Big Tech as an Actor of Global Security and Geopolitical Conflicts

An International Conference

organized by Center for Interdisciplinary Media Research and Analysis (CARISM), Paris-Panthéon-Assas University

and by Centre Internet et Société, French National Centre for Scientific Research (CNRS)

in scientific partnership with the Strategic Research Institute of the French Ministry of Armed Forces (IRSEM)

2-3 May 2024, Salle des Conseils du Centre Panthéon

Call for Proposals

From the war in Ukraine to geopolitical rivalries between China and the USA, and terrorism-related threats, the digital giants colloquially known as “Big Tech” corporations are increasingly involved in issues of national and international security.

Most often, their involvement stems from **their services and platforms serving as new theaters of conflict in cyberspace** (Singer & Brooking, 2018), as with Russian or Chinese information operations on social media during elections (Jeangène Vilmer et al., 2018; Charon & Jeangène Vilmer, 2021; Marangé & Quessard 2021); or when Donald Trump, then President of the United States, took to Twitter to threaten North Korea with nuclear war (Schwartz, 2022). In such cases, the role of Big Tech companies in conflict is an infrastructural, near invisible one, as the services they provide and govern are used as intermediaries for conflict (Musiani et al. 2016). In other cases, **these firms are themselves the objects of conflict**, as with the multiple bans on Huawei's 5G (Statista, 2020) and on the social network TikTok owned by Chinese conglomerate ByteDance (Chan, 2023); or Russia's designation of Meta as a "terrorist" organization in the context of the Ukraine war (Euronews, 2022). In International Relations scholarship, it is commonly assumed that private corporations act as “ambassadors” of their country of origin and that their technical innovations are prolongations of national power on the world stage (Carr, 2016; Strange, 1996; Keohane & Nye, 1998). It therefore comes as no surprise that conflict situations involving Big Tech are becoming more common with the internationalization of Chinese internet giants, signaling the emergence of non-American Big Tech. Meanwhile, tech giants’ political power is increasingly recognized by the traditional actors of international affairs, with multiple states

naming “tech ambassadors”. Finally, Big Tech companies are increasingly becoming **actors of global security in their own right,** by “co-producing” security alongside public authorities (Bellanova & de Goede, 2022) and even in some cases launching their own initiatives, such as Microsoft’s Digital Geneva Convention, or YouTube, Twitter, Facebook and Microsoft’s launch of the Global Internet Forum to Counter Terrorism (GIFCT) in 2017.

While it is not unprecedented for private companies to be involved in security issues, policymaking and enforcement (Abrahamsen & Leander, 2016), and especially so in cyberspace (Dunn Cavelty, 2016), the variety and importance of current ties between digital giants, security and conflict seems to indicate a general trend towards the privatization of security through these (quasi-) global players. Due to their scale and economic clout, Big Tech companies profit from a particular form of “entrepreneurial private authority” (Srivastava, 2021) or “platform power” (Culpepper & Thelen, 2020). In practice, this notably means a privileged access to public authorities and international fora, and the ability to impose standards ("best practices", definitions, processes), as well as to form coalitions to defend their interests. As its central position in the digital industry and economy is being translated into a centrality in security-related policy areas, Big Tech can leverage its integration within security governance networks and geopolitical rivalries to fend off threats of antitrust action (Woll, 2019), thereby consolidating its market power and becoming further integrated into high politics, raising multiple concerns in terms of legitimacy, accountability, and sovereignty (Monsees et al., 2023).

Such developments invite us to look beyond the instrumental study of Big Tech platforms, services and technologies, and to turn our attention to the agency of these actors in global security and geopolitical conflicts. With this in mind, the aim of this conference is to initiate a holistic discussion on the diversity of the security roles played by these companies, how they “learn to see the world through a security lens” (de Goede, 2018:26) and their relationship to traditional security networks. A number of disciplinary perspectives and fields of study are relevant to this theme, and the goal is to bring together their respective contributions. This conference will be of relevance for, and expects contributions from, a range of disciplines including but not limited to international relations, political science, media studies, security studies, science and technology studies and political economy.

