence of international law did not put an end to wars, the development of international law applicable to cyberspace

would certainly not end states' active engagement in cyberspace – but it would certainly contribute to identifying the perimeter of states' legitimate activities in cyberspace. The first obstacle to this advance is probably cultural: although cyberspace is more than 30 years old, we still approach it as a "new" domain. This is somehow understandable, as the digital revolution is unfolding at a pace that we all struggle to keep up with. Developing doctrines, policies, procedures, human skills and norms of behaviour takes time, and major developments in international relations have historically been associated with painful wars, for which (luckily!) we still have no cyber equivalent, yet. Moreover, the cyber domain is global, instantaneous, asymmetrical: attackers may strike at the speed of light from every network's entry-point, taking advantage of virtually any vulnerability in hardware, software and operating procedures. Also, attacking in cyberspace costs much less than defending, because (and this a major stumbling block) threats typically strike under the threshold of the use of force and attribution is cumbersome: the Internet might be militarizing, but militaries alone can hardly retaliate, which in many ways complicates the picture. Another obstacle lies in the intrinsic difficulty in regulating among sovereign peers a domain which is populated by a multitude of non-state actors (OTTs and the ICT industry, hacktivists, criminals) whose operational capabilities may easily exceed those of many sovereign states. States try to assert their prominence in cyberspace through military or intelligence operations, the promotion of international normative approaches, national regulations or technological solutions, but the struggle is continuous and the relationship very complex. For instance: criminals are enemies, but may sometimes provide useful capabilities and plausible deniability to governments' doings. The private sector is not only a competitor to states' prominence in cyberspace: it is also where innovation happens and technological superiority materialises, and it is essential for states in order to mobilize cyber power. Therefore, in order to enhance cyber security at the national level, a comprehensive "whole of society" approach must be established, which in turn brings us back to our first point: cultural change takes time.

If the picture already looks gloomy, there's a more fundamental question hampering the development of global norms, and therefore making a persistent fight among states in cyberspace unavoidable. As we explained in ISPI's first Report of the Center on Cybersecurity, Confronting an 'Axis' of Cyber?, while the West sees the Internet as a "neutral" infrastructure where content cannot be constrained because "centuries-old battles over human rights and fundamental freedoms are now playing out online", autocratic regimes view the Internet as a threat to their grip on power, and social media servers located outside of the government's control as an intrinsic risk to their survival. This fundamental cleavage emerged more than twenty years ago at the United Nations, when, in 1998, the Russian Federation presented to the UN General Assembly a proposal for a resolution titled "Developments in the field of information and telecommunications in the context of international security". The

Russians wanted to discuss both cyber security and the limitations to destabilizing online content (revealingly gathered together by Moscow under the label of "threats to the information space"). The West refused to have that discussion, on the grounds, essentially, of its self-proclaimed moral superiority: if we want to safeguard an open Internet and freedom of expression, the West argued, it is not possible to negotiate information's content. Ironically, more than twenty years later, the West is accusing Moscow of manipulating online content in order to destabilize the social order and democratic processes. Since then, five successive rounds of negotiations unrolled at the UN within the Group of Intergovernmental Experts on Developments in the Field of Information and Telecommunications. Some successes were achieved in developing a voluntary code of conduct for states in cyberspace – we will see what the ongoing sixth Group will be able to accomplish - but the cleavage between the West and autocratic regimes regarding the freedom of Internet content seems irreconcilable.

The Internet is therefore one of the privileged platforms of the ongoing Great Power competition. The immediate result is the diffusion at the global level of the principle of digital sovereignty, intended as the application of technological and normative solutions to uphold the ultimate responsibility of the state over national cyber infrastructures and data. This is not only a development we observe in China or Russia, that are both busy implementing technical solutions to allow the segregation of their Internet traffic from the rest of the world's. The ongoing decoupling of the ICT supply chain can also be understood in this context, and this is certainly a process impacting heavily even in the West, as shown by the harsh debate about Chinese hardware and 5G connectivity. But there is more: in this ISPI Dossier we consider cleavages that are widening even amongst like-minded and allied countries, such as those resulting from the global normative patchwork created by different national legislations in cyber security, or the restrictions to the free flow of data because of privacy and national security concerns, or, even, the discovery of long-term computer network operations against own allies' most sensible targets.

