The Emperor's New E-Clothes: State Sovereignty in the Cyber-era

https://www.e-ir.info/2018/01/02/the-emperors-new-e-clothes-state-sovereignty-in-the-cyber-era/

MATTIA TOMAY, JAN 2 2018

On October 20, 2017, the interior ministers of the G7 countries met in the island of Ischia, Italy, to discuss cooperation with regard to security information exchange and the fight against terrorist-sponsored propaganda on the Internet. This year, the exclusive forum of the "big seven" of the world economy was joined by the "big 4" of the world-wide web: Google, Microsoft, Facebook and Twitter. Together, they agreed to enhance cooperation between the public and the private sector on issues such as counterterrorism and counter-radicalization, and to increase the power of the Global Internet Forum to Counter Terrorism – a newly-born forum launched by Facebook, Microsoft, Twitter and YouTube bringing together government representatives, e-businesses and civil society organizations (Biagio, 2017).

That of the G7 is yet another example of the latest trend in international Internet governance where the boundaries between public and private, regulator and regulated, ruler and ruled, sovereign and dependent have become more blurred than ever before. Arguably, this may be of little shock to anyone living in the era of globalization, where the thought of states being the only actors of the international system sounds to many as naïve – to say the least. However, what makes the case of the Internet – and more generally that of the cyberspace – particularly interesting and worth investigating, is the extent to which it challenges and at times even competes with the classical privileges of the sovereign actor (i.e. the nation state).

The distinctiveness of this unusual relationship between the *body politic* and the *body cyber* becomes ever clearer when issues of internal security and the national interest are at stake. For instance, in the wake of the Charlie Hebdo attacks Microsoft stated to have received as many as 14 government requests for accessing data which public authorities considered useful in the chase of the suspected terrorists. What is even more surprising is that Microsoft was able to provide some of this data in less than one hour, but only once the company itself had concluded that the governments followed a proper recourse and that the emergency context justified their solicitation (Bodoni, White, & Hodges, 2015). When it comes to the disclosure of sensitive information to governments, that of Microsoft does not seem to be an exception: Facebook, too, has a "three steps" internal procedure it follows before proceeding passing on the data (Senese, Mossé, Kent & Sacquet, 2017). Another great example of the rising importance of "international data politics" is represented by the recent decision of the Russian government to block access to LinkedIn. The decision came after the giant of professional-network refused to move its servers to the country, in order to meet the Kremlin's desire to "protect Russian citizens from having their personal data abused by foreign governments" (Walker, 2016). Moscow is surely not alone in its attempt to keep its citizens' data within the national borders, Turkey, China and even Germany being other notable cases (Cory, 2017).

This being said, some legitimate questions may arise. Should big tech companies arrogate to themselves the discretionary powers of deciding whether a situation is "urgent" enough? What if these examinations require prior knowledge of highly confidential material related to national security: should governments be put in a position where they are pressured to share this information with a foreign private corporation? And again, should data be confined within the territorial limitations of nation-states? Does it make sense to apply the logic of territorial sovereignty to the seemingly borderless dimension of "the cloud"?

In short, does the cyber-era urge us to make new sense of the conception of sovereignty?

Traditional sovereignty: a brief overview

In answering these questions, we should first recall the philosophical foundations of traditional Westphalian sovereignty. As challenged as it may be (and rightly so) from innumerable standpoints – in academia as well as in practice – this is in fact the paradigm of sovereignty which has dominated the western model of political organization both at the national and the international levels. Therefore, understanding its classical assumptions is essential to grasping the considerable extent to which the logic of sovereignty is being challenged in the cyber age. As we will see, among these assumptions the desire of order is one claiming a paramount role in the justification of sovereignty – from both an internal and an external perspective.