1. Big Tech in transnational conflicts and social movements

How do Big Tech companies position themselves or try to remain neutral when their services are used during armed conflicts or insurrections? We seek to understand how companies shape their ‘crisis response’, both in relation to international conflicts, where Big Tech takes a stand for one country against another (or avoids taking a stand altogether), and to local conflicts where one party seems to be favored by Big Tech in the context of social movements.

a. Transnational conflicts

Facebook/Meta’s communication on the subject is clearly the most open one, ever since it was formally accused by the UN of contributing to the Rohingya genocide in Myanmar (Whitten-Woodring *et al.,* 2020). Following the Rohingya scandal, in 2019 Facebook created a Strategic Response Team (Meta, 2019) with a mission to operate global watch of international conflicts to better adapt its services’ features and avoid escalating the situation on site. Five years since its launch, the team’s efficiency remains hard to measure, while its functioning itself is quite vague. It appears that conflicts are still handled by the company on an *ad hoc* basis. Since its launch, Meta’s Oversight Board insists on the

need for a specific conflict management policy that is seemingly being developed but is yet to come into effect (Oversight Board, 2022).

The company has also adapted its content policy in Eastern Europe following the Russian invasion of Ukraine (Meta, 2022), and in Afghanistan after the US army left the country and the Taliban regained power (*The New York Times*, 2023). In other conflicts, namely in Ethiopia or during frequent clashes between Israel and Palestine, Meta is regularly accused (including by its own Oversight Board) of being too passive or the other way around, of ruthless censorship of certain parties to the conflict (notably Palestinian voices) (Human Rights Watch, 2022).

According to recent studies (Kaneva *et al.*, 2023), the role of social media in the Russia-Ukraine conflict is quite unprecedented, with Ukraine using social media to crowdfund the war and creating an IT army (Manor, 2023). On a more personal level, the new owner of Twitter (X) Elon Musk taking a clear stand on the Ukraine conflict and sending Starlink Internet drones to Ukraine caused controversy as well (Twitter, 2022). As far as Google is concerned, a recent study shows the introduction of bias and manipulation in search engine results in favor of pro-Kremlin sources for Ukraine-related requests made from Russia (*Novaya Gazeta*, 2023), in what can only be described as a counterintuitive move, given that these same sources are blocked by the company on YouTube.

b. Social movements

Big Tech companies' role in social movements became clear during the "Arab Springs", with Facebook playing a defining role (Wolsfeld, 2013), while social media affordances allowing transnational connections and global support for local causes go as far back as the Zapatista movement in the nineties (Russel, 2005).

Traditionally, social media are viewed as facilitating social movements' development, without, however, guaranteeing their efficiency (Tufekci, 2019). On the other hand, Access Now claims that Big Tech's sanctions against Russia have a negative impact on Russian civil society (Access Now, 2022).

Partisan conflicts between the right and left are also of relevance when they generate violence. A telling case in this regard was President Donald Trump's suspension from all mainstream social media platforms in January 2021 following the Capitol attack. The move fueled accusations of "wokeness" (Sobande *et al.,* 2022) and censorship, leading to a notable growth of existing alt-right platforms and the creation of new ones (including Trump's own, Truth Social). In response, Apple and Google (Android) banned the most libertarian services from their app stores for failing to protect their users, while Amazon (AWS) kicked them off of its cloud services -- a phenomenon that has been called "deplatformization" (van Dijck et al., 2021).

2. Big Tech and everyday "trust and safety"

While moments of crisis concentrate exceptional threats over a short period of time, platform companies must also deal with safety and security issues that are ongoing. These include threats related to terrorism and violent extremisms (Borelli, 2021), disinformation and hate speech (Badouard, 2021), and organized crime. How do Big Tech companies integrate security considerations into their respective product development processes, platform governance and internal organization?

As security and safety-related scrutiny and demands from public authorities and users grow, Big Tech companies are increasingly forced to respond in order to adapt to multiplying regulations, and/or to

preempt scandals and new projects to regulate them. In the European Union, the DSA notably mandates that VLOPs assess the "systemic risks" associated with their services and deploy mitigation strategies. As Big Tech adapts to these new roles, its products evolve. Visible changes in the name of safety include, for instance, prominent reporting buttons, ReDirect links, fact-checking labels or 'sensitive content' warnings on Facebook, YouTube's information panels for Covid content or state-owned media, or Twitter (X)'s "are you sure you want to retweet this without having opened the link first" pop-up. Other adaptations which are more opaque to end users bring out questions of censorship (Badouard, 2020), such as the formation of "content cartels" (Douek, 2020)[1] and other industry standard-setting mechanisms[2], the deployment of "automated" moderation (Gorwa et al., 2020) or delisting/downranking/demonetization[3] (Goldman, 2021).