Since, in cyberspace, the weakest link is the most likely next target, every state has an international obligation to "do its part" by strengthening its domestic cyber resilience, and a national duty to build its relative cyber power. But cybersecurity is a team sport, and individual efforts will not suffice in order to safeguard a secure and free "cyber global common" for mankind. We might never see a cyber domain such as the one dreamt of by Barlow or even vaguely resembling Rousseau's ideal "State of Nature", but we need to avoid drifting in cyberspace towards a Hobbesian homo homini lupus that would justify Leviathans which areincompatible both with cyberspace stability and with the values the West needs to preserve.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

April 2020

Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road

Dennis Broeders
Institute of Security and Global Affairs - Leiden University
Fabio Cristiano
Institute of Security and Global Affairs - Leiden University

'Cyberspace' became a UN issue in 1998 when Russia first tabled a resolution on 'Developments in the Field of Information and Telecommunications in the Context of International Security' with the aim of starting negotiation of a treaty to regulate the possible use of ICTs in international conflict. Interestingly, what Russia feared most at that time was the 'development, production or use of particularly dangerous forms of information weapons', i.e. information warfare, which is arguably what Russia is best at today. Most Western states – in this debate often grouped under the term 'likeminded states' – did not want to go down the route of negotiating a multilateral treaty. In their view cyberspace did not substantially differ from the offline world and thus standing international law would be sufficient for its regulation. The compromise between these positions was the start of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (commonly referred to

Dennis Broeders is Associate Professor of Security and Technology and Senior Fellow of The Hague Program for Cyber Norms at the Institute of Security and Global Affairs of Leiden University, the Netherlands.
Fabio Cristiano is a postdoctoral researcher of The Hague Program for Cyber Norms at the Institute of Security and Global Affairs at Leiden University in the Netherlands.

as UN GGE). In 2002 the first UN GGE went to work. Since then, a succession of six different working groups has contributed, through ups and downs, to fostering the role of the United Nations as a normative power in the promotion of responsible state behaviour in cyberspace.

THE YEARS OF CONSENSUS AND FAILURE

The first round did not yield a result, but in in 2010, 2013 and 2015 the groups produced reports, which some countries lovingly refer to as the 'acquis' of the process. The 2010 report reached consensus on what threats were emerging in cyberspace. The 2013 report made its mark by recognizing that international law – especially the Charter of the United Nations – is applicable in cyberspace. The 2015 report found a way around the difficult negotiations on the question of how international law applies in practice, by formulating eleven 'non-binding rules for responsible state behaviour' some of which echo principles of international law, such as due diligence and human rights protection.

In 2017 the group again tried, and failed, to tackle the contentious issue of how international law applies in cyberspace: there was no consensus report. Moving beyond the general dictum that 'international law applies' has proven to be stumbling block. Uncharacteristically for a closed diplomatic process, two delegations publicly vented their frustration, with the American expert accusing some countries of wanting to 'walk back progress made in previous GGE reports' and the Cuban delegation accusing some countries of trying to militarize cyberspace by focusing the discussion on the right to self-defence, countermeasures and international humanitarian law.

FRAGMENTATION AND RESURRECTION

After the failure of the 2017 round, some commentators were quick to declare the UN GGE process dead. In the lull that followed the 'norms process' found other outlets and fragmented. Work continued in multilateral regional fora, such the ASEAN Regional Forum, the Organisation of American States and the Organisation for Security and Cooperation in Europe, in new private initiatives such as those led by Microsoft or Siemens, and in multistakeholder fora such as the Global Commission on the Stability of Cyberspace. Moreover, in 2018 France launched 'the Paris Call for Trust and Security in Cyberspace', a non-binding set of norms that reads like a 'best of' album, that was signed by 78 states.

The reports of the UN GGE's death had been greatly exaggerated, as there is currently a sixth UN GGE in place. However, things are not back to business as usual at the UN. In November 2018 the UNGA adopted two resolutions: one American-backed resolution calling for a sixth UN GGE (2019-2021) and a Russian- backed initiative establishing the first UN Open-Ended Working Group (OEWG) for cyberspace, fragmenting the norms space further. The mandates of these two processes overlap for 90% but the membership is vastly different. The UN GGE consists of 25 national experts negotiating a report, while the OEWG is open to all UN member states. In promoting the OEWG Russia 'championed' the cause of legitimacy and representativeness,

claiming that "the practice of some club agreements should be sent into the annals of history", and all member states should have a say.

MUTUALLY ASSURED DIPLOMACY: BETWEEN GEOPOLITICS AND THE NEED FOR A RULES-BASED ORDER

As geopolitical winds blow strong both inside and outside of the cyber domain, countries may harden some of their long-held positions. Russia and China's focus on information security and regime continuity - opposed to the likeminded states' focus on technical cyber security – is now firmly connected to the principle of 'digital sovereignty', that appeals to many countries and feeds further polarisation. The Sino-American tensions on trade - and particularly on 5G and Huawei - translated into China's demand to address supply chain security in both UN processes, stressing that "states should not use national security as a pretext" for limiting market access.

Both UN processes will also have to revisit the issue of a new treaty vis-à-vis standing international law and norms. Most recently, and brazenly, the Russian delegate to the OEWG commented that "if international law applies in cyberspace, why are foreign hackers electing the president of the United States?" to underscore the point that maybe norms will not be enough for holding wrongdoers to account. Meanwhile, further deliberation is required to address some of the actual security issues in cyberspace that occur below the threshold of armed conflict: how will states address those cyber operations like NotPetya, the attacks on the Ukrainian electricity grid, or election interferences?