First, the need of order, harmony and an efficient organization of human activity served as the main motor behind the institution of a sovereign. To put it in Hobbesian terms, due to the multitude of contradictory human needs and desires, life without a state would be nothing but "solitary, poor, nasty, brutish, and short" (Hobbes, 2015, p. XIII, 9) – a so-called "state of nature". In order to bring peace and order in this context, the self-governing agency of each and every individual needs to be somehow constrained and transferred to a new self-governing collective: a political community, a state, a "commonwealth". The sovereign can therefore be identified in a figure (for Hobbes, the absolute monarch), an organic collective (for Rousseau and Locke, "the people" or a representative body thereof) or even a document (e.g. a constitution). By this sort of collective agreement, properly said social contract, and a gradual process of legitimization (Weber, 1965), it becomes conceivable for individuals to think of themselves as citizens. In renouncing a part of their own "personal sovereignty" (of self-help, self-determination, self-preservation), they in fact delegate it to the sovereign entity which – through its monopoly on the means of coercion (e.g. violence, taxation, as well as other forms of social regulation) – administers mutual rights and obligations and better assures security and prosperity (at least in relative terms).

Secondly, the need of order, peace and independence is also crucial to the external idea of sovereignty, which depicted states as the primary members of international society since 1648. It was in fact with the Peace of Westphalia that statehood, sovereign equality and independence became the foundations of the international system, the paradigm based on which international affairs would be conducted ever since (Pufong, 2001, p. 480). Isolated states replicate in fact at the international level the same anarchical condition preceding the establishment of the state. In order to insure order, states recognize each other as the sole responsible and legitimate authorities over specific territories and populations. By agreeing to common principles and frameworks of cooperation – a sort of international contract – they restrain themselves from conquest and expansion for the sake of stability and orderliness. Perhaps, therefore, external sovereignty is best summarised by the eminent wordings of the Permanent Court of International Justice in the Lotus case: "the first and foremost restriction imposed by international law upon a State is that (…) it may not exercise its power in any form in the territory of another State" (*P.C.I.J. Lotus – France v. Turkey*, 1927, para. 45).

This brief and perhaps stylized account of internal and external sovereignty may raise a few eyebrows. Indeed, throughout the last century, both have evolved and proved less dogmatic in theory as well as in practice. The rise of non-state actors (international organisations, non-governmental organisations, multinational corporations, criminal organizations, etc.,), the consolidation of human rights norms, the emergence of "general interests" and "common resources" at the international level and – indeed – the rise of the Internet, seem to have rescaled claims of undisputed sovereign authority. But can we really say they have dismissed it?

Practical challenges to sovereign prerogatives in the cyberspace

In view of the above, it should not come as a surprise that the official discourse surrounding the Internet, the cyberspace and its governance is often state-centred. One of the most important pieces of soft international law in the realm of privacy and data protection, UN Resolution 68/167, is exemplar. In fact, the document inevitably ends up envisioning states as the primary responsible actors with regard to the respect, assurance and enforcement of fair cyber practices, while remaining silent on the roles and responsibilities of other entities on the matter. International

relations and international law are no strangers to this latter issue, that is to say the place of individuals and non-state actors in a realm which by definition concern the conduct of affairs between nation states. Since the last century, however, multi-national corporations, non-governmental organizations and individuals have been recognized at least partial international legal personality, notably in the realm of international human rights law and international criminal law. However, if in the case of international relations this became possible as a "top-down" development where states were in a position to "grant" rights in a judicial space created by themselves, the case of the cyber dimensions presents some thorny specificities. As we will see, concepts such as coercive monopoly, territoriality, and order make little sense in this dimension.