From the point of view of civil society organizations and individuals, platform design and affordances are particularly salient. For instance, the availability of strong encryption on given services can contribute to protecting users from authoritarian regimes. However, measures implemented in the name of user safety also have unforeseen externalities: encryption can complicate the investigative process for security services, seemingly neutral platform design choices were shown to favor conservative viewpoints (Schradie, 2019), while some content moderation policies disproportionately affect certain vulnerable groups' right to free expression (Common, 2020), such as LGBTQ+ activists (Grison & Julliard, 2022), or journalists documenting war crimes (Human Rights Watch, 2020). Meanwhile, actors who are deplatformed hone their camouflage techniques (Renaut, 2020; Criezis, 2023) or migrate to services lacking the human and/or technical capacity or the willingness (small, encrypted and/or alt-right platforms, Fediverse) to moderate their services (Conway, 2020). The most extreme individuals then find themselves in spaces where they are less likely to be contradicted, and where it is more difficult for the authorities to monitor them, hence a lively debate on deplatforming and its efficiency. How do the Big Tech arbitrate between freedom of speech, user safety and national security concerns, all the while balancing them with their commercial interests ?

As technology companies appropriate these new considerations, their sociology as organizations is also evolving. The hiring of experts, often with previous backgrounds in academia or law enforcement roles is an important aspect of this adaptation, given that those companies' cultures traditionally favor engineering roles (Frenkel & Kang, 2021). Public-facing Public Policy and Government Affairs teams are tasked with responding to ever-increasing demands from public authorities and regulators, while behind-the-scenes Product Policy and Trust & Safety teams develop rules, plan for use cases involving so-called "bad actors" and mitigate recurring threats. For social media corporations like YouTube (Google) and Meta, large numbers of content moderators to enforce policies --usually subcontractors— are a key part of the equation as well (Roberts, 2019). What means are these staff given to conduct their mission, and how do they make themselves heard by upper management? Despite all the evidence that safety, in particular through content moderation, is what makes (or breaks) the value of a platform (Gillespie, 2018), Frances Haugen's testimony and recent layoffs appear to show that these teams are still seen as adjustment variables which are peripheral to the 'core (engineering-based) business' of Big Tech, thereby questioning the industry's capacity for collective learning. A noteworthy development in

[1] Examples include the GIFCT on terrorist content, the Tech Coalition for child sexual abuse materials (CSAM), or the informal group to secure the 2020 US election from foreign interference (Isaac & Conger, 2020).
[2] For instance the Digital Trust and Safety Partnership.
[3] This last 'freedom of speech, not freedom of reach' approach is particularly favored by X (formerly Twitter) owner Elon Musk.

this regard is the move towards a structuration of 'trust and safety' as a new professional field, with the emergence of a Trust and Safety Professional Association (TSPA) to advance the interests of these professionals within Silicon Valley.

3. Big Tech and digital sovereignty

Never in history has it been clearer than today: digital infrastructures, from the physical ones (submarine cables, data centers, Internet Exchange Points) to the "logical" ones (protocols such as TCP/IP or algorithms such as Google's PageRank) are crucial components in arrangements of power. Thus, the private entities that design these infrastructures and keep them operational, as well as leverage them for their profit, are key actors in these arrangements of power (DeNardis, 2012; Easterling, 2014; Amoore, 2018; Möllers, 2021).

Indeed, Big Tech actors are the designers and de facto "governors" of the infrastructures that influence the field of possibilities for actors of international security. These infrastructures are doubly relevant, because on the one hand, the private actors who manage them follow their own agendas and on the other hand, they act as vectors for the political and cultural soft power of the states where they are situated; in both dimensions, stark conflicts can emerge. In some instances, such private actors can even be likened to technical "standards entrepreneurs", as was the case during the controversy surrounding Huawei as a provider of 5G technology.