Providing answers to these open-ended questions will affect whether both processes will yield a meaningful result, as both require consensus and affect each other. The UN's facilitation of two different but entangled processes might be characterised as 'Mutually Assured Diplomacy', as it appears likely that either both initiatives will be successful or that both will fail. If one political camp sabotages the other's process, the other camp is likely to respond in kind. Moreover, geopolitics are as likely to steer the direction and outcome as cyber issues themselves. And, as often with new technologies, powerful states will favour at least some strategic ambiguity to keep their hands free, while smaller states will tend towards increasing predictability by arguing for rules of the road.

ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

April 2020

Overcoming Fragmentation in Cyber Diplomacy: The Promise of Cyber Capacity Building

Andrea Calderaro
Political Analyst

The Internet is a decentralised structure whose functioning depends on a series of complementary technical protocols, laws, and international regulations. As a result of this, its well-functioning entails negotiations among a variety of stakeholders, including those responsible for developing digital markets, policies, legal frameworks and technical standards. It is this shared responsibility among industry, citizens and governments that translates into what is called the multistakeholder approach – a model that enables relevant stakeholders to jointly engage in negotiations concerning principles, rules, norms and technical standards. This approach has characterized the global governance of the Internet since its early stages in the 1990s when the main challenge was the identification of a management solution for the Internet domain name system (DNS), in accordance with economic and policy priorities of governments and industry. In order to move the debate beyond the technical dimension of the Internet, the World Summit of Information Society (WSIS) was the first forum promoted by the United

Andrea Calderaro is a Senior Lecturer (Associate Professor) in International Relations at the Department of Politics and International Relations and the director of the Centre for Internet and Global Politics at Cardiff University.

Nations in 2003 to launch international cooperation to establish a sustainable transnational governance model for the Internet, involving civil society, in addition to industry and governments. Of particular relevance, one of the key outcomes of the WSIS was the formalisation of multistakeholder inclusivity as a defining feature of the next two decades of Internet governance.

FROM INTERNET GOVERNANCE TO CYBER DIPLOMACY

Since then, the massive expansion of digital infrastructure, and markets, society and governments subsequent dependency on connectivity, has increased the exposure to cyber threats, and pushed cybersecurity to the centre of governments' agenda. Some cyber threats are perceived as an attack on a state's sovereignty, and approaches to cybersecurity include among other military responses. As a matter of national security, states are therefore increasingly taking control over the governance of cybersecurity, moving debates over safe and stable connectivity infrastructure ever more toward intergovernmental fora and bi-lateral agreements among governments. This multilateral approach defining cybersecurity initiatives is effectively a dialogue between states, largely excluding other stakeholders from decision-making processes. As a result, the multistakeholder model that enabled civil society and industry to play an active role in Internet governance next to state actors, are slowly either replaced or developing alongside and apart from cyber diplomacy dialogues, which are principally led by governmental actors. Along this line, the UN has formalized a multilateral approach to cybersecurity, specifically through the establishment of the UN Group of Governmental Experts (UNGGE) intended to "advance responsible State behaviour in cyberspace in the context of international security" (United Nations 2015). While the UN has announced the support of a multistakeholder approach to cybersecurity by inviting civil society and industry representatives to contribute to the UNGGE via the Open-Ended Working Group (OEWG), we have little evidence that these inputs will influence negotiations between the formal UNGGE members. At this point in time, we can conclude that given the relocation of states to the forefront of negotiations around norms, international law, and Internet governance models, the established format of multistakeholder governance has slowly been replaced by multilateral forms of negotiations. This transition represents a shift of narratives in international cooperation in the cyber domain, from Internet Governance as one of the key challenges of Global Governance, to Cyber Diplomacy where dialogue among states is by and large in line with state-based approaches adopted in the domain of international security.

NEW INTERNET GEOGRAPHY AND CYBER CAPACITY BUILDING

In order to strengthen a coherent and coordinated Cyber Diplomacy dialogue and avoid a fragmented approach in the domain of cybersecurity, it is crucial to take into consideration the fast-changing geography of the Internet, which is increasingly moving away from its original concentration in the global north. Today, more than the 50 per cent of the global Internet

population lives in Asia, while North America and Europe only represent 8 per cent and 20 per cent of the Internet population, respectively. [1] However, countries in the global south are expanding their connectivity infrastructure faster than their technical and policy capacity to deal with potential cyber threats. Given the expectations that by 2025, 75 per cent of the Internet population will be living in the global south,[2] there is a significant need to develop a Cyber Diplomacy dialogue beyond the global north.