While the origins of the state date back to the Middle Ages, those of the cyberspace are rooted in the Cold War's technological arm race between the United States and the Soviet Union. It was within the walls of the American Information Processing Technique Office, in fact, that the idea of creating a series of linked computers which would allow people to access and share information was born (Kleinrock, 2008). From this (apparently) simple foundational core, the whole current World Wide Web would spring. The basis of the new technology, which was later adopted by universities to connect research communities, was a host-to-host type of communication relying on protocol-based networking between two or more nodes (i.e. a communication end-point). In this information exchange, the code (i.e. the commands, the algorithms containing the instructions about the transmission) has a role of paramount importance. As Lessig (2000) noted in his famous essay "Code is Law", codes represent the very architecture of the cyberspace, as they contain the rules based on which interactions between servers and machines function. This way, codes function like the social norms and the laws which regulate relations between members of a society derived from the state structure. Thus, we can see protocols as all powerful "internet laws", whose importance (and only apparent "neutrality") can dictate the type of interaction between not only computers, but also the actors behind them. Nevertheless, there is one important disparity we should make between the "normative/legal architecture" of the social and the cyber worlds: knowledge access. Though laws are often far from being easy, usually one needs not be a lawyer to understand the foundations of her/his country's legal system, how they are taken are implemented. In fact, these are the basics of civic culture and open societies. But what about code? Laypeople (and I count myself among them), which is to say the vast majority of internet users, hardly know what protocols are, let alone how they work and what their content is. On top of this, this type of information can even be difficult to attain by tech gurus – think of closed-source softwares. Hence, expertise plays a pivotal role in the cyberspace, which speaks volumes about the challenges this places on state apparatuses and bureaucracies which often encounter difficulties with the slightest technological change. While Goliath-states might have represented the most adequate organizational structure to the capitalist mode of production, the management of natural resources, the mobilization of intercommunal violence (international war), they now find themselves confronted by David-hackers, rootkits and viruses-writers, seemingly more knowledgeable and better-equipped to act in the cyber-environment. In short, the Internet world is partly a meritocratic "leveller" which magnifies the importance of actors endowed with high expertise and quick adaptability (individuals or small groups), at the expenses of complex organisms resisting change and technological development (state bureaucracies). Thus, mutually beneficial cooperation becomes vital.

Some may argue that the issue of expertise is just a temporary one and that states will eventually be able to catch up with the times or embrace (force?) cooperation. Surely, the developments described in the beginning of the text seem to support this argument. Nevertheless, another challenge emerges when we consider some technological developments which undermine altogether the important role of the state as the intermediary of social relations. This is the case of Blockchain technology – the building block of ventures such as Bitcoins and Bitnation. Before tackling this issue, something needs to be said about the "nature" of data. Data are not imaginary figures flying above us in an intangible cloud, they are real information which is stored in physical servers in a specific country and under a specific national legislation. Especially after Edward Snowden's revelations on US domestic and international surveillance, many states have pushed for a much stricter regulation of data localisation, justifying it by reference to the need of securing their national interest and the personal information of their citizens (Polatin-Reuben & Wright, 2014). This type of "data nationalism", is particularly appealing for governments: it reinforces their idea of sovereignty by plausibly making foreign intervention and surveillance more difficult, while making it easier for them to scrutinize (whether lawfully or not, this is another question) their own domestic flow of data. This being said, what makes Blockchain critical, is the way through which it manages to evade political attempts to enforce the principle of territoriality principles into the cyberspace. In (very) simple terms, Blockchain can be described as a vast, shared

database of information which is continuously updated, available and visible by and on each computer device with access to it (Bagley, 2016). None of these databases is a "copy" and none them is the "original" to be preserved somewhere. On the contrary, millions of computers host the same content, a fact which surely guarantees for transparency and accessibility. But while preventing information from being violated by hackers and governments, this also has important implications with regard to central transactional institutions such as the state. Bitcoins illustrate this case well. Our monetary system is based on trust: trust on the value of a currency, trust on creditors to reimburse debts, trust on banks operating transactions on our behalf, trust on the stability of a central bank. What happens when the whole system is replaced by a stateless currency created by an algorithm? What happens if people start shifting away their trust from fallible central bankers toward a nearly all-mighty computer treasury? For some libertarians and some anarchists, this feels like the coronation of a dream: freedom from government can finally be absolute. For others, this development represents the ultimate madness of neoliberalism. Surely enough, on their part, governments are not excited to see their undisputed right to issue currency being eroded by a computer (see, e.g., Das, 2017; Higgins, 2017; Mangoli, 2017). And just if Bitcoins were not enough cause of worry, governments are now also faced by a project, that of Bitnation, which describes itself as:

"a decentralized, open-source movement, powered by the Bitcoin blockchain 2.0 technology, in an attempt to foster a peer-to-peer voluntary governance system, rather than the current 'top-down', 'one-size-fits-all' model, restrained by the current nation-state-engineered geographical apartheid, where your quality of life is defined by where you were arbitrarily born." ("Join The Team," 2015)

These examples of decentralized forms of Internet governance clearly go further than the internal organization of cyberspace business. By taking on regulatory and distributive functions, they establish themselves as competitors to the state structure in key realms of sovereignty. While states can move towards the banning of certain technologies and a sort of "nationalization" of key Internet fields such as that data storing, it seems unlikely and unfeasible for them to be able to assert their power in the cyberspace ad libitum. Thus, in conclusion, we should try to answer one last question: what is the future of state sovereignty in the cyberspace?

Towards a cyber social contract?

More often than not, political scientists tend to look at technology and the cyberspace as developments threatening the established order, developments that states need to tame or turn in their favour. In his famous "Abiding Sovereignty" Krasner (2001) mentions cyber only in relation to cybercrime and potential criminal activities; Hare (2009) defends borders as useful constructs in the field of cyber relations. Jensen (2014) and Shen (2016) both understand cyber sovereignty as the need to impose national sovereignty on cyber actors. The main problem with these ideas is that they all end up forcing a concept originated in the Europe of 1648 to a contemporary issue. By looking at IT as a source of "disorder" and a problem to be solved, states and scholars alike miss the fundamental differences between the cyberspace and the international arena. The new dimension introduced by the Internet revolution is one where territoriality, nationality, laws, monopolies and war make little sense. There, states co-exist with a multiplicity of actors in a way which is far from our classical understandings of hierarchy and legitimacy, which instead are continuously questioned and overturned. Thus, interaction is not thoroughly institutionalized, coercion is not centralized, laws, norms and "cyber consciousness" are barely present. In a nutshell, agents in the cyberspace find themselves in a state-of-nature condition, in a cyber polity-in-the-making where reciprocal actions have still not evolved into mature cooperation. A "cyber social contract" is absent, and those that expect it to be imposed by governments are doomed to disappointment. In fact, states are one among the many potential "citizens" of the cyberspace, not as the ex-ante sovereigns. It is unimaginable to think that any political community could emerge from the Rousseauian and Hobbesian states of nature through the imposition of a certain rule by one member upon everyone else. The first step sustaining order is the realization of the disadvantages coming from the collective "abuse" of our natural freedoms and the willingness to partly renounce them for the sake of living in a functioning society. Thus, unless a Cyber Sovereign able to guarantee and uphold the rights of all its members is established, each actor is set to encroach the freedoms of the others – which explains our difficulty in understanding the awkward positions of companies like Facebook and Microsoft vis-à-vis powerful nation state, and vice versa when it comes to data protection and surveillance.

Classical political philosophers envisioned the state as a human body, the organs of which represented different societal figures, fulfilling different roles for the sake of the whole. Just like different organisms in nature function in different ways, the Cyber Sovereign would not need to function in the same way as modern nation states: regulated codes could perform the role of laws; institutionalized cooperation between the public, private and corporate sectors could represent a viable branch of "government"; decision-making processes could take advantage of the great opportunity the Internet offers with regard to direct democracy; and so on. A new, revolutionary conception and practice of sovereignty will need to be paired by a congruous type of governance which, indeed, will not emerge from one day to another but will take time to be institutionalized and legitimized, just as modern states did in the past.

Sure, the future of the cyberspace and that of state sovereignty are all but certain in today's ever-changing world. But anarchy, for once, may have its perks: allowing us to reimagine and reinvent – hopefully for the better – our outdated conceptions of what sovereignty means.