For states, particularly in Europe (e.g. Tréguer, 2017), but also in Russia and China (e.g. Budnitsky & Jia, 2018), and other BRICS countries such as India (Gurumurthy & Chami, 2016) Big Tech services raise questions related to "digital sovereignty" (Pohle & Thiel, 2020). While this label is primarily understood to indicate a legal concept and a set of political discourses, digital sovereignty can also be understood as a set of infrastructures and socio-material practices; the concept of sovereignty is re-defined today by a number of political and economic projects which aim to establish autonomous digital infrastructures in a hyperconnected world (Musiani, 2022).

Manifold examples in recent history illustrate this, such as when European or Russian governments host security-defense data at AWS, use Palantir software, or, as mentioned, debate the security soundness of 5G technology provided by Huawei. Finally, regulatory efforts from public institutions sometimes clash with geopolitical considerations, showing the ever more complex relationship between states and platforms. For example, the American peregrinations of TikTok show that, on one hand, the United States is also concerned about digital sovereignty when the hegemony of its champions is compromised; and on the other hand, digital sovereignty issues concern both the lower layers of cyberspace and the surface of the web and the application layer, as shown by data protection and disinformation issues.

4. Big Tech and its relations to traditional security actors

In 2013, Edward Snowden revealed the extent of long-suspected ties between Big Tech firms and the US security apparatus, as leaked documents showed that all major US commercial online service providers participated in the NSA's global PRISM surveillance program. Ties between the American public sector and the tech industry on security issues are prolific and multifaceted, spanning over the whole spectrum of defense, intelligence and law enforcement. They range from strategic R&D investments and service contracts which can be considered part of the US military-industrial complex, to informal relations on foreign policy and law enforcement (Lakier, 2021), and punctual staged or real

resistance[4] (Tréguer, 2019; Thibout, 2021). A decade after the Snowden affair, what do we know of public-private relations between Big Tech and the American security apparatus ?

Beyond the US, the Big Tech firms have also had to develop relations to security and foreign policy bureaucracies in the various regions of the world where they operate. Vice versa, some states have named "tech ambassadors" (Denmark, France, etc.) and the EU opened a permanent office in the Silicon Valley in 2022. In the European Union, intense public pressure around the question of terrorist uses of the internet has led to the establishment of new norms and permanent fora for public-private cooperation at the national and regional levels[5], through which security is "co-produced" across public-private boundaries (Bellanova & de Goede, 2022). But sometimes, public authorities themselves constitute the threat, and the UN's public recognition of Facebook and WhatsApp's role in the Rohingya genocide has also posed the pressing question of how these firms should proceed in cases where their users need protection from their own government.

Lastly, Big Tech is also becoming further integrated within the existing multilateral international security governance landscape, for instance by participating in United Nations Security Council, G7 or G20 meetings. Here, Microsoft stands out due to its longstanding presence at the UN, where it maintains a permanent office and is particularly involved in cybersecurity governance (Hurel & Lobato, 2018; Fairbank, 2019).

How do national and international bureaucracies and regulators manage their relationship to the Big Tech corporations in security-related domains? How do they organize to navigate these relationships? How is the political division of labor negotiated, and what are the power dynamics within the novel "assemblages" of networked security governance (Abrahamsen & Williams, 2010) involving Big Tech? The salience of these questions increases as Big Tech becomes further integrated into global security governance, but such public-private relationships are especially difficult to investigate because of the cultures of secrecy and opacity traditional to both security bureaucracies and Big Tech. Leaks, scandals and transparency efforts (voluntary or mandated) provide periodic glances into their workings, and recent scholarship also shows that revolving door phenomena and public tendering records can provide fruitful insights (Tréguer, 2019; Thibout, 2021; Valdivia et al., 2022).

Organizing Committee

Marguerite Borelli (Carism, Université Paris-Panthéon-Assas)
Ksenia Ermoshina (Centre Internet et Société, CNRS)
Francesca Musiani (Centre Internet et Société, CNRS)
Gulnara Zakharova (Carism, Université Paris-Panthéon-Assas)

[4] Some of the publicized conflicts between the US administration and Big Tech have included privacy-related debates (for instance Apple's refusal to break encryption on the San Bernardino terrorists' iPhone), conducting business in China and periodical resistance from Big Tech staff on specific contracts (e.g. in 2018 with Google employees' vocal resistance to Project Maven, or when Microsoft employees protested a contract with ICE over Trump's immigration policies).