In this context, the development of global cybersecurity goes together with the launch of strategies aimed at supporting states in their efforts to develop cyber capacities, referred to "the diffusion of technical, governance and diplomatic skills among relevant stakeholders, in order to ensure the development of sustainable connectivity".[3] Examples of this such initiatives targeting the global south include the Global Forum of Cyber Expertise, which brings together governments, international organizations and industry engaged in cyber capacity building initiatives, and the formalization of an EU Cyber Capacity Building strategy with the release of the "Operational Guidance for the EU's International Cooperation on Cyber Capacity Building" in 2018. These initiatives lend evidence to how the promotion of cyber capacity building initiatives is an emerging priority in state's foreign policy to support countries in the global south to develop their competences and response capacities to cyber threats, but also to enhance their role in the Cyber Diplomacy dialogues by playing an active role in the negotiations of cybersecurity treaties in intergovernmental venues, such as the UN GGE.

In this critical juncture for global cybersecurity governance, it will be important to diversify participatory practices, and to ensure that transnational non-state actors and governments from the global south are included in core circles and debates. By expanding cyber capacity building efforts, we may enhance the prospects of an inclusive and robust governance model that will outlive the current securitization of cyber policies.

1. ITU defines as "Internet users" individuals that have accessed the Internet from any devices within the last 12 months. ITU Statistics "Global ICT developments 2001-2017", available at: http://www.itu.int/ict/statistics

2. Kleiner, B.D., Nicholas, P.J., Sullivan, K., 2014. Cyberspace 2025: today's decisions, tomorrow's terrain'. Microsoft, Redmond, WA.

3. Calderaro, A., Craig, A., 2020. Transnational Governance of Cybersecurity: policy challenges and global inequalities in cyber capacity building. Third World Quarterly.

Don't Kill the Internet: Governments' Shuting-Down Practices

Samuele Dominioni
ISPI

Last February, a few days before the presidential election in Togo, around 30 human rights and press freedom organizations sent a letter to the incumbent president calling upon him to maintain the stability and openness of Internet. The letter encouraged the government to "undertake the necessary measures to ensure that the Internet service providers and relevant actors ensure an open, accessible, and secure Internet throughout Togo during this electioneering period." Indeed, there were growing concerns that the authorities could have blocked web traffic through an "Internet shutdown". This is "an intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information."[1] Togo already experienced something like this in 2017 amid a wave of protest against authorities; the government is now facing a trial for shutting down Internet on that occasion. Luckily, this time, as

Samuele Dominioni is a Research Fellow at the ISPI Centre on Cybersecurity, in partnership with Leonardo. He holds a Ph.D. double degree in political sciences and political history at the Institut d'Etudes Politiques de Paris (Sciences Po) and at the IMT School for Advanced Studies in Lucca.

the preliminary election report by the ECOWAS election observation mission suggests, there were no cases of Internet blocking during last February's presidential election. Nevertheless, the letter sent to the president is emblematic insofar as it clearly depicts a worrisome trend taking place around the world: government Internet shutdowns. Given the paramount importance of cyberspace to our societies, the practice of blocking or slowing down access to the net constitutes, for the United Nations Human Rights Council, a violation of the fundamental human rights law. Despite this condemnation took a form of a non-binding resolution, it shall set the agenda for more relevant initiatives at UN level.

This practice, also known as "internet kill switch", has become more and more common all around the world since 2011. According to the latest report published by KeepItOn there has been an increase in the number of countries using this practice (25 in 2018 and 33 in 2019) and it also signals a trend toward sustained and prolonged shutdowns. It would be common sense to think that authoritarian countries, which usually curb media and freedom of expression, would be at the forefront in Internet kill switch practices. However, as the report highlights, more than half of the shutdowns in 2019 occurred in India, which is the largest democracy in the world. It should be mentioned that these shutdowns are not always nationwide but refer to specific regions or localities such as Jammu or Kashmir. The country with the most nationwide shutdowns is Algeria, with 6 cases in 2019. Authoritarian regimes also implement practices other than Internet kill switch, and they often take the form of censorship policies implemented through legal or informational measures. For example, as reported by Freedom House, there are 12 countries around the world that resort to criminal charges to control online speech during electoral periods. Another 24 countries use informational measures like content manipulation in the form of propagandistic news, outright fake news or the hijacking of real social media accounts.

A question naturally arises: how it is possible for a government to shut down the Internet? In fact, there is no such a thing as a turn-off button. Indeed, purposely shutting down the connection in a specific location or at the national level is a practice that requires some level of government control over the infrastructure comprising Internet, which – by definition – is a network of networks. In order to block the flows of data it is necessary to interrupt the process by which data are transmitted between hosts (i.e. computers). This is permitted by a protocol called Transmission Control Protocol/Internet Protocol (TCP/IP) that has four levels of transmission: application, transport, Internet, and network interface. A government that wants to block or slow down access to the net has to intervene at application and network interface levels. At the application level the government has to control (directly or indirectly) the Internet Service Providers (ISPs), through which it can change the configuration of Internet traffic for their users. The government in some cases may also decide to interrupt the work of the local internet exchange points (IXPs) located

on its national territory. The IXPs are physical infrastructures that facilitate the exchange of data between ISPs (inside and outside a country). Cutting off Internet cables is another option, certainly with higher costs, and it won't affect connections via satellite (even if the latter counts for less than 1% of overall data traffic). Moreover, a government must also control two elements located in the network interface level. The first one relates to the Domain Name System (DNS) that translates IP addresses into readable texts (such as ispionline.it). In this case a government may remove access to its country code DNS (for example websites ending with . it for Italy); however, other DNSs will be still working. Last but not least, interrupting data flows at the Border Gateway Protocol (BGP), which is the routing protocol – an essential part to connect ISPs, also those that are not part of the same network. In other words, shutting down Internet is not easy but possible. While there are ongoing debates about to what extent a country can be really isolated from the net, for sure it is possible to cut out some part of Internet. Everything depends on the presence of, and on the control that a government has over, Internet infrastructures.