References

Bagley, J. (2016, September 18). What is Blockchain Technology? A Step-by-Step Guide For Beginners. Retrieved October 28, 2017, from https://blockgeeks.com/guides/what-is-blockchain-technology/

Biagio, S. (2017, October 20). Terrorismo, i big hi-tech al G7: così contrasteremo la cyberpropaganda.*Il Sole 24 ORE*. Retrieved from http://www.ilsole24ore.com/art/tecnologie/2017-10-20/terrorismo-big-hi-tech-g7-cosi-contrasteremo-cyberpropaganda-163932.shtml?uuid=AEFcJisC

Bodoni, S., White, A., & Hodges, J. (2015, January 20). Microsoft Gave Data on Charlie Hebdo Probe to FBI in 45 Minutes. *Bloomberg.Com*. Retrieved from https://www.bloomberg.com/news/articles/2015-01-20/microsoft-fights-unregulated-snooping-amid-terrorist-threat

Cory, N. (2017). *The Worst Innovation Mercantilist Policies of 2016*. Information Technology and Innovation Foundation. Retrieved from https://itif.org/publications/2017/01/09/worst-innovation-mercantilist-policies-2016

Das, S. (2017, October 27). Bitcoin Banned as a Payment Method in Indonesia, Adopters Will Be "Dealt With." *CryptoCoinsNews*. Retrieved from https://www.cryptocoinsnews.com/bitcoin-banned-payment-method-adopters-will-dealt-indonesian-central-bank/

Hare, F. (2009). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?, *3*, 88–105. https://doi.org/10.3233/978-1-60750-060-5-88

Higgins, S. (2017, September 28). Russia Likely to Ban Bitcoin Payments, Deputy Finance Minister Says. *CoinDesk*. Retrieved from https://www.coindesk.com/russia-likely-ban-bitcoin-payments-deputy-finance-minister-says/

Hobbes, T., & Gaskin, J. C. A. (1998). *Leviathan*. Oxford: Oxford University Press.

Jensen, E. (2014). Cyber Sovereignty: The Way Ahead. *Texas International Law Journal 50*, 275–304.

Join The Team. (2015, September 13). Retrieved October 28, 2017, from https://bitnation.co/join-the-team/

Kleinrock, L. (2008). History of the Internet and its flexible future. *IEEE Wireless Communications*, *15*(1), 8–18. https://doi.org/10.1109/MWC.2008.4454699

Krasner, S. D. (2001). Abiding Sovereignty. *International Political Science Review / Revue Internationale de Science Politique*, *22*(3), 229–251.

Lessig, L. (2006). Code: Version 2.0. *Basic Books*. Retrieved from http://codev2.cc/download

Mangoli, D. (2017, October 23). ICO Ban in Japan a "Definite Possibility." *CryptoCoinsNews*. Retrieved from https://www.cryptocoinsnews.com/japan-may-no-longer-be-a-safe-haven-for-icos/

Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. Presented at the 4th Workshop on Free and Open Communications on the Internet, San Diego (CA). Retrieved from https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben

Pufong, M. G. (2001). State Obligation, Sovereignty, and Theories of International Law. *Politics & Policy*, *29*(3), 478–519. https://doi.org/10.1111/j.1747-1346.2001.tb00600.x

Senese, A., Mossé, M., Kent, G., & Sacquet, M. (2017, October 9). *The Internet, private actors and security challenges.* Sciences Po, Paris, France.

Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace.*Chinese Political Science Review*, *1*(1), 81–93. https://doi.org/10.1007/s41111-016-0002-6

S.S. Lotus – France v. Turkey (P.C.I.J. September 7, 1927). Retrieved from http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm

Walker, S. (2016, November 17). Russia blocks access to LinkedIn over foreign-held data. *The Guardian*. Retrieved from http://www.theguardian.com/world/2016/nov/17/russia-blocks-access-to-linkedin-over-foreign-held-data

Weber, M. (1965). *Politics as a Vocation*. Fortress Press Philadelphia, PA.

Written by: Mattia Tomay

Written at: Sciences Po Paris

Written for: Ksenia Ermoshina

Date written: November 2017