[5] See for instance the Groupe de contact permanent in France, or at EU level, the EU Internet Forum and Europol's Internet Referral Unit (Vieth, 2019).

International Scientific Committee

Olivier Alexandre (Centre Internet et Société, CNRS, France)
Maxime Audinet (IRSEM, Ministère des armées, France)
Romain Badouard (Carism, Université Paris-Panthéon-Assas, France)
Anne Bellon (COSTECH, Université de technologie de Compiègne, France)
Enka Blanchard (LAMIH, CNRS/Université Polytechnique Hauts de France, France)
Maura Conway (Dublin City University, Ireland and VOX-Pol coordinator)
Valentine Crosset (Université de Genève, associée au médialab, Sciences Po Paris, France)
Frédérick Douzet (IFG Lab et GEODE, Université Paris 8, France)
Bharath Ganesh (University of Amsterdam, NL)
Rikke Bjerg Jensen (Information Security Group, Royal Holloway-University of London, UK)
Rikke Frank Jørgensen (The Danish Institute for Human Rights, DK)
Fabrizio Li Vigni (Centre Internet et Société, CNRS, France)
Ilan Manor (Ben Gurion University of the Negev)
Tristan Mattelart (Carism, Université Paris-Panthéon-Assas, France)
Cécile Méadel (Carism, Université Paris-Panthéon-Assas, France)
Julien Nocetti (Centre d'analyse, de prévision et de stratégie, Ministère des Affaires étrangères, chercheur associé à l'IFRI et à GEODE, France)
Sarah Perret (ESPOL, Université catholique de Lille, France)
Maud Quessard (IRSEM, Ministère des armées, France)
Pablo Rauzy (LIASD-PASTIS, Université Paris 8 Vincennes-Saint-Denis, France)

Key Dates

October 10th, 2023: Call for Papers

December 5th, 2023: Submission Deadline

December 15th, 2023 - February 1st, 2024: Evaluation of submissions by the ISC

February 15th, 2024: Notification of Acceptance

May 2nd and 3rd: 2024: Conference at the Centre Panthéon

Guidelines for Submission

Please plan to submit an extended abstract (800-1000 words long, excluding bibliography) that should include one or more research question(s), a description of the data supporting the proposal, the used methodology, the main findings of the paper, and the paper's primary contributions to literature and/or ongoing policy debates.

Panel submissions and alternative formats are also welcome. In this case, please submit a proposal including a working title, brief description of the modalities and questions raised, participants and their affiliations (if relevant), and proposed duration.

Submissions should be sent by December 5th, 2023 to the following address:

bigtechinsec@protonmail.com

References

URLs were active on 11/09/2023.