Therefore, beyond figures about Internet shutdowns, what should be monitored closely is the ongoing trend among public authorities to gaining control over Internet infrastructures. There are some countries, such as Russia, that are reformulating their cyber governance policies to gain the ability to detach their portion of the net from the rest of the Internet. Although this is often justified in terms of a cybersecurity countermeasure in case of massive cyber-attacks, it can have another use – a political one. The latter must be considered for what it is both at the normative and ethical levels. An issue that should be addressed with urgency by the international community to set clear codes of conduct, for example in case of elections, or even binding resolutions. We are speaking about a fundamental human right, after all.

1. See the report here.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

April 2020

Chinese Behaviour in the Information Domain: A New Norm of "Informational Mercantilism"?

Dean Cheng
Asian Studies Center - Davis Institute for National Security and Foreign Policy

The People's Republic of China (PRC), and more importantly the ruling Chinese Communist Party (CCP), is a major factor in the global information environment. China is both a consumer and a supplier for that network. Some 850 million Chinese people have access to the Internet. China is an integral part of the global supply chain for information and communications technologies (ICT). As one of the world's most important political as well as economic powers, the PRC also has an enormous impact on both the governance of that environment, and the norms that influence it.

Unfortunately, the PRC's perspective on international norms indicates that it has an approach that is fundamentally at odds with those of the West.

The PRC has long valued sovereignty as a key international principle. Indeed, it might be said that there is no greater defender of the Westphalian system of sovereign states in today's world than the PRC. While Europe has sought to create a transnational structure

Dean Cheng is Senior Research Fellow, Asian Studies Center, Davis Institute for National Security and Foreign Policy, The Heritage Foundation

erasing international boundaries, China has very clearly worked to strengthen them. China's claims to the South China Sea, Tibet, and Xinjiang, as well as Taiwan, are all based on the notion of territorial sovereignty (and its view of where its boundaries lie). But its support for sovereignty is not limited to the geographic and political space, but also extends to the cyber domain.

The PRC has long opposed the role of the Internet Corporation for the Assignment of Names and Numbers (ICANN) in administering the Internet. ICANN pursues a multi-stakeholder model, which includes not only nations but academia, civil society (e.g., religious institutions, non-governmental organizations). From the Chinese perspective, Internet governance should solely be the purview of states—not surprising given China's growing political influence.

In proposing Internet codes of conduct at the United Nations, the PRC (along with Russia and several Central Asian republics) has consistently emphasized that "policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international internet-related public policy issues."

As important, in the PRC view, non-state actors should have limited access to the Internet. This begins with Taiwan. China opposed granting Taiwan its own domain suffix (--.tw), insisting that it should use China's domain suffix (--.cn). But it extends to other non-state actors as well. Chinese-backed proposals also state that the Internet should not be used to disseminate calls for "separatism," which would affect not only Taiwan, but also Uighur and Tibetan activists.

If the state should be sovereign in establishing international norms for information, it has no limits on domestic norms. China's rejection of informational privacy is a matter of record, reflected in the creation of the Orwellian "social credit score" system. PRC officials make no effort to hide the fact that not only are Chinese citizens under constant monitoring, but that the information that is derived will be used to preemptively control their actions. Some 11 million flights and 4 million train trips were prohibited because the would-be traveler had a social credit score problem.

Meanwhile, under a variety of Chinese laws, including the National Security Law (2015), Cybersecurity Law (2016), and National Intelligence Law (2017), firms and corporations, including Internet Service Providers and hardware vendors, and even foreign firms can be required to provide Chinese officials with access to a variety of data. Under the National Intelligence Law, for example, companies would have to "grant intelligence officials the right to enter otherwise restricted facilities, examine private records, investigate and question personnel, and access or even requisition communications or transport equipment owned by companies or individuals." Notably, this is not only in response to criminal investigations, but in order to support Chinese collection of intelligence.

This incredibly expansive view of the writ of the Chinese government is reinforced when one examines other, more problematic

Chinese activities in the information domain, such as exploitation of the Border Gateway Protocol (BGP) system. The BGP system helps route Internet traffic, but is built upon the presumption that key players will not abuse their role as traffic directors. A recent paper, however, suggests that China Telecom, a state-owned telecom provider, has used its "points of presence" in North America and elsewhere to redirect significant chunks of global Internet traffic to China. The professors note that, unlike accidental rerouting, these shifts were marked by "lengthened routes and abnormal duration." A similar incident involving European mobile traffic occurred in June 2019, with "traffic destined for some of Europe's biggest mobile providers … misdirected in a roundabout path through the Chinese-government-controlled China Telecom" for over two hours.

Such incidents suggest that China is pushing a norm of informational mercantilism, centered on extending its sovereignty within the information domain. Viewed in parallel with similar Chinese efforts to extend its sovereignty into other international common spaces (e.g., the South China Sea), it suggests a broader Chinese effort to define a new set of norms which challenges the current international rule set. In particular, China appears to be trying to create a self-serving set of norms, whereby, it will expand its own rights in international common spaces, whether in the cyber or physical realms, while rejecting others' rights to do the same. In particular, in the cyber realm, China's actions suggest that it will expand its own access to others' information, whether through legal, technical, or illicit means, even as it closes off its own market to foreign competitors and vendors.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

April 2020

On the Geopolitics of Russia's Sovereign Internet Law

Xymena Kurowska
Central European University

Russia's sovereign Internet law, a series of legal acts that came into force in November 2019, has made headlines as a sign of the increasing fragmentation of Internet governance. Russian authorities justify the laws as a defensive measure against the threat of being cut off from the global Internet, following the US' National Cyber Security Strategy adopted in September 2018, which accused Russia, along with China, Iran, and North Korea, of using "cyber tools to undermine [the US] economy and democracy."

The coalition of states advocating for "free, open, and secure" Internet based on the multistakeholder model,[1] known as "the like-minded", interpret the law as yet another manifestation of growing digital authoritarianism. These positions arguably represent distinct and divergent visions of the Internet, commonly referred to as "open" versus "state-controlled". But these broad geopolitical stances conceal as much as they reveal.

The idea of a lost Golden Age of the Internet,

Xymena Kurowska is Associate Professor of International Relations at Central European University and special rapporteur on norms for EU Cyber Direct.

when we were all presumably empowered by global connectivity, in contrast to the current threat of fragmentation, is a distinct political narrative. However, the narrative downplays the extent to which the Internet never operated independently from existing political, economic, and social dynamics and power structures. In fact, it has often provided a platform for a digital version of off-line configurations, such as, for example, a marketable space for big corporations to determine the contours of the contemporary international society of consumers.[2]

The New America Foundation's Sasha Meinrath captures well the ambiguous dynamics of both the "unfragmented space" and challenges to it when he complains that "the motivations of those nations questioning America's de facto control over the global Internet may vary, but their responses are all pointing in the same troubling direction: toward a Balkanized Internet."

What the narrative of the threat of fragmentation obscures in particular is the emergent macro-securitisation[3] of the Internet, which binds cyberspace through threat rather than market opportunity. Whatever liberal democratic rhetoric may say, there is a definite global shift away from the multistakeholder model towards multilateralism, understood in its traditional sense as alliance politics—that is, as the competition of rival groups of states that align to balance against threats by their adversary. In other words, we do have a consensus in the global Internet that it is a strategic space that generates security threats.

As a result, and as Milton Muller also argues, the fragmentation narrative is really about the future of national sovereignty in the digital world. This global consensus that digitalisation is dangerous is indeed how the Internet has been hacked. That is, first economic dominance and then security politics have crowded out the empowering potential of unrestrained global connectivity. Russia has played a crucial role in the latter aspect of this process. It has laboured since the late 1990s to regionally and globally streamline the notion of "international information security" and to regulate the Internet in a regime similar to nuclear and other weapons of mass destruction, thereby branding the Internet itself as a weapon.

There is a distinct rationale behind this. In contrast to Western approaches focused on technology, protection of communication infrastructure, and free access to information, Russian authorities want to have control over the contents of the information itself: unregulated information creates vulnerability since it can be used as a tool of influence in the socio-humanitarian sphere, that is, for "winning hearts and minds". Russia has been somewhat vindicated in this rationale, like many other state and non-state actors, in the aftermath of the Snowden revelations which cracked the ideal of a globalised free flow of information.

The Kremlin's expansion of its "digitally sovereign" Russia programme reflects, in this context, the dynamics of global cybergeopolitics. The development of the Russian segment of the information and communication network, known as Runet, is part of this agenda. It serves, above all, as a defence of the regime against

unchecked external influence, which is blamed for sowing discontent among Russia's population. It requires Russian telecom firms to install '"technical means" to re-route all Russian Internet traffic to exchange points managed by Roskomnazor, Russia's telecom watchdog, as a precaution in the case of threat of disconnection from the global Internet.

However, the roll-out of Runet is technically challenged and its implementation may never meet the demands of the rhetoric of technological sovereignty. Russia missed the opportunity of building a firewall similar to China's. And yet while it may not be able to fully escape global interoperability, its technical cooperation with China over Internet infrastructure makes the technical fragmentation of the global Internet closer to becoming a reality.