Abrahamsen, R. and Leander, A. eds. 2016. *Routledge Handbook of Private Security Studies*. London ; New York: Routledge, Taylor & Francis Group.
Abrahamsen, R. and Williams, M.C. 2010. *Security Beyond the State: Private Security in International Politics*. Cambridge: Cambridge University Press.
Access Now. 2022."Civil society to U.S. government: Do not disrupt internet access in Russia or Belarus", 10.03.2022, URL: https://www.accessnow.org/press-release/us-government-internet-access-russia-ukraine-war-sanctions/
Amoore, L. 2018. "Cloud geographies: Computing, data, sovereignty", *Progress in Human Geography*, *42*(1), 4-24.
Badel, L. 2018. Diplomatie économique, diplomatie d'entreprise. In: Balzacq, T. et al. eds. *Manuel de diplomatie*. Relations internationales. Paris: Presses de Sciences Po, pp. 243–261.
Badouard, R. 2020. *Les Nouvelles Lois du web: Modération et censure*. Paris: Seuil.
Badouard, R. 2021. Moderation on social networks. *Réseaux* 225(1), pp. 87–120. doi : 10.3917/res.225.0087.
Bellanova, R. and de Goede, M. 2022. Co-Producing Security: Platform Content Moderation and European Security Integration. *JCMS: Journal of Common Market Studies* 60(5), pp. 1316–1334. doi: 10.1111/jcms.13306.
Borelli, M. 2021. Social media corporations as actors of counter-terrorism. *New Media & Society*. doi: 10.1177/14614448211035121.
Budnitsky, S. & Jia, L. 2018. "Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance", *European Journal of Cultural Studies*, 21, 594–613.
Carr, M. 2016. *US power and the Internet in international relations: the irony of the Information Age*. Houndmills, Basingstoke, Hampshire ; New York, NY: Palgrave Macmillan.
Chakrabarti, S., Birch, R., "Understanding Social Media and Conflict", *Meta*, 20.06.2019, [online], URL: https://about.fb.com/news/2019/06/social-media-and-conflict/
Chan, K. 2023. Here are the countries that have bans on TikTok. URL: https://apnews.com/article/tiktok-ban-privacy-cybersecurity-bytedance-china-2dce297f0aed056efe53309bbcd44a04
Charon, P. and Jeangène Vilmer, J.-B. 2021. *Les opérations d'influence chinoises. Un moment machiavélien*. Paris: Institut de Recherche Stratégique de l'Ecole Militaire (IRSEM). URL: https://www.irsem.fr/institut/actualites/rapport.html
Common, M.F. 2020. Fear the Reaper: how content moderation rules are enforced on social media. *International Review of Law, Computers & Technology* 34(2), pp. 126–152. doi: 10.1080/13600869.2020.1733762.
Conway, M. 2020. Routing the Extreme Right - Challenges for Social Media Platforms. *The RUSI Journal* 165(1), pp. 108–113. doi: 10.1080/03071847.2020.1727157.
Criezis, M. 2023. Wilayat Facebook and Instagram: An Exploration of Pro-IS Activities on Mainstream Platforms. *GNET* 21 April. URL: https://gnet-research.org/2023/04/21/wilayat-facebook-and-instagram-an-exploration-of-pro-is-activities-on-mainstream-platforms/
Culpepper, P.D. and Thelen, K. 2020. Are We All Amazon Primed? Consumers and the Politics of Platform Power. *Comparative Political Studies* 53(2), pp. 288–318. doi: 10.1177/0010414019852687.
DeNardis, L. 2012. Hidden levers of Internet control: An infrastructure-based theory of Internet governance. *Information, Communication & Society*, *15*(5), 720-738.
Douek, E. 2020. The Rise of Content Cartels. URL: https://papers.ssrn.com/abstract=3572309
Dunn Cavelty, M. 2016. Cyber-security and private actors. In: Abrahamsen, R. and Leander, A. eds. *Routledge Handbook of Private Security Studies*. London ; New York: Routledge, Taylor & Francis Group, pp. 89–99.
Easterling, K. 2014. *Extrastatecraft: The Power of Infrastructure Space*. Verso Books.

Euronews 2022. Russia adds Meta to list of 'terrorist and extremist organisations'. URL: https://www.euronews.com/2022/10/12/russia-adds-meta-to-list-of-terrorist-and-extremist-organisations

Fairbank, N.A. 2019. The state of Microsoft?: the role of corporations in international norm creation. *Journal of Cyber Policy* 4(3), pp. 380–403. doi: 10.1080/23738871.2019.1696852.

Frenkel, S. and Kang, C. 2021. *An ugly truth: inside Facebook's battle for domination*. First edition. New York, NY: Harper, an imprint of HarperCollinsPublishers.

Gillespie, T. 2018. *Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media*. New Haven: Yale University Press.

Goede, M. de 2018. The chain of security. *Review of International Studies* 44(1), pp. 24–42. doi: 10.1017/S0260210517000353.

Goldbaum, C., Padshah, S., The Taliban Government Runs on WhatsApp. There's Just One Problem, *The New York Times*, 17.06.2023, URL: https://www.nytimes.com/2023/06/17/world/asia/taliban-whatsapp-afghanistan.html

Goldman, E. 2021. Content Moderation Remedies. *Michigan Technology Law Review* 28(1), pp. 1–60. doi: https://doi.org/10.36645/mtlr.28.1.content.

Gorwa, R. et al. 2020. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society* 7(1), p. 2053951719897945. doi: 10.1177/2053951719897945.

Grison, T. and Julliard, V. 2022. Se mobiliser contre la censure en ligne quand on est pd, trans, gouine ou pute. *Mouvements* 112(4), pp. 167–175. doi: 10.3917/mouv.112.0167.

Gurumurthy, A. & Chami, N. (2016). "Internet governance as "ideology in practice" – India's "Free Basics" controversy", *Internet Policy Review*, 5.

Human Rights Watch 2020. *"Video Unavailable" - Social Media Platforms Remove Evidence of War Crimes*, p. 100.

Human Rights Watch. 2022. "Statement Regarding BSR's HRA for Meta on Palestine & Israel", 27.09.2022, URL: https://www.hrw.org/news/2022/09/27/statement-regarding-bsrs-hra-meta-palestine-israel

Hurel, L.M. and Lobato, L.C. 2018. Unpacking cyber norms: private companies as norm entrepreneurs. *Journal of Cyber Policy* 3(1), pp. 61–76. doi: 10.1080/23738871.2018.1467942.

Isaac, M. and Conger, K. 2020. Google, Facebook and Others Broaden Group to Secure U.S. Election. *The New York Times* 12 August. URL: https://www.nytimes.com/2020/08/12/technology/google-facebook-coalition-us-election.html

Jeangène Vilmer, J.-B. et al. 2018. *Les manipulations de l'information: Un défi pour nos démocraties*. Paris: Centre d'analyse, de prévision et de stratégie (CAPS, ministère de l'Europe et des Affaires étrangères); Institut de recherche stratégique de l'École militaire (IRSEM, ministère des Armées)., p. 214. URL: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/manipulations-de-l-information/rapport-conjoint-caps-irsem-les-manipulations-de-l-information-un-defi-pour-nos/.

Kaneva, N., Dolea, A., Manor, I. 2023. "Public diplomacy and nation branding in the wake of the Russia–Ukraine War", *Place Branding and Public Diplomacy*, Palgrave Macmillan, vol. 19(2), 185-189, DOI: 10.1057/s41254-022-00293-z

Keohane, R.O. and Nye, J.S. 1998. Power and Interdependence in the Information Age. *Foreign Affairs* 77(5). URL: https://www.foreignaffairs.com/articles/1998-09-01/power-and-interdependence-information-age

Lakier, G. 2021. Informal Government Coercion and The Problem of 'Jawboning'. *Lawfare* 26 July. URL: https://www.lawfareblog.com/informal-government-coercion-and-problem-jawboning

Manor, I., "The Power of Memes: Analyzing War-Time Messaging", *The Times of Israel,* 08.08.2022, URL: https://blogs.timesofisrael.com/the-power-of-memes-analyzing-war-time-messaging/

Marangé, C. and Quessard, M. eds. 2021. *Les guerres de l'information à l'ère numérique*. Paris: Presses Universitaire de France.

McGee-Abe, J., "One year on: 10 technologies used in the war in Ukraine", Tech Informed, 26.02.2023, URL: https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/

Meta. 2022. "Meta's Ongoing Efforts Regarding Russia's Invasion of Ukraine", 26.02.2022, URL: https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/