In summary, then, Runet is a geopolitical gesture made in relation to power struggles over the idea of digital sovereignty; however, seen in a broader context, it is ultimately about building a new world order. Russia capitalises on existing digital inequalities and perceptions of digital chaos to sow its own version of global discontent. Exacerbating fears and excavating alliance strategies from the past, it contributes to creating a mindset of global militarisation. In its geopolitical pursuit of a leading role in the global order managed by a few great powers, Russia has effectively neutralised the politically empowering potential of the Internet by reasserting powerful security logics. The world has swiftly bought into this tactic—the US as much if not more than any other actor—and this is how the Internet has indeed been hacked.

1. The multistakeholder model of Internet governance envisages broad participation and collaboration among governments, private sector, civil society, academia and technical community, in contrast to "the sovereign Internet" which is fully controlled by national governments.

2. On the fallacies of the fragmentation narrative more broadly see Milton Meuller, Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace, Polity Press, 2017.

3. On the concept of macro-securitisation see Barry Buzan and Ole Waever, "Macrosecuritisation and security constellations: Reconsidering scale in securitisation theory," Review of International Studies, 35(2009), 253-276.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

April 2020

Privacy Shield EU vs. USA: Transatlantic Cleavages?

Marco Bassini
Bocconi University

The field of privacy and data protection is probably the one where the most interesting moves occurred in the European Union's legal system over the last decades, leading to remarkable political externalities, most notably in the relationship with the United States. If a "Balkanization" of cyberspace did take place, the protection of privacy and personal data offers a privileged standpoint from which to look at how the European Union institutions, and above all the Court of Justice, contributed to such a result.

The "Privacy Shield", as it is known, came into force after the Court of Justice invalidated the "Safe Harbour" agreement between the European Union and the United States. By handing down its decision in the Schrems case, the Court of Justice marked a point of no return, finding that it was no longer allowed to transfer personal data from the EU to the US in the absence of safeguards ensuring that European citizens' privacy received an adequate degree of protection. The Court of Justice, in fact, found that the mechanism provided in the

Marco Bassini, PhD, is a postdoctoral researcher in Constitutional Law at Bocconi University (Milan), where he is also an adjunct lecturer of Public Law and Fundamentals of IT Law.

Safe Harbour agreement, ratified by the European Commission in 2000, did not secure a level playing field in terms of personal data protection.

The reasons behind this failure lie especially in the unprecedented consequences of the digital revolution, which led to new challenges for the right to privacy. Additionally, the Court of Justice stance was not immune, perhaps, to the influence of the NSA scandal, which had just then brought to light the controversial attitude of the US government and its respective agencies towards the personal information of non-American citizens. Last but not least, the Court of Justice handed down the Schrems judgment amidst the long-awaited passing of the GDPR (which came only a few months later, in May 2016), which marked a Copernican paradigm shift in Europe.

In light of this, the legal consequences of the Schrems judgment were definitely significant, but its political implications were probably even more momentous, for a variety of reasons.

The US government was de facto forced to enter into negotiations with the European Union to revisit its own legislation and practice on the processing of personal data (including of non-American citizens). Indeed, the judgment of the Court of Justice formally concerned the European Commission decision, which green-lighted the Safe Harbour agreement, i.e., an act of EU law. Nonetheless, the reasons why said decision was struck down have to do with US law and practice concerning data protection, which the Court of Justice deemed inadequate for safeguarding the fundamental rights of European citizens to privacy and data protection.

On the other hand, this outcome could not be avoided by the US government. In fact, most Internet service providers (e.g., cloud computing service providers, search engine service providers, social media networks) are based in California, and the data processing activities (including of data of European residents) they carry out take place in the US, so that they can benefit from the more lenient approach of that legal system. Since the most prominent market players of the digital economy are American companies, the adoption of a new scheme governing the transfer of data from the EU was an inevitable choice. From the US perspective, building a new "transatlantic bridge" became a priority to allow data flows from the European Union and thus ensure the continuity of those services which, albeit operated by American companies, targeted European residents. Likewise, from the EU perspective, entering a new agreement was essential to avoid a substantial shutdown of the services made available by digital and tech companies.

The Privacy Shield came therefore into force with high expectations, substantially strengthening the safeguards for European citizens. But was the lesson actually learned? Now, whether the level of protection granted to the personal data of European citizens is actually fit for its purpose is something that must be assessed on a regular basis. This requires the US Department of Commerce and the European Commission to carry out an annual review of the Privacy Shield to confirm the effectiveness of the important measures

that have been undertaken. At the same time, it also implies that the Privacy Shield is equally affected by "downward" and "upward" fluctuations in the degree of protection of personal data occurring on both sides of the Atlantic. Since the European Union attaches a greater significance to privacy, it should not come as a surprise that (also as result of the GDPR) the EU nowadays stands out as a modern flag-bearer of data protection, thus being able to largely influence even US-based players. It is not by coincidence that some scholars (e.g, Oreste Pollicino) correctly argue that, the EU being such a privacy "fortress", it should be able to develop flexible mechanisms for a transatlantic dialogue — mechanisms that appear more and more necessary in an interconnected world, at least to avoid a "Cold War" 2.0 based on the governance of personal data.

ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

April 2020

OTT & Metadata vs. Users' Privacy: Same Team?

Gianmarco Cristofari
University of Macerata

To talk about Over-the-Top companies (OTT), like Google or Facebook, and their successful data-driven business model implies the need to take technological development into account. The idea is quite simple and reasonable: new technologies – from big data to machine learning - allowed unprecedented technical possibilities that were not only simply available but also thinkable less than 20 years ago.

As a consequence, we have been witnessing an incremental focus on the onlife behaviour in relation to new technologies, especially the Internet and user's privacy. We can now connect the whole world – the argument goes – but this comes with a cost: someone can see my behaviour online, as I constantly leave digital traces whatever I do; and to be seen is to be controlled. The notions of informational privacy and data protection have therefore evolved in this framework.

Cutting-edge was the idea that behaviour

Gianmarco Cristofari is a Phd student in "Global Studies" at the University of Macerata. He conducts research on the relationship of law, new technologies and politics, with particular reference to the privacy legislation

meant money. This might still be a little counterintuitive and it struggles to become common sense, but a descriptive element can be isolated from ideological interpretations: it is possible to make money by collecting and aggregating personal data, using the data to make predictions on future behaviours and sell them to someone. This new logic has been astutely called "surveillance capitalism". This is an entire business model and a logic of accumulation based on the necessity to monitor human experience. Indeed, the new technical possibilities allow to objectively observe human behaviour in its historical development and interaction on a statistical level (e.g. social networks). From observation comes high precision in the prediction of future behaviour and, therefore, the possibility to modify this behaviour via advertising. Indubitably, this ongoing process plays a relevant role even in the formation of our digital identity. However, if the invasion of privacy has become an economic necessity, what is then left of the notion of privacy?

By investigating the historical relevance of the concept of privacy itself, one could also claim that it is time to change our glasses. In fact, the already vague definition of privacy has blurred drastically since its creation and faced a sociological mutation. The right to privacy was detected in the folds of the American Constitution to protect the private sphere against the new technological means of intrusion. Anyhow, it was understood either as a shield against the State (public vs private) and its excessive power or as the thing that allows having an intimate, personal life inter pares (private vs private). In this sense, the emersion of OTT creates a new theoretical challenge. Are they still only private entities or rather are they gathering a "quasi-public" relevance by providing crucial services for our lives and the world around us?

However, the picture sketched so far is much more complex as information on personal data acquired importance also for political purposes. This is blurring the traditional lines around which privacy was conceptualized (private vs public). Indeed, knowledge and technical tools for data and metadata elaboration are fundamental elements of power also for the State in its interplays both at domestic and international level. Therefore, data protection is in a certain measure linked to and dependent on other systems, and considering it by itself may fall short: it will be difficult to regulate properly the asymmetrical relationship of extraction of user's privacy if the State itself has decided to turn to the same logic in his quest for social control. This approach could have relevant consequences, especially for democratic regimes. For example, the recent scandals as Wikileaks and Cambridge Analytica have shown that OTT, as well as governments, gained unprecedented instruments for behavioural monitoring and modification that affect deeply and directly the democratic process.

In addition, little democratic debate took place to decide if and under which limitations these instruments are lawful. Privacy and data protection laws – including the General Data Protection Regulation (the "GDPR"), the boldest and most advanced existing laws

on the matter – do not take into account the asymmetrical dimension of knowledge and power. In this sense, the OTT appear to be the contractors in charge of the digitization of some services of public relevance, with great informational power. For instance, right now, the hairdresser around the corner and Amazon have basically the same obligations under GDPR. Of course, assessments and actions to comply with the GDPR differs greatly under an accountability[1] approach, but there is no distinction among actors and, therefore, no effective control of the OTT's activities.

Nowadays, the surveillance logic of the extraction of human experience is broadly diffused. Nevertheless, there has never been any constitutive act where stakeholders agreed upon the rule of the game. It was just a bunch of companies, some of which are now considered OTT, that set the rules. This process, called fracture of law, implies that when a new field (so far unregulated) is discovered, the first one that manages to grasp its relevance can rule according to its preferences. The law tries to follow as it can, regulating specific matters, with all the issues arising from a multi-level and multi-agent complex system rapidly developing over time. Nowadays, our existing privacy laws struggle to control the OTT's activities on privacy matters.

Then maybe we should not only be asking if OTT and user's privacy playing in the same team, but also if they are playing the same sport.

1. Accountability means that every data controller has to self-assess the risk in data processing, and take adequate measure to avoid or minimise the risk. Therefore, high risk and a large-scale processing lead to a greater work do in term of compliance. See also art. 24 of the GDPR.