Möllers, N. 2021. “Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State”, *Science, Technology, & Human Values*, *46*(1), pp. 112-138.
Monsees, L. et al. 2023. Transversal Politics of Big Tech. *International Political Sociology* 17(1), p. olac020. doi: 10.1093/ips/olac020.
Musiani, F. et al. 2016. *The Turn to Infrastructure in Internet Governance*. London ; New York: Palgrave Macmillan.
Musiani, F. 2022. “*Infrastructuring* digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices”, *Information, Communication & Society*, 25(6), p. 785-800.
Musk, E., “Starlink service is now active in Ukraine. More terminals en route”, Twitter, 26.02.2022, [online], URL: https://twitter.com/elonmusk/status/1497701484003213317
Oversight Board 2022. Oversight Board upholds Meta’s decision in ‘Tigray Communication Affairs Bureau’ case (2022-006-FB-MR). URL: https://www.oversightboard.com/news/592325135885870-oversight-board-upholds-meta-s-decision-in-tigray-communication-affairs-bureau-case-2022-006-fb-mr/
Pohle, J., & Thiel, T. (2020). “Digital sovereignty”, *Internet Policy Review*, *9*(4).
Renaut, L. 2020. Sur les réseaux sociaux, une djihadosphère en constante évolution. URL: http://theconversation.com/sur-les-reseaux-sociaux-une-djihadosphere-en-constante-evolution-149754
Roberts, S.T. 2019. *Behind the screen: content moderation in the shadows of social media*. New Haven: Yale University Press.
Russell, A. 2005. “Myth and the Zapatista movement: exploring a network identity”, *New Media & Society*, 7(4), 559–577. https://doi.org/10.1177/1461444805054119
Schradie, J. 2019. *The Revolution That Wasn’t: How Digital Activism Favors Conservatives*. Cambridge : Harvard University Press.
Schwarz, J. 2022. Does Elon Musk Know Trump Could Have Started Nuclear War via Twitter in 2018? URL: https://theintercept.com/2022/05/14/twitter-elon-musk-trump-nuclear-war-north-korea/
Singer, P.W. and Brooking, E.T. 2018. *Likewar: the weaponization of social media*. Boston: Houghton Mifflin Harcourt, an Eamon Dolan Book.
Sobande, F., Kanai, A., & Zeng, N. 2022. “The hypervisibility and discourses of ‘wokeness’ in digital culture”, *Media, Culture & Society*, 44(8), 1576–1587. https://doi.org/10.1177/01634437221117490
Srivastava, S. 2021. Algorithmic Governance and the International Politics of Big Tech. *Perspectives on Politics* , pp. 1–12. doi: 10.1017/S1537592721003145.
Statista 2020. Infographic: Which Countries Have Banned Huawei? URL: https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products
Strange, S. 1996. *The Retreat of the State: The Diffusion of Power in the World Economy*. Cambridge University Press.
Thibout, C. 2021. Google et l’État fédéral états-unien : interdépendance, contestation et hybridation. *Entreprises et histoire* 104(3), pp. 142–163. doi: 10.3917/eh.104.0142.
Tréguer, F. 2017. “Intelligence Reform and the Snowden Paradox: The Case of France”, *Media and Communication*, 5,https://doi.org/10.17645/mac.v5i1.821
Tréguer, F. 2019. Seeing like Big Tech: security assemblages, technology, and the future of state bureaucracy. In: Bigo, D. et al. eds. *Data Politics: Worlds, Subjects, Rights*. Routledge Studies in International Political Sociology. Routledge.
Tucker, M., “The Ukrainian honeytrappers persuading Russian soldiers to reveal all”, The Times, 19.07.2023, URL: https://www.thetimes.co.uk/article/ukrainian-honey-trappers-russian-soldiers-russia-ukraine-war-9kxzqwqp8
Tufeksi, Z. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, London: Yale University Press, 360 p.
Tumakova, I., «Гугл у них — слева, Яндекс — справа, администрация президента оперирует ими, как захочет» (“They have Google to the left, Yandex to the right, the Presidential administration operates them to its liking”), *Novaya Gazeta*, 27.06.2023, URL: https://novayagazeta.ru/amp/articles/2023/06/27/gugl-u-nikh-sleva-iandeks-sprava-administratsiia-prezidenta-operiruet-imi-kak-zakhochet

Valdivia, A. et al. 2022. Neither opaque nor transparent: A transdisciplinary methodology to investigate datafication at the EU borders. *Big Data & Society* 9(2). doi: 10.1177/20539517221124586.

Van Dijck, J. et al. 2021. Deplatformization and the governance of the platform ecosystem. *New Media & Society* , p. 14614448211045662. doi: 10.1177/14614448211045662.

Vieth, K. 2019. Policing 'Online Radicalization': The Framing of Europol's Internet Referral Unit. In: Wagner, B. et al. eds. *Research handbook on human rights and digital technology: global politics, law and international relations*. Research handbooks in human rights. Cheltenham: Edward Elgar Publishing.

Whitten-Woodring, J., Kleinberg, M. S., Thawnghmung, A., & Thitsar, M. T. 2020. Poison If You Don't Know How to Use It: Facebook, Democracy, and Human Rights in Myanmar. *The International Journal of Press/Politics,* 25(3), 407–425. https://doi.org/10.1177/1940161220919666

Wolfsfeld, G., Segev, E., & Sheafer, T. 2013, "Social Media and the Arab Spring: Politics Comes First", *The International Journal of Press/Politics,* 18(2), 115–137. https://doi.org/10.1177/1940161212471716

Woll, C. 2019. Corporate Power Beyond Lobbying. *American Affairs* III(3), pp. 38–